kuppingercole ANALYSTS

Intelligent SIEM Platforms

Warwick Ashford

February 12, 2024

This KuppingerCole Leadership Compass provides an overview of the market for Intelligent SIEM (I-SIEM) Platforms that go beyond traditional Security Information and Event Management (SIEM) capabilities to identify threats proactively and automatically suggest mitigation measures to meet the requirements of modern IT environments that are typically on premises as well as being mobile and distributed across multiple cloud environments.

Contents

Introduction / Executive Summary

Traditional SIEMs were introduced less than 20 years ago as unified platforms for gathering, analyzing, and correlating security events from multiple sources to provide a centralized overview of all security-related events across the whole enterprise, alert the team of security experts, and provide tools for forensic analysis. For many companies, SIEMs have served as the focal point of their in-house or outsourced security operations centers (SOCs) for several years to support threat detection, investigations, incident management, and regulatory compliance.

However, since SIEM systems were first introduced, the rate at which enterprises are generating data and the IT attack surface have both expanded massively. IT environments have become increasingly mobile and cloud-based, driven by digital transformation, which was accelerated by Covid 19 pandemic due to the need for organizations to enable their employees to work from home. The pandemic also led to an increase in the use of personal devices for work purposes. At the same time, there has been an exponential increase in the number and sophistication of cyberattacks and cyber attackers. The increased size and complexity of corporate IT infrastructures and the proliferation of threats is forcing most enterprises to realize that their existing tools face inherent limitations, preventing them from responding effectively to cyberthreats.

Despite dominating the enterprise security market since the early 2000s, it has become increasingly difficult for organizations to sustain traditional SIEM systems or derive full value from them due to high deployment and operating costs, the shortage of cybersecurity skills, and the rapidly expanding attack surface that has resulted in an unprecedented volume of logs and security alerts being generated by most businesses. This has often meant that SIEM solutions were unable to identify and respond to threats effectively. The lack of automation capabilities and support for two-way integrations with security controls such as firewalls has also limited SIEM systems' ability to make forensic investigations easier for analysts, and consequently, their job remained largely manual and time-consuming.

As a result, SIEM solutions have come under pressure from alternative approaches such as specialized security monitoring solutions for different attack surfaces (endpoints, networks, APIs, and databases) and unified extended detection and response (XDR) solutions. However, SIEM solutions have continued to evolve, expand their coverage, and address their historical challenges. As a result, modern SIEM systems are quite different to their predecessors, taking advantage of several key technological advancements.

The evolution of SIEM solutions has been facilitated mainly by the emergence of breakthrough technologies such as data analytics, machine learning (ML), and cloud-based services that have driven innovation in the cybersecurity market for at least the past decade.

New intelligent automation capabilities, whether integrated directly into newer SIEM solutions or augmenting the existing ones with new functions, ensure that security monitoring, forensic analysis, and incident response remain a core component of any modern cybersecurity architecture, supported by a new generation of SIEM solutions, which will be discussed in further detail in the chapter on the Market Segment.

Despite their checkered history, SIEM tools remain as relevant today as they have ever been because they perform the essential function of providing centralized collection and management of security information across all corporate IT systems.

This Leadership Compass is designed as a tool to help organizations to identify their requirements and map them to the capabilities offered by specific vendors, taking into consideration the size, growth, skills, and budget of the customer organization. To better understand the fundamental principles this report is based on, please refer to KuppingerCole's Research Methodology.

Highlights

- SIEM solutions have dominated the enterprise security market for nearly two decades, but due to high operating costs, an increasing shortage of skilled security experts, and the rapid pace of change in the business IT and cyber threat environments, traditional SIEMs are no longer effective.
- Legacy SIEM tools typically cannot deal with the volume of security alerts generated across an expanding attack surface, they cannot prioritize alerts for investigation, and they lack automation capabilities and two-way integration with security tools to support forensic investigations.
- The SIEM market is experiencing pressure from alternative approaches such as specialized security monitoring solutions and unified XDR solutions, but SIEM solutions continue to evolve and address historical challenges.
- The evolution of SIEM solutions has been facilitated mainly by the emergence of technologies like data analytics, ML, and cloud-based services, which, together with threat hunting and remediation capabilities have ensured the significant improvement of SIEM tools.
- Incorporation of advanced security orchestration, automation, and response (SOAR) capabilities either directly or via two-way API integrations ensures that forensic analysis and incident response can be automated to a high degree, reducing the time needed to respond to a breach.
- Modern SIEM tools continue to evolve, with solutions gaining new capabilities, merging previously standalone tools such as behavior analytics and SOAR into integrated platforms, and updating licensing policies to provide modern, scalable, and I-SIEM platforms.
- The most innovative solutions offer fully integrated unified platforms, fast hot and cold search, and fully federated search capabilities.
- Future innovation will be focused on faster and easier search capabilities, interactive chatbot/assistants, and greater automation and collaboration capabilities.
- Search functionality using natural language processing (NLP) and digital assistants based on generative AI are likely to become standard in the next 12 to 18 months.

Market Segment

In this Leadership Compass, we are looking at the latest SIEM solutions, which tend to be predominantly cloud-based services and continue to evolve as security management and intelligence platforms, incorporating innovative intelligence and automation capabilities.

While we recognize that the market continues to evolve and expand, with other segments like SOAR maturing in parallel, we observe the trend to incorporate these related capabilities into integrated, yet modular and flexible platforms that we consider to be next generation “intelligent SIEM" solutions that provide a high degree of visibility across modern IT environments and deliver a small number of key actionable insights for security teams.

Next-generation I-SIEM solutions are typically designed to cater for businesses of all sizes with the ability to scale as organizations grow, to support all modern IT environments across multiple locations, to automate and coordinate detection and response activities, and to enable security teams to get most out of the resources at their disposal to help address the shortage of cybersecurity skills.

There is also typically a focus on using a combination of real-time correlation, anomaly detection, and user behavior analytics to detect known and unknown threats and to identify related threat activities rather than raising isolated alerts. The most innovative solutions support intelligent decision-making, include sophisticated forensic tools, and support orchestration and automation for incident response. Some are also designed to maximize storage, search, and reporting capabilities, while minimizing the cost, and providing out-of-the-box (OOTB) pre-packaged content in the form of pre-written rules, analytics, and correlation policies to enable customer organizations to get immediate value.

The market for these modern security intelligence and automation solutions continues grow and evolve, with solutions gaining new capabilities, merging previously standalone tools into integrated platforms, and updating licensing policies to provide modern, scalable, and intelligent solutions to ensure that SIEM systems remain a core component of modern enterprise security architectures. While there are several new and smaller players in the market, I-SIEM offerings from larger vendors are likely to benefit as the market appears set to pursue a security vendor consolidation strategy due to reduced security team staffing, and in pursuit of improved security capabilities and improved risk management.

The adoption of I-SIEM platforms is being driven by:

- The worldwide shortage of cybersecurity professionals.
- The rapidly increasing adoption of cloud services and the need to secure critical data in the cloud.
- The growing number of cyberattacks as the attack surface increases with digital transformation.
- The expansion of IT environments to include mobile, edge, and cloud computing.
- The adoption of home working/hybrid working post pandemic.
- The increase in data breach threats driven by state-sponsored cyberattacks.
- Increase in cyber espionage, targeting personal information, credentials, and IP.

- The rapid increase in the amount of data that organizations are producing.
- The need to contain and respond to threats quickly.

The most important driver listed above is the lack of people with the information security skills required to use tools to monitor, analyze, and respond to cyber threats. This underlines the point that intelligent, next-generation SIEM solutions should not require a team of trained security experts to operate. Instead, they should provide actionable alerts that are understandable to businesspeople, a high degree of workflow automation, and a comprehensive end-to-end solution for the security operations center (SOC). Having the solution available as a managed service is crucial and will directly influence its rating.

Delivery Models

Traditional SIEM solutions were mainly deployed on premises, with a substantial investment required for hardware and other infrastructure, as well as a team of skilled professionals to operate them. As a result, SIEM tools tended to be used only by large enterprises or specialized managed security providers (MSSPs) with big enough budgets.

However, with the growing scale, number, and complexity of enterprise networks, applications, and devices, even the most powerful traditional SIEM solutions could no longer keep up with the overwhelming amount of security telemetry produced by all those systems. Unsurprisingly, modern SIEM solutions usually support deployments in cloud-hosted environments with varying degrees of shared management between customers and vendors or third-party MSSPs. However, even such products must still rely on a multitude of connectors, sensors, or APIs scattered across enterprise IT environments to collect and process security telemetry.

More recently, a growing number of vendors have begun offering their SIEM solutions as fully managed software as a service (SaaS) offerings, hiding the operational complexity from their customers. Unfortunately, these services, while offering huge improvements in usability and cost reduction, come with the usual potential challenges of the SaaS model that the customers must be aware of. These include compliance issues with regards to data residency and handling sensitive personal information, as well as limited customization options, potential latency and performance issues, and a generally lower degree of control for the customer. And, of course, even fully cloud-based SIEM solutions must still collect security data from various on-premises sources, although this can also be partially simplified through cloud-native integrations with existing security tools (such as EDR, NDR, and CSPM).

The cost of storage and transmission for cloud-based SIEM solutions can vary depending on the vendor and the specific solution. Some may charge for data storage and transmission, while others may include these costs in their pricing model. It is therefore important to check the pricing model of cloud-based SIEM solutions before making a choice.

Additionally, organizations have to consider that many SIEM products have not evolved entirely organically but are the result of acquisitions or technology partnerships and are offered as suites of different products or services with different deployment options. This is especially relevant for capabilities that rely heavily on machine learning, such as user

behavior analytics, which sometimes do not even support on-premises deployments. This essentially makes every SIEM deployment an inherently heterogeneous, distributed, and hybrid, or even multi-cloud architecture project.

All these challenges make selecting the right SIEM solution even more complicated, especially for smaller companies. It is important to understand that a next-generation SIEM platform should not be considered as just another security tool in a growing arsenal of security experts. On the contrary, the main reason these solutions emerged was to address the growing lack of skilled people in information security to use such tools to monitor, analyze, and respond to cyber threats.

As opposed to traditional SIEMs, next-generation solutions should not require a team of trained security experts to operate. Instead, I-SIEM platforms should provide actionable alerts that even businesspeople can understand, a high degree of workflow automation, and a complete end-to-end solution for a SOC. Helping organizations to find the right balance between functional coverage, usability and efficiency, and budget constraints is the primary goal of this Leadership Compass.

Required Capabilities

This Leadership Compass analyzes I-SIEM offerings or next-generation security analytics solutions that offer substantial improvements in functionality and efficiency over traditional SIEMs by:

- Performing real-time or near real-time detection of security threats without relying on predefined rules and policies.
- Correlating real-time and historical data across a wide range of sources using statistical algorithms and ML to identify malicious operations rather than raising separate alerts.
- Dramatically decreasing the number of alarms by filtering out statistical noise, eliminating false positives, and providing clear risk scores for each detected incident.
- Offering a high level of automation for typical analysis and remediation workflows, thus significantly improving the work efficiency for security analysts.
- Providing integrated forensic and incident management capabilities.

We expect solutions to cover most of these capabilities, and in addition to delivering functionality to support them, they must also meet our requirements for deployment and interoperability with other security tools.

This report, therefore, considers and rates the following capabilities to:

- Work well across on-premises, cloud, multi-cloud, and hybrid cloud environments.
- Integrate well with all data sources, intelligence sources, and existing security technologies.
- Facilitate relatively quick and easy implementations.
- Collect and parse security data from multiple sources in various formats.
- Enrich collected data with additional context from external threat intelligence feeds.

- Apply data analytics and machine learning algorithms to detect patterns and outliers in the collected data to identify previously unknown threats and suspicious activities.
- Provide built-in or tightly integrated tools for incident response and threat remediation.

Drilling into more detail, this report evaluates key capabilities to:

- Collect and parse all system, application, service, or device logs.
- Capture and analyze network traffic info in real time or near real time.
- Collect security data directly from endpoints using agent-based or agentless methods and efficient storage of security events.
- Provide integrations with various third-party sources of security events like firewalls, databases, and application servers.
- Provide integrations with cloud services to enable visibility into hybrid environments.
- Enrich collected data with business-related context information from various sources, including current threat intelligence from external sources.
- Detect patterns and anomalies in security data, thus removing statistical noise and reducing false positives and other unnecessary alerts.
- Identify multiple events from different sources as parts of a single security incident.
- Assign risk scores to each incident according to one or more predefined risk models.
- Provide configurable dynamic dashboards for monitoring various aspects of corporate security and risk posture.
- Deliver a low number of alerts for discovered security incidents, ranked by risk scores.
- Provide on-demand access to all contextual and source security information related to an incident.
- Pivot to related events, entities, or users for a better understanding of the impact.
- Provide a high degree of automation with a large number of prepackaged risk models, policies, reports, and workflows tailored to a specific industry or market.
- Provide built-in or closely integrated incident response capabilities to initiate a fast and coordinated response.
- Provide incident management workflows and threat hunting capabilities.

Additional capabilities considered by this report include:

- Mapping of alerts to known tactics and techniques (e.g., MITRE ATT&CK®)
- Decision support and actionable recommendations enriched with business context information and suggestions for analysts for remediation actions.
- Security orchestration and automation functions.
- Out-of-the-box compliance reporting for major industry frameworks.
- Availability as a managed service.

Consideration is also given to the ease with which solutions integrate with:

- Third-party products and services to expand monitoring to applications, cloud services, security devices as well as support for standard protocols and APIs.

- Third-party security tools for automated threat mitigation such as: firewalls, identity management systems, cloud services, threat intelligence tools, and SOAR tools.
- Own or third-party incident response solutions.

Leadership

Selecting a vendor of a product or service must not be based only on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help to identify vendors that should be further evaluated. However, a thorough selection process should also include a subsequent detailed analysis and a proof of concept (PoC) or pilot phase, based on the specific criteria of the customer.

Based on our research, we have created various Leadership ratings. The Overall Leadership rating, shown in Figure 1, provides a combined view of the ratings for:

Product Leadership
Innovation Leadership
Market Leadership

Overall Leadership

Figure 1: The Overall Leaders in the I-SIEM market

Overall Leaders are (in alphabetical order):

- Exabeam
- Fortinet
- Gurucul
- IBM Security
- Logpoint
- NetWitness
- Securonix

Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of solution features and the overall capabilities of the various solutions. In the Product Leadership rating, we look for the functional strength and completeness of the vendors' solutions, regardless of their current ability to gain a substantial market share.

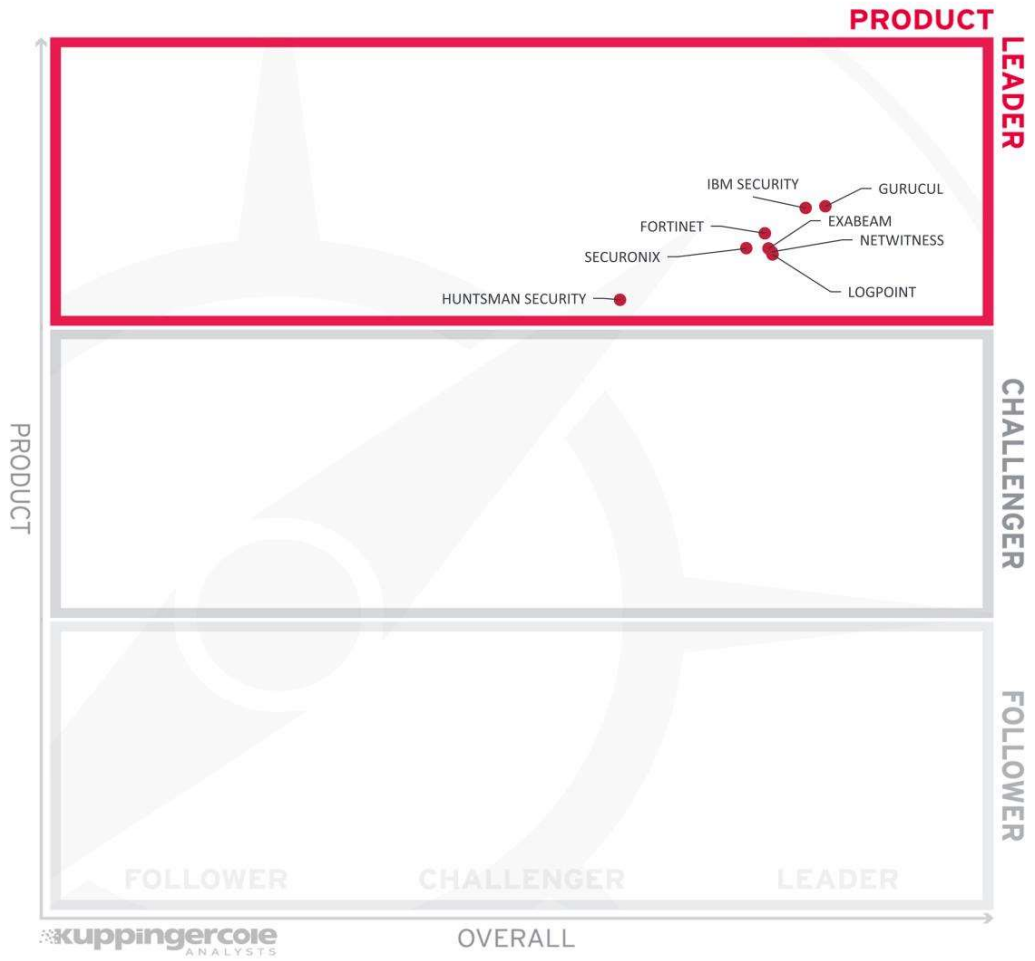


Figure 2: Product Leaders in the I-SIEM market

To be rated as I-SIEM leaders, vendors must meet most of the key capabilities defined in chapter 1. In this mature and competitive market, all the vendors that agreed to participate in this report are product leaders with comprehensive offerings.

Product Leaders (in alphabetical order):

- Exabeam
- Fortinet

- Gurucul
- Huntsman
- IBM Security
- Logpoint
- NetWitness
- Securonix

Innovation Leadership

Innovation from our perspective is a key capability in all IT market segments. Customers require innovation in order to meet evolving and emerging business requirements. Innovation is not about delivering a constant flow of new releases and upgrades. An innovative approach is about being able to provide customer-focused upgrades, as well as other cutting-edge features, while maintaining compatibility with previous versions.

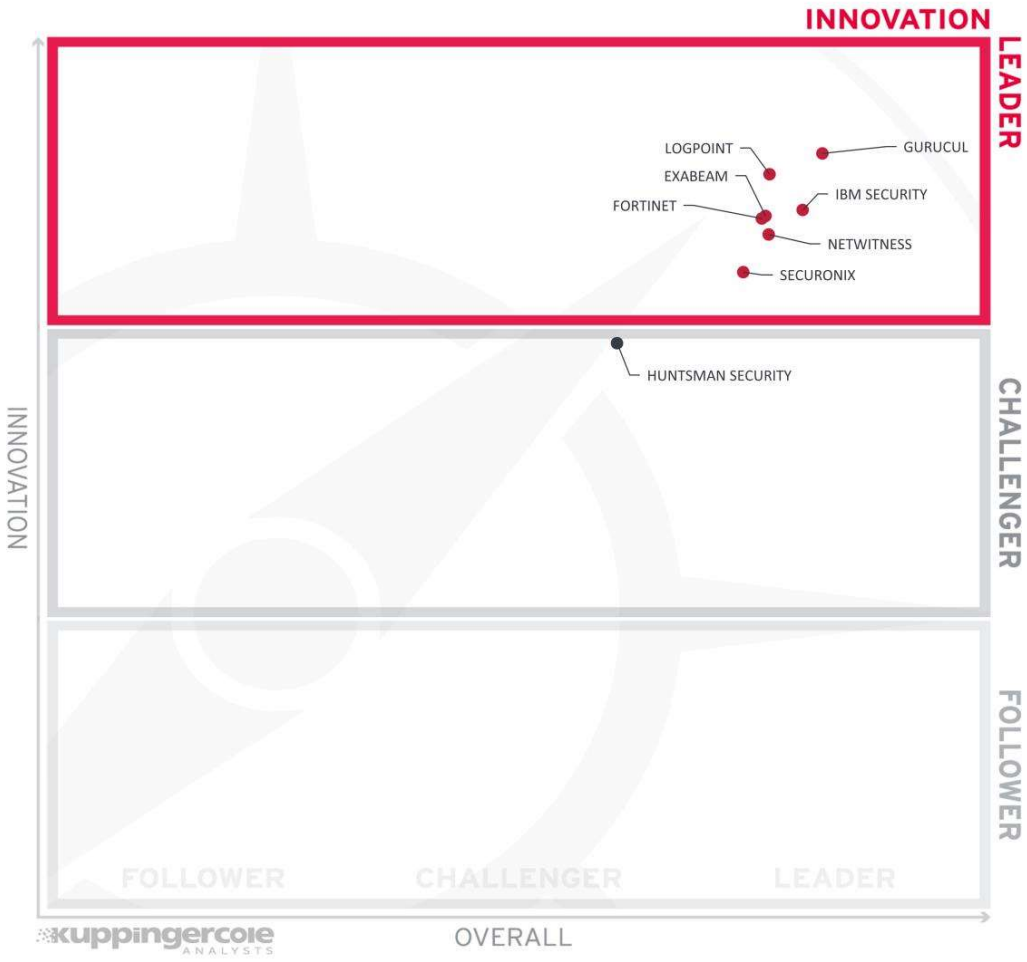


Figure 3: The Innovation Leaders in the I-SIEM market

The majority of vendors in this market are focusing on innovation to remain competitive. The main areas of innovation observed in the I-SIEM market include fully integrated unified platforms, improved search functionality including NLP methods, fast search, and fully federated search.

Planned innovation in the I-SIEM market will include further improvements to make search functionality faster and easier to use, greater use of assistants/chatbots based on generative AI, new automation and collaboration capabilities (typically supported by AI), support for operational technology (OT) and internet of things (IoT) environments, and new visualization capabilities.

Innovation Leaders (in alphabetical order):

- Exabeam
- Fortinet
- Gurucul
- IBM Security
- Logpoint
- NetWitness
- Securonix

Market Leadership

Lastly, we analyze Market Leadership. This is an amalgamation of the number of customers, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

Figure 4: The Market Leaders in the I-SIEM market

The I-SIEM market continues to grow and evolve in response to market demand as organizations face a growing number of cyberattacks and struggle to find and retain the cybersecurity professionals that they need to defend the rapidly increasing attack surface due to the adoption of cloud services and other emerging technologies. Market Leadership is determined by combining the scores for a wide variety of market-related factors.

The I-SIEM Market Leaders in alphabetical order are: Exabeam, Fortinet, Gurucul, IBM Security, Logpoint, NetWitness, and Securonix. Huntsman Security could move up into the leadership category by improving across all the determining factors, such as expanding the size and global distribution of their customer base.

Market Leaders (in alphabetical order):

- Exabeam
- Fortinet
- Gurucul

- IBM Security
- Logpoint
- NetWitness
- Securonix

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking for a product leader and for a vendor that delivers a solution that is both feature rich and continually improved. This would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix

Figure 5: The Market/Product Matrix for the I-SIEM market

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

All vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

Exabeam, Fortinet, Gurucul, IBM Security, Logpoint, NetWitness, and Securonix are (in alphabetical order) the Market Champions in the top right corner. This means that product strength correlates closely with market position.

Huntsman Security is in the center right square, indicating that it has a relatively strong I-SIEM solution in terms of features and functionality, which is not yet matched by the size and geographical spread of its customer base.

The Product/Innovation Matrix

This matrix illustrates the correlation between Product Leadership and Innovation Leadership. It is clear that technological innovation drives product success, which means there is typically a close relationship between innovation and product strength.

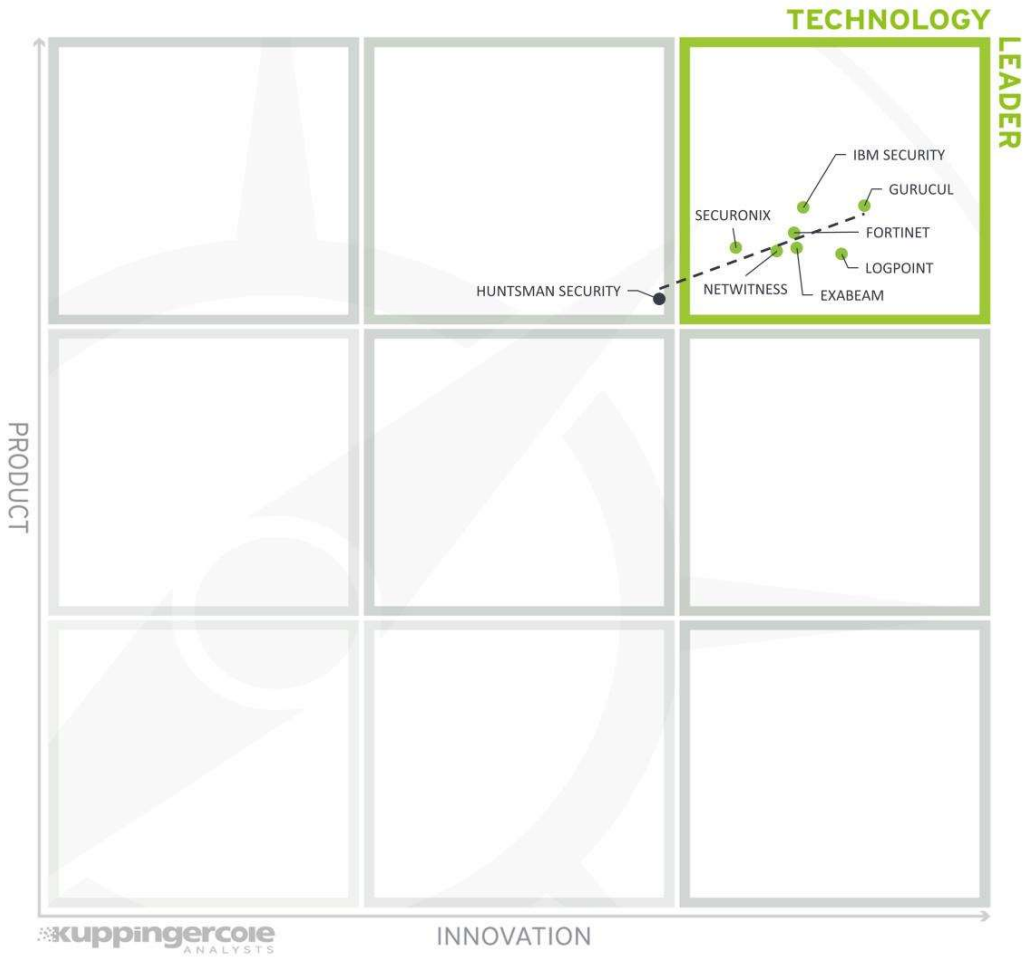


Figure 6: The Product/Innovation Matrix for the I-SIEM market

Vendors below the line are more innovative, while vendors above the line are, compared with the current Product Leadership positioning, less innovative.

The Technology Leaders in alphabetical order are Exabeam, Fortinet, Gurucul, IBM Security, Logpoint, NetWitness, and Securonix.

Huntsman Security is in the top center square and has the opportunity to become a leader by putting a greater focus on aligning innovation with overall strength.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

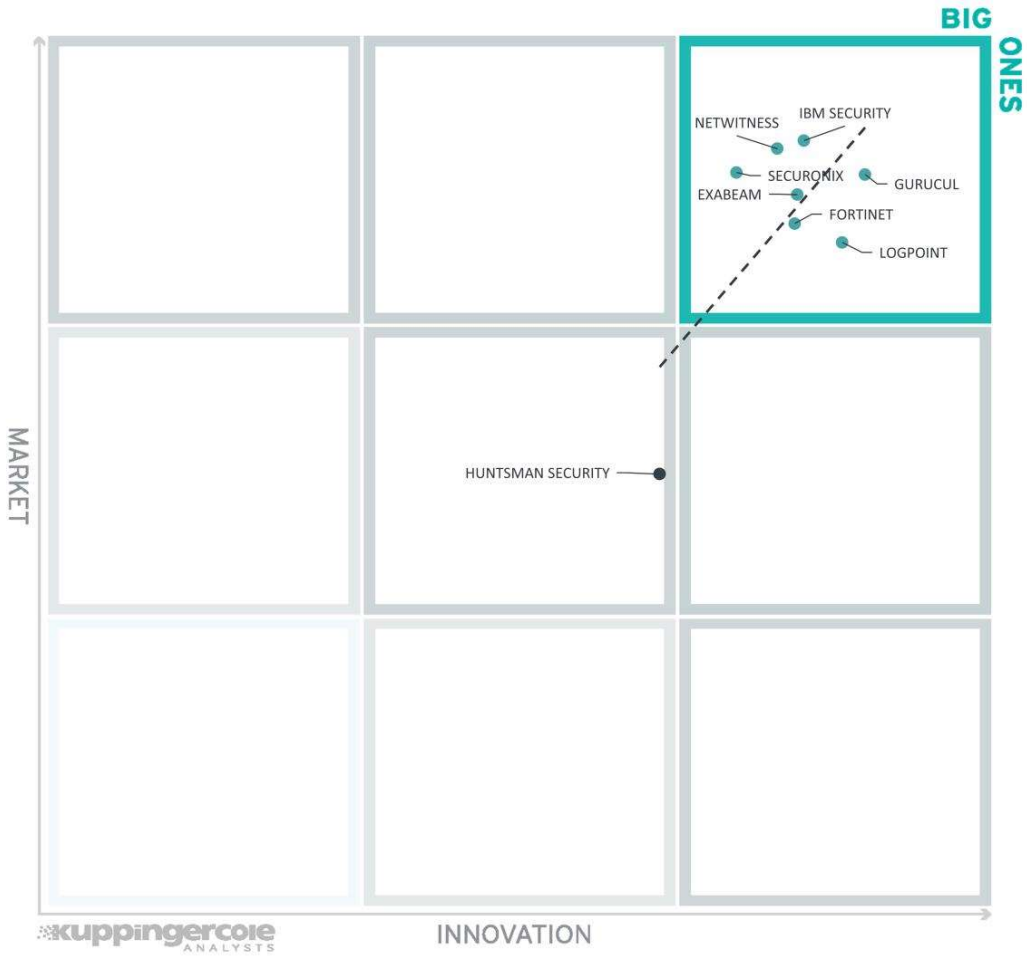


Figure 7: The Innovation/Market Matrix for the I-SIEM market

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate despite having less market share, and thus the biggest potential for improving their market position.

The Big Ones are Exabeam, Fortinet, Gurucul, IBM Security, Logpoint, NetWitness, and Securonix.

Huntsman Security is in the center square, which means it has the potential to drive market growth by increasing its efforts in terms of innovation.

Products and Vendors at a Glance

This section provides an overview of the various products analyzed within this KuppingerCole Leadership Compass on I-SIEM Platforms. As well as the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These help to identify highly innovative, but specialized vendors or local players that provide strong product features, but do not have a global presence and large customer base yet, for example.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
Exabeam	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Fortinet	Strong Positive	Strong Positive	Strong Positive	Neutral	Strong Positive
Gurucul	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Huntsman Security	Positive	Positive	Positive	Positive	Positive
IBM Security	Strong Positive	Positive	Positive	Strong Positive	Strong Positive
Logpoint	Positive	Strong Positive	Positive	Positive	Strong Positive
NetWitness	Strong Positive	Strong Positive	Positive	Positive	Positive
Securonix	Strong Positive	Strong Positive	Positive	Positive	Strong Positive

Table 1: Comparative overview of the ratings for the product capabilities

Table 2 contains four additional ratings for each vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor as a whole, the other ratings apply to the product under review.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Exabeam	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Fortinet	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Gurucul	Strong Positive	Positive	Strong Positive	Strong Positive
Huntsman Security	Neutral	Neutral	Neutral	Neutral
IBM Security	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Logpoint	Strong Positive	Strong Positive	Strong Positive	Positive
NetWitness	Positive	Strong Positive	Strong Positive	Strong Positive
Securonix	Positive	Strong Positive	Strong Positive	Strong Positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC I-SIEM, we look at the following eight categories:

Data Collection – The collection and efficient storage of security events from various sources is the original and primary goal of SIEM solutions. This includes parsing system, application, service, or device logs in various formats; capturing and analyzing network traffic information; collecting security data directly from endpoints using agent-based or agentless methods; as well as integrating with cloud services and other third-party sources.
Correlation and Enrichment – This involves identifying relationships between data from various sources in real time using statistical algorithms and machine learning methods, adding business context information collected from other enterprise IT systems, and incorporating threat intelligence from external feeds.
Threat Detection – This evaluates the ability to detect patterns and anomalies in security data beyond the traditional rule-based approach. We expect modern I-SIEM solutions to be able to remove the statistical noise and reduce false positives without human intervention, by

relying on techniques like behavior analysis and/or machine learning. Identifying security incidents across multiple events and assigning risk scores according to threat models and other methods of improving analyst productivity will lead to higher ratings.

Forensic Investigation – This refers to the provision of on-demand access to all source and contextual security information relevant for an incident or proactive threat hunting; the ability to pivot to related events or entities; and automated forensic analysis supported with workflows, policies, and risk models tailored to specific industries or markets.

Incident Response – This evaluates built-in or closely integrated capabilities to initiate and orchestrate incident response processes. Even though we cover specialized SOAR solutions in a separate Leadership Compass, platforms that include these capabilities directly or through partnerships with third-party vendors get more favorable ratings.

Intelligence and Automation - The primary advantage of next-generation I-SIEM platforms over traditional rule-based solutions is their ability to address analyst fatigue and the skills shortage through the high degree of intelligent automation. They should not require a team of trained security experts to operate, relying instead on actionable alerts and automated workflows, and ideally providing a complete end-to-end solution for a security operations center.

Compliance - Addressing regulatory compliance requirements is one of the primary use cases for modern SIEM solutions. Long-term security data retention, normalization, and correlation across multiple IT systems, and rich visualization and reporting capabilities, make SIEMs ideal tools for compliance audit and reporting. Solutions that provide out-of-the-box support for major regulatory frameworks and are themselves certified to comply with security standards will receive high ratings here.

Cloud Support – This evaluates the degree to which solutions support the collection of logs from cloud services and applications, including shadow IT. It also looks at the number of out-of-the-box integrations and connectors that are provided for cloud services and applications. Most organizations are migrating to cloud services. It is therefore important that next-gen I-SIEMs provide good support for cloud computing.

Exabeam – Exabeam Fusion

Exabeam is a private cybersecurity company founded in 2013 and headquartered in the US in Foster City, California, with another US office in Plano, Texas, and offices in Mexico, Colombia, Ireland, UK, Dubai, Australia, Singapore, Japan, and India.

Exabeam has a global partner network and supports companies of all sizes around the world, with most customers in the mid-market segment and located in North America, followed by the EMEA and APAC regions, and Latin America.

The company has evolved quickly from its beginnings as a UEBA add-on to existing SIEMs into a full-scale and highly modular general-purpose security operations platform, which can either replace an existing SIEM deployment or allow customers to mix and match individual modules with other third-party SIEM or SOAR products.

Exabeam Fusion is the latest incarnation of the company's unified security operations platform, which is deployed primarily as a cloud-native service. However, there is still an on-premises solution for those customers that require that.

Exabeam Fusion combines four sets of capabilities in a single architecture that is flexible and modular to support diverse use cases The Exabeam Security Operations Platform offers five package options: Exabeam Security Log Management, Exabeam SIEM, Exabeam Security Analytics, Exabeam Security Investigation, and Exabeam Fusion for customers who want all features available. Exabeam has a simple licensing model based on the amount of data ingested. The cost of each gigabyte depends on the package or combination of packages chosen by customers.

The solution supports a comprehensive range of log sources, including OT, IoT, and mobile devices. It is also able to configure custom log formats and develop custom connectors for log collection. Exabeam supports various formats for the same log ingestion type, such as JSON and JSON Array. Custom connectors allow integration with different products via generic transport such as AWS S3, Azure Storage, and Apache Kafka queues. However, there are technical limitations on the number and size of logs collected, and the solution does not natively support capturing and analyzing network traffic. Exabeam uses partners for this. The solution supports virtualized network infrastructures and OSI layer 7 traffic analysis, but cannot capture network traffic on a gateway, does not support passive mode (SPAN/TAP), and does not support some common protocols and services. The solution supports collecting data directly from endpoints using APIs and agents, which will run on cloud infrastructure, Linux, and Windows. Agentless collection is supported.

The Exabeam platform correlates real-time and historical security data from different sources, and it collects, enriches, and analyzes data from all sources. There are more than 1,700 pre-packaged correlation rules and a wizard tool for creating custom correlation rules. There is also support for external threat intelligence feeds. There is no built-in support for STIX/TAXII, but Exabeam supports custom integrations with threat intelligence providers by providing an API to create any custom context. Exabeam also provides its own threat intelligence sources. The solution supports enriching security data with location, identity, and

business context information, with a large library of behavioral rules that take business context into consideration. The solution is able to identify multiple events from different times and sources as parts of a single incident by ingesting events from a variety of different sources using its unified ingestion pipeline with more than 9,500 parsers. It then combines all events into “Smart Timelines” that show alerts, anomalies, and events in chronological order. The ML-based detection engine assigns a risk score and automatically creates an incident when a certain threshold is reached.

The solution is able to establish behavioral baselines, and it can detect anomalies and outliers in the security data, which includes comparing normal profiles with current and historical events. The solution provides relative risk scores for each threat/incident, and it comes with more than 2,500 rules and models that trigger ML-based risk scoring. It also includes functionality to identify ransomware behaviors. The solution provides risk models for various industries, specifically healthcare, critical infrastructure, aviation, and finance. It also allows for customization of these models. The solution provides some OOTB integrations for third-party behavior analytics products, including Dtex Systems, Gurucul, IBM QRadar UBA, ObserveIT, Rapid7 InsightIDR, Splunk UBA, Varonis, Microsoft, LogRhythm, ManageEngine, and CyberArk.

The solution is able to prioritize alerts based on risk scores, it can prioritize groups of related alerts based on combined risk scores, and it can correlate alerts for each user account or entity to calculate a risk score. The solution also provides automatic triage and prioritization of alerts, automatic remediation of common threats, and automatic recommendations based on historic data. Availability of natural language searches of collected data is scheduled for Q1 2024, following customer testing via Exabeam Early Access. The solution enables users to pivot to related events, entities, or users to better understand the relationships between them and to estimate the impact. Exabeam Smart Timelines automatically reconstruct the events underlying security incidents to avoid analysts having to look through raw logs.

In terms of incident response, Exabeam Fusion provides a centralized interface for collaborating across all organizational units and full lifecycle management for the creation, tracking, and management of incidents, which contain a full audit history. The solution supports incident simulation for testing and improving existing workflows, and it includes direct remediation capabilities with OOTB actions with different native and third-party services to perform remediation, including EDRs, firewalls, SIEMs, CASBs, and email security products. However, there is no support for visualization of network flows. Exabeam provides integrations with SDN/SDCI solutions, and it provides functionality to discover shadow IT and collects logs from shadow IT directly. There is also functionality to map SIEM alerts and response actions to the ATT&CK framework, and to help customers prioritize the ATT&CK techniques they believe are the most relevant to the organization. Exabeam is working on a heatmap for a visual representation of customers’ coverage of ATT&CK TTPs and what they can do to improve coverage. Exabeam also provides a prescriptive data visualization focused on use case outcomes, that helps users map their data and parsing configurations to improve use case and threat coverage.

Exabeam Fusion includes automation capabilities for various parts of incident response workflows. Exabeam TDIR use case packages provide prescriptive workflows and pre-

packaged content to enable customers to automate detection, investigation, and response. It is also possible to automate actions that involve third-party products. The solution includes a visual designer for automation of workflows/playbooks by integrating native and third-party services. The solution offers a catalog of pre-built playbooks for common scenarios for malware, phishing, and reputation lookup, as well as a catalog of actions or other building blocks for playbooks. Playbooks/workflows support conditional logic as well as manual approvals. The solution uses both supervised and unsupervised ML detection models, but it does not use DL algorithms to preserve transparency in all UEBA detections. Exabeam maintains DL is a black box approach that lacks transparency, which is key to core UEBA work in detections. ML is used for a wide range of purposes, including prioritizing alerts based on historic response actions by analysts. Exabeam provides support in tuning inputs for ML algorithms, and it enables predictive analytics to anticipate and prevent future cyberattacks.

Exabeam Fusion supports compliance with SOC 2 type 2 and ISO 27001. The company is pursuing attestations of support for PCI-DSS, US FedRAMP, HITRUST, and ISMAP. The solution itself is compliant with ISO 27001, ISO 27017, ISO 27018, and AICPA's SSAE 18 SOC 2 Type 2. It also has IRAP (Infosec Registered Assessors Program) attestation in Australia. The solution supports a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, incident responders, compliance managers, and developers. Access to specific incidents can be restricted to specific individuals, specific roles, and geographic locations. The solution supports automatic compliance reporting against standards and offers pre-built compliance reports for on-premises customers. The solution enables customers to keep data entirely on premises and offers guaranteed data/metadata residency for the EU, US, Japan, Singapore, and Australia, and is expanding into the Middle East.

The solution is built on cloud-native architecture, supports multi-cloud deployments, and covers logs from cloud services and applications. Cloud infrastructure is supported by agents, and connectors are provided for a wide range of services under Microsoft Azure, GCP, and AWS. It also provides integrations for a fairly wide range of cloud-based business applications, and provides functionality to connect to a CASB to collect logs from cloud-based shadow IT.

Exabeam Fusion is suitable for end user organizations of all sizes and all verticals, particularly highly regulated industry sectors such as finance, healthcare, government, and manufacturing. Direct customers range from the world's largest companies and governments to companies with as few as 30 employees. Smaller companies are serviced by MSSP partners.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 3: Exabeam's rating

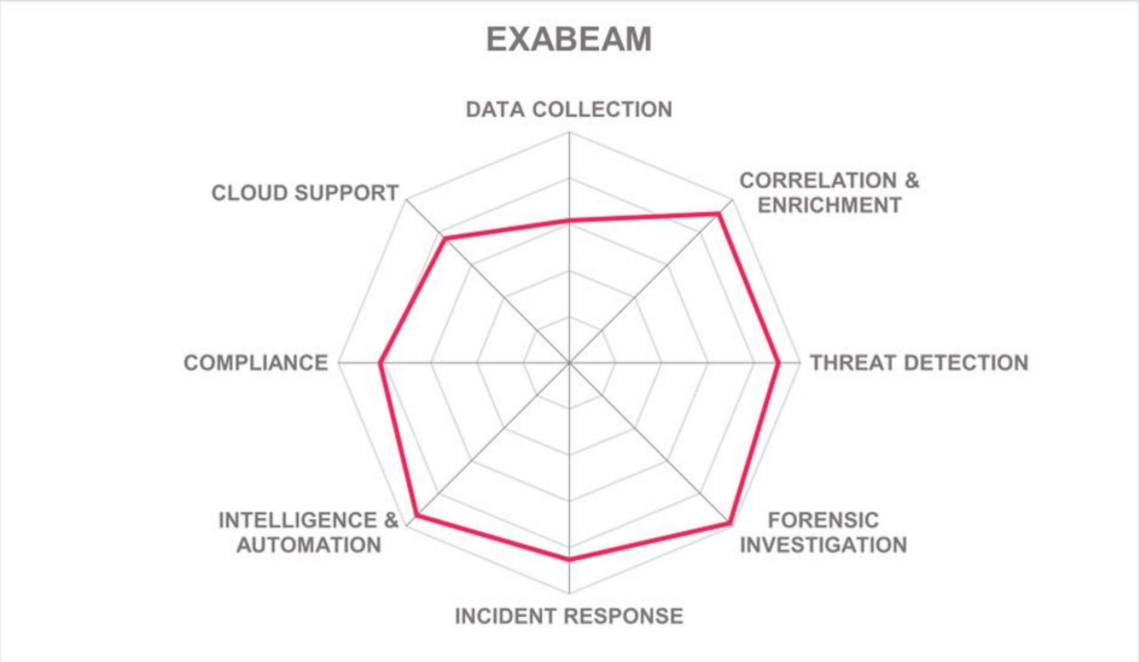
Strengths

- Simple package-based licensing model focused on outcomes.
- Employs ML detection models, especially for UEBA.
- Persona-based approach for greater relevance of information.
- Different views for different roles such as SOC analyst and engineer.
- Fast search capability for both hot and cold data.
- Good, intuitive user interface.
- Strong behavior analytics capabilities.
- Automatic enrichment of incoming log data with threat intelligence information.
- Smart Timelines display the full scope of a user's or device's activity in a graphical manner, identifying anomalous behavior and risk.
- The platform supports incident simulation for testing and improving existing workflows.

Challenges

- No native support for capturing and analyzing network traffic or capturing network traffic on a gateway. This is enabled through partner integrations.
- Currently no special pricing model for MSSPs, but this is on the roadmap.
- As a behavior analytics specialist, support for third-party UEBA products is relatively limited.
- No visualization of ATT&CK information, but heatmap is on the roadmap.
- No guarantee of data/metadata residency for UAE, but this is under development.
- Exabeam does not offer the services of an expert team for assisting in incident analysis and/or remediation.
- Support services available only in English.

Leader in


EXABEAM
DATA COLLECTION
CORRELATION & ENRICHMENT
THREAT DETECTION
FORENSIC INVESTIGATION
INCIDENT RESPONSE
INTELLIGENCE & AUTOMATION
COMPLIANCE
CLOUD SUPPORT

Fortinet – FortiSIEM

Fortinet is a public, US-based cybersecurity company founded in 2000 and headquartered in Sunnyvale, California. The company provides a wide range of network security and threat protection solutions for carriers, datacenters, enterprises, and distributed offices. Its solutions are integrated into the Fortinet Security Fabric, including enterprise security products for secure networking, cloud security, OT security, and security operations (SecOps). The Fortinet SecOps portfolio includes SIEM, SOAR, EASM, NDR, EDR, and XDR capabilities.

Fortinet's sweet spot is the mid-market and large enterprises in North America and the EMEA region, with most R&D based in North America. The company has a large global network of partners, system integrators, service providers, cloud providers, and distributors.

FortiSIEM can be deployed on-premises (including as an appliance), as a cloud service (SaaS), or in a hybrid model. There are three main licensing models for MSSPs, on-premises deployments, and cloud deployments. The MSSP model is based on the number of devices being monitored, the number of agents deployed, and the number of users. The on-premises model is based on the number of devices and the number of agents, and it includes an EPS (events per second) allowance for each device. There is a charge for additional EPS. There are also additional charges for appliances, UEBA, threat intelligence, and support services. Cloud licensing is based on storage, archive storage, and FortiSIEM Compute Units (FCUs), where 10 FCUs typically equate to an ingestion rate of 1,000 EPS.

The solution supports a wide range of log sources, including OT and IoT, but not mobile devices. It is possible to configure custom log formats and develop custom connectors for log collection. FortiSIEM has an open parsing framework to allow customers to create their own parsers and a no-code API GUI integration framework for integrating with API endpoints. There is no technical limitation on the number or size of collected logs, and while the solution supports analyzing network traffic, this traffic cannot be captured directly. It relies on PCAP information from a firewall. It also does not support passive mode (SPAN/TAP) or OSI layer 7 traffic analysis directly, but it can do so via FortiNDR. The solution supports only around half of common protocols and services, relying on FortiNDR for protocol or NDR capabilities. It does, however, support collecting data directly from endpoints using APIs and agents, which will run on Bastion, containers, Linux, Unix, and Windows. Agentless log collection is supported using RPC, SSH, syslog, NetFlow, IPFIX, SNMP, Traps, REST APIs, and vendor specific APIs.

FortiSIEM correlates real-time and historical security data from different sources, and collects and analyzes data from all sources, including on-premises and cloud. The solution integrates with FortiGuard Threat Intelligence and supports external threat intelligence feeds. It also provides relative risk scores for each threat/incident and supports the STIX/TAXII and CSV threat intelligence standards. However, FortiSIEM provides a Python-based framework to allow customers to customize their threat feed integrations. For security data enrichment, the solution is able to use information from IAM/IGA systems, from FortiSIEM UEBA, and business context information. The solution is able to identify multiple events from different sources and times as part of a single security incident.

Threat detection is supported by the solution's ability to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The solution provides relative risk scores on a per entity basis for each threat/incident and includes specific rules to detect ransomware behaviors and rules that incorporate SIGMA detections that can identify ransomware. The solution provides risk models for various industry use cases that can be customized. However, FortiSIEM provides no OOTB integrations for third-party behavior analytics products, relying on its native UEBA capabilities.

The solution can correlate alerts for each user account or entity to calculate a risk score. However, the solution cannot prioritize alerts based on risk scores or prioritize groups of related alerts based on combined risk scores. The solution provides automatic triage of alerts and automatic remediation of common threats, but it does not provide automatic recommendations based on historic data. However, the solution enables users to pivot to related events, entities, or users to better understand the relationship between them and to estimate the impact. While it does not support natural language searches of collected data via the search interface, Fortinet Advisor (introduced in FortiSIEM version 7.1.0) is able to retrieve the current health of FortiSIEM nodes, get the list of the latest vulnerabilities in a customer environment, answer questions based on product documentation and knowledge base articles, get analysis and recommendations for logs and incidents, and help in building a FortiSIEM report.

The solution provides good incident response capabilities, including a centralized interface for collaborating across all organizational units, and full lifecycle management for the creation, tracking, and management of incidents. The solution supports incident simulation for testing and improving existing workflows, and the visualization of network flows. It also includes direct remediation capabilities. Fortinet currently has no plans for integration with SDN/SDCI solutions due to a lack of customer demand. The solution provides functionality to discover shadow IT and collect logs from shadow IT directly. Alerts are mapped to the ATT&CK framework, and the solution enables users to prioritize ATT&CK techniques they believe are the most relevant to the organization.

FortiSIEM offers basic automation for various parts of incident response workflows, including actions involving third-party products, but for more sophisticated automation and enrichment capabilities, it requires Fortinet's FortiSOAR product. FortiSIEM also relies on FortiSOAR to provide a visual designer for the automation of workflows/playbooks and a catalog of pre-built playbooks for common scenarios. However, FortiSIEM does offer a catalog of more than 30 actions or building blocks for playbooks, with the ability to add more using a Python-based framework. Workflows/playbooks support conditional logic and manual approvals. The solution uses supervised and unsupervised ML detection models, but it does not use DL algorithms. ML is used for a wide range of purposes, including prioritization of alerts based on historic response actions by analysts. Fortinet provides support in tuning inputs for ML algorithms, and the solution includes ML-based data analytics, but this does not enable predictive analytics to prevent future attacks on IT systems.

FortiSIEM is not independently certified to support compliance with any of the major security standards, but the product itself has achieved ISO/IEC 27001 compliance, and FortiSIEM

Cloud is SOC2 Type 2 certified against an expanded control set, including control alignment against the HIPAA Security Rule. The solution supports a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, and incident responders, as well as providing support for multiple groups, with the ability to restrict access on a need-to-know basis to enable segregations based on departments and geographic locations. FortiSIEM supports automatic compliance reporting against regulatory standards customer organizations need to meet, it allows customers to keep their data entirely on-premises, and it offers guaranteed data residency for the EU, US, Canada, UK, and Australia, but not the UAE.

In terms of cloud support, the solution is built on cloud-native architecture, supports multi-cloud deployments, supports logs from cloud services and applications, includes agents for cloud infrastructure, and provides connectors for a range of services under Microsoft Azure, GCP, and AWS. FortiSIEM can connect to a CASB to collect logs from cloud-based shadow IT, but it has a limited number of OOTB integrations with cloud service/business applications. Only by leveraging FortiSOAR can FortiSIEM integrate with more than 500 different applications.

FortiSIEM provides a comprehensive platform for parsing of logs, storage, reporting, UEBA, security analytics, infrastructure discovery, threat detection, and automated response, that can run alone or in conjunction with other Fortinet products. The solution is particularly well suited to MSSPs and end user organizations that have mature SOC teams and are already invested in other components of the Fortinet security fabric, especially FortiSOAR.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Neutral
Usability	Strong Positive

Table 4: Fortinet's rating

Strengths

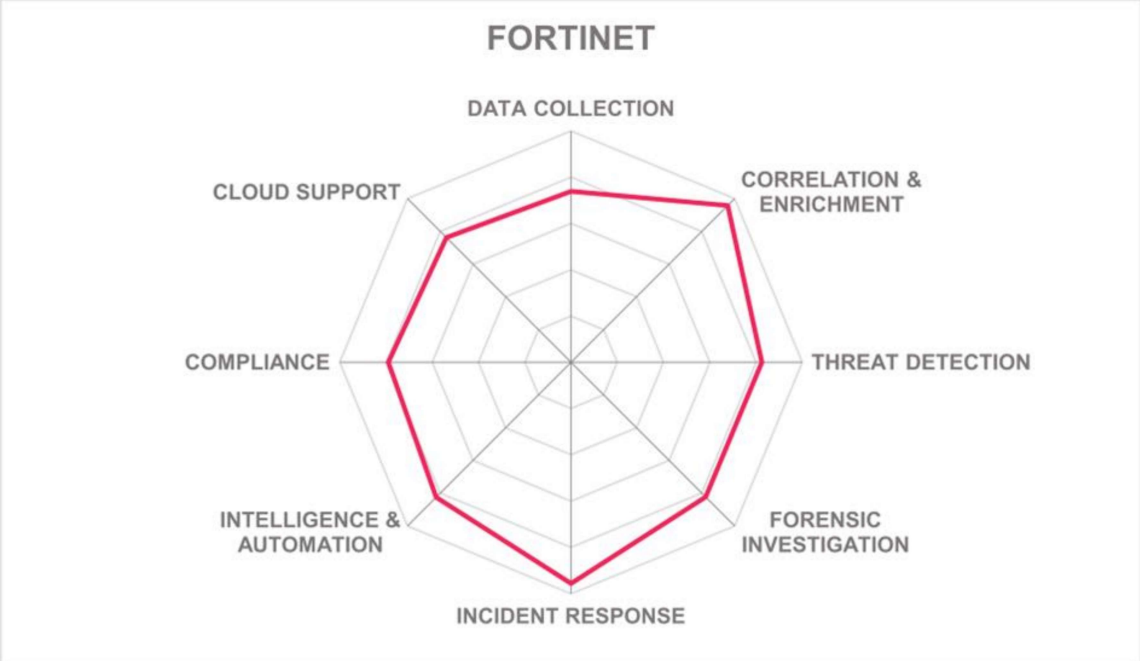
- Flexible deployment modes.
- Flexible and simple licensing models, with a special model for MSSPs.
- Centralized management across different geographies and deployment types.
- Pre-integrated part of Fortinet's wide security fabric portfolio.
- Built-in configuration management database (CMDB) capability that is shared across different device types.
- Supports SOC for IT and OT.
- Wide range of technology partners for OT.
- Worldwide SaaS distribution supported by AWS.
- Functionality to show performance and availability information.

- Can do file integrity monitoring and registry monitoring.
- Functionality to compare configurations side by side and highlight differences.
- Rule engine works in real time, which means rules are constantly active.
- Dynamic device information, including performance and applications running.
- Support services available in seven languages.
- The platform supports incident simulation for testing and improving existing workflows.

Challenges

- Only basic response actions within FortiSIEM without subscription to FortiSOAR.
- Limited integrations with cloud services and business applications without FortiSOAR.
- Relatively fewer OOTB integrations with DLP and NDR solutions.
- No current or planned integrations with SDN/SDCI solutions.
- No single screen to access all aspects of investigations, but this is on the roadmap.
- Does not yet support logs from mobile devices.
- Documentation available only in English.

Leader in



Gurucul – Gurucul Next Generation SIEM

Gurucul is a private American cybersecurity company founded in 2010 and headquartered in Los Angeles, California, with a strong focus on user and entity behavior analytics (UEBA) and security analytics. The company has research and development labs in the US and India, and sales offices around the globe, primarily in the US, APAC, and EMEA, supplemented by a strong channel of distributors and partners.

Gurucul has customers of all sizes, particularly mid-market sized organizations, followed by enterprise, medium, and small business, predominantly in North America, followed by EMEA, APAC, and Latin America.

Gurucul's Next Generation SIEM is available as on-premises software, software on physical and virtual appliances, as a cloud service, and as a managed service, supporting hybrid-cloud and multi-cloud environments, with flexible and simple pricing models based on the number of managed assets and/or users, depending on the chosen solution package. MSSP licensing is tailored to their specific business model.

The platform supports a comprehensive range of log sources, including OT, IoT, mobile devices, IAM, PAM, IGA, CMDB, Active Directory, and DLP. It allows customers to configure custom log formats and develop custom connectors for log collection through the UI. Data ingestion pipelines support modifying any existing pipeline and building new ingestion pipelines for new or custom data sources. There is no technical limitation to the number and size of logs collected. The platform can capture network traffic on a gateway, it supports passive mode (SPAN/TAP), it supports virtualized network infrastructure, and it supports OSI layer 7 traffic analysis. The platform supports all common protocols and services, including legacy protocols. It supports collecting data directly from endpoints using APIs and agents, with all operating systems supported by agents. Agentless data collection is also supported.

Gurucul's Next Generation SIEM platform correlates real-time and historical security data from different sources, and collects and analyzes data from all sources, including on-premises and cloud. It can correlate security data from any data source and comes with integrations for the most common security solutions. The platform also comes with pre-defined correlation rules, and it provides a wizard-based UI (Gurucul STUDIO) that allows users to build custom rules, ML models, and workflows. The platform comes with its own threat intelligence sources as well as supporting external intelligence feeds and a wide range of threat intelligence standards, including STIX/TAXII, YARA, SIGMA, Open TPX, MAEC, IODEG, VERIS, IDMEF, and X-ARF. The platform supports enriching security data with identity information and contextual business information, including data gathered by Gurucul's ML-supported UEBA. The platform is also able to identify multiple events from different sources and times, and link them to a single security incident. Gurucul's model chaining, with the ability to analyze the chain (often called link chain analysis) helps eliminate ambiguity in determining a threat through automated alert cross-validation.

Gurucul has a mature UEBA capability. The platform is able to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The platform provides relative risk scores for each

threat/incident using a risk intelligence engine. It also includes functionality to identify ransomware behaviors. The platform provides customizable risk models for various industry use cases, with a library of more than 2,500 pre-packaged ML models that are tuned to predict and detect threats aligned with specific use cases and vertical industries. Gurucul also offers industry specific pre-packaged analytics. The platform provides no OOTB integrations for third-party behavior analytics products, but can communicate with them via a syslog pipeline.

The platform prioritizes alerts based on normalized risk scores. It can prioritize groups of related alerts based on combined risk scores, and it can correlate alerts for each user or entity to calculate a risk score. The platform also provides automatic triage of alerts, remediation of common threats, and recommendations based on historic data. The platform offers natural language search via the AI Assistant functionality, but it is not available directly in the search interface. The platform enables users to pivot to related events, entities, or users to better understand the relationship between them and to estimate the impact. Gurucul's link chain analysis provides this set of relationships between events, users, and entities with additional context.

The platform provides good incident response capabilities, including a centralized interface for collaborating across organizational units, and full lifecycle management for the creation, tracking, and management of incidents. It supports collection, processing, and analysis of data locally, but once the data is processed, alerts/case metadata can be shared with the centralized environment. The platform supports incident simulation for testing and improving existing workflows, direct remediation capabilities, and visualization of network flows. It also has integrations with SDN/SDCI solutions. The platform includes functionality to discover shadow IT and collect logs from shadow IT directly. Alerts are mapped to the ATT&CK framework, and the platform enables users to prioritize the ATT&CK techniques they believe are the most relevant to the organization.

The platform offers automation for various parts of incident response workflows. It comes with an automated incident response and case management feature that is integrated with threat intelligence. The platform also supports the automation of actions that involve third-party products. A visual designer for automation workflows and playbooks is included. Gurucul STUDIO provides a step-by-step graphical interface to select attributes, train models, create baselines, set prediction thresholds, define feedback loops, and build automated workflows. The platform offers a catalog of more than 500 pre-built playbooks for common scenarios to trigger actions on external systems such as DLP, EDR, and firewalls, and provides a catalog of actions or other building blocks for playbooks. Workflows/playbooks support conditional logic and manual approvals. The platform uses supervised and unsupervised ML detection models, and also uses DL algorithms. ML is used for a very wide range of purposes, including prioritization of alerts based on historic responses by analysts. Gurucul provides support in tuning inputs for ML/DL algorithms, and the platform provides ML-based analytics, including predictive analytics.

The platform supports compliance reporting with most major security regulations and frameworks, but not the US FedRAMP. The platform itself, however, is not yet compliant with ISO27001, but is working towards certification. It is also not compliant with ICPA's SSAE 18

SOC 2 Type 2 requirements but is working towards SOC2 Type 1 certification. The platform supports a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, and incident responders, as well as providing support for multiple groups, with the ability to restrict access on a need-to-know basis to enable segregations based on departments and geographic locations. The platform supports automatic compliance reporting against standards customer organizations need to meet. It is possible for customers to keep their data entirely on premises, and the platform offers guaranteed data/metadata residency for the EU, US, India, and UAE. Gurucul supports distributed deployment architecture. This ensures localized data collection, processing, and compression for regulatory compliance and reducing the network upstream bandwidth requirements.

The platform is built on cloud-native architecture, supports multi-cloud deployments, and covers logs from cloud services and applications. Cloud infrastructure is supported by agents, and connectors are provided for a wide range of services under Microsoft Azure, GCP, and AWS. Gurucul has built direct bi-directional integrations with the full suite of Microsoft business applications, GCP Workspace and related products, and AWS application, security, and cloud capabilities. It also provides integrations for a very wide range of other cloud-based business applications, and can connect to a CASB to collect logs from cloud-based shadow IT.

Gurucul Next Generation SIEM caters for organizations of all sizes, especially those looking for strong UEBA and security analytics capabilities in regulated and high security sectors such as financial services, healthcare, government, pharmaceuticals, energy, and education, with strong support for compliance and compliance reporting.

Security	Strong Positive	GURUCUL
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 5: Gurucul's rating

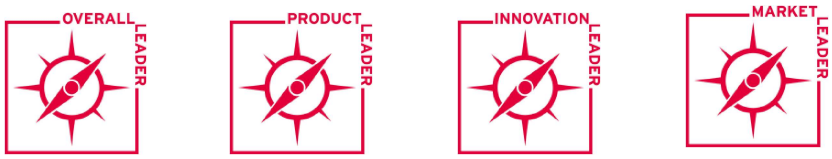
Strengths

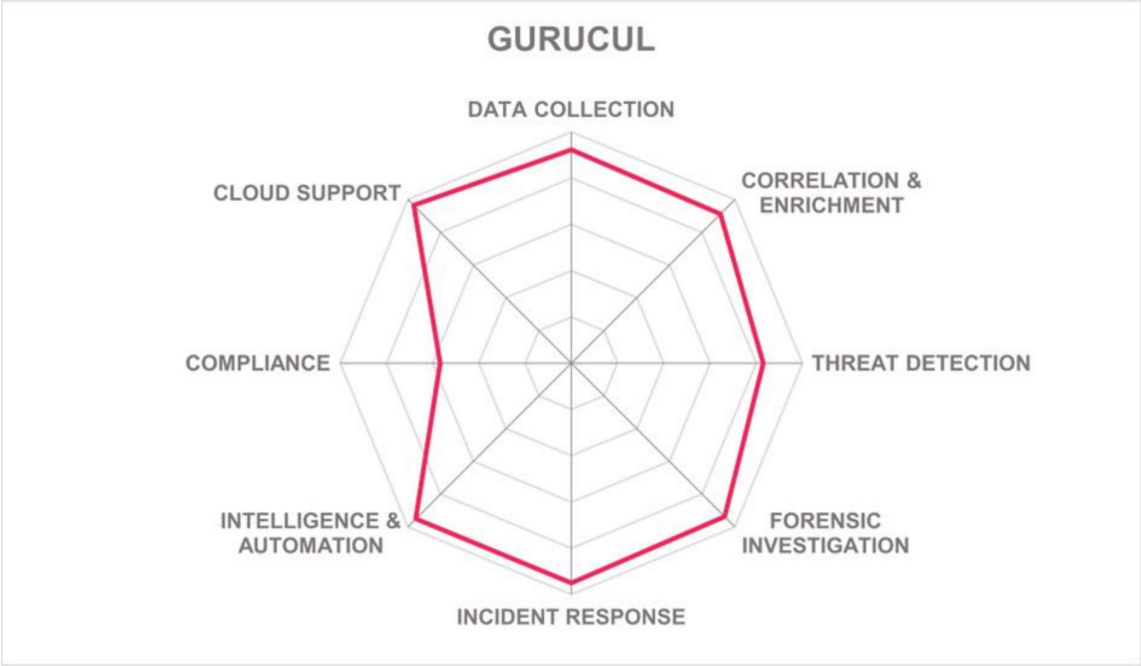
- A wide range of deployment options.
- Simple and flexible pricing models, with special licensing for MSSPs.
- Strong and mature UEBA and security analytics capabilities supported by ML/DL.
- Rapid and unlimited data collection, including cloud, identity systems, and IoT devices.
- Context-driven threat hunting and attack investigation.
- Dynamic and precise response with dynamically generated playbooks.
- Good support for hybrid-cloud, multi-cloud, and geographically distributed environments.
- Automated data parsing.
- Federated search across distributed architectures and a wide range of storage models.
- Attack chain identification capability across wide range of security telemetry.
- Very granular role-based access and privacy controls.
- Good incident response capabilities.
- Strong support for regulatory compliance and reporting.
- The platform supports incident simulation for testing and improving existing workflows.

Challenges

- Natural language search is not available in the search interface, only via AI Assistant.
- No OOTB integrations for third-party behavior analytics products, relies instead on a syslog pipeline.
- Still working towards some key security certifications.
- Support services available only in English, Spanish, and Mandarin.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


GURUCUL
DATA COLLECTION
CORRELATION & ENRICHMENT
THREAT DETECTION
FORENSIC INVESTIGATION
INCIDENT RESPONSE
INTELLIGENCE & AUTOMATION
COMPLIANCE
CLOUD SUPPORT

Huntsman Security – Huntsman Enterprise SIEM

Huntsman Security is a privately owned cyber security software company based in Sydney, Australia. Founded in 1999, the company has additional offices in Canberra, Australia; London, UK; and Tokyo, Japan.

Huntsman Security focuses on SIEM with security analytics and SOAR, and cyber risk measurement. The company's customer base includes government agencies and other public sector companies, as well as critical infrastructure providers, telcos, system integrators (Sis), and MSSPs.

Huntsman Enterprise SIEM is a cybersecurity analytics application designed to provide cyber threat detection, incident management, and actionable reporting. It combines the capabilities of a SIEM with behavioral and security analytics in a single platform with true multitenant architecture, making it suitable for use by MSSPs.

Licensing is mainly based on storage requirements rather than EPS, but Huntsman offers great flexibility and will tailor licensing to customer requirements, particular MSSPs, where additional flexibility is available to suit individual MSSP business models. Huntsman also offers flexible deployment options, including on-premises, in the cloud, hybrid, and as a managed service via partners. The solution is not available in a SaaS model because it is designed to operate in government and defense environments that are not typically connected to the internet.

The solution supports all log sources, including OT, IoT devices, mobile devices, cloud storage, and SaaS applications. It allows customers to configure custom log formats and develop custom connectors for log collection, providing support if necessary. There are no technical limitations on the number or size of collected logs because the solution is software based and can be installed on any platform. The solution supports capturing and analyzing network traffic using a module installed on endpoints and servers, including virtualized network infrastructure. It also supports capturing traffic on a gateway and passive mode (SPAN/TAP), but it does not support OSI layer 7 traffic analysis. The solution supports many of the most common protocols and services OOTB. It supports collecting data directly from endpoints using APIs and agents, which will run on most operating systems and platforms, excluding AIX, Android, Bastion, and mainframes. Huntsman uses agentless collection for AIX and mainframes. Agentless collection is supported using syslog, TCP/IP, UDP, HTTP, HTTPS, SNMP, SDEE, FTP, FTPS, SFTP, SMB1/2/3, and Cisco pxGrid.

Huntsman Enterprise SIEM supports correlating real-time and historical security data from different sources, and collects and analyzes data from all sources, including cloud and on-premises. Huntsman does not provide a source of threat intelligence, but open-source threat intelligence is available OOTB. In addition to external feeds, internal customer-centric threat intelligence feeds are supported. However, the solution does not include support for any threat intelligence standards such as STIX/TAXII. The solution supports enrichment of security data with identity information from IAM/IGA systems, UEBA systems, and business context information. The solution is able to identify multiple events from different sources and times as parts of a single security incident.

Threat detection is supported by the solution's ability to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The solution provides relative risk scores for each threat or incident, and it includes functionality to detect ransomware. It does not provide risk models for various industry use cases, but it does allow customers to define their own risk models. The solution has its own built-in behavior and anomaly detection engine but provides no OOTB integrations for third-party behavior analytics products.

The solution can prioritize alerts based on risk scores, it can prioritize groups of related risk scores based on combined risk scores, and it can correlate alerts for each user or entity to calculate a risk score. The solution also provides automatic triage of alerts and remediation of threats, but it does not provide automatic recommendations based on historic data. The solution also does not support full natural language searches of collected data, but searches can be conducted using drop-down selections. There is no need to learn a query language. The solution does enable users to pivot to related events, entities, or users to better understand the relationship between them and to estimate the impact.

The solution provides good incident response capabilities, including a centralized interface for collaborating across all organizational units, full lifecycle management for the creation, tracking, and management of incidents. The solution supports the visualization of network flows and includes direct remediation capabilities. Huntsman does not have any plans for integration with SDN/SDCI solutions. The product can discover shadow IT and alerts are mapped to the ATT&CK framework. The solution also enables users to prioritize the ATT&CK techniques they believe are the most relevant to the organization.

The product provides automation capabilities for various parts of incident response workflows, and it supports automation of actions that involve third-party products, but it does not include a visual designer for automation workflows and playbooks. The product offers a catalog of pre-built playbooks for common scenarios, and it provides a catalog of actions or other building blocks for playbooks. Workflows/playbooks do not support conditional or manual approvals. Huntsman Enterprise SIEM uses only unsupervised ML detection models and does not use DL algorithms. ML is used for a wide range of purposes, but not including the prioritization of alerts based on historic responses by analysts. Huntsman provides support in tuning inputs for ML algorithms, and the solution provides ML-based analytics, but that does not include predictive analytics.

Huntsman Enterprise SIEM is independently penetration tested and used in accredited environments but is not independently certified to support compliance with any of the major security standards. The product has a built-in, highly granular role-based access control (RBAC) system. This enables it to support a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, and incident responders, as well as providing support for multiple groups, with the ability to restrict access on a need-to-know basis for alerts and events to enable segregation based on departments and geographic location. The product supports automatic compliance reporting, enables customers to keep data entirely on premises, and offers guaranteed data/metadata residency for all customers because there is no mandatory cloud component.

The product is not built on cloud-native architecture, but it does support the collection of logs from cloud services and applications, it does support multi-cloud deployments, it does have agents for cloud infrastructure, and connectors are provided for a wide range of services under Microsoft Azure, GCP, and AWS. It provides a relatively limited number of OOTB integrations with other cloud-based business applications and cannot connect to a CASB to collect logs from cloud-based shadow IT.

Huntsman Enterprise SIEM provides a complete foundation for an enterprise-grade security operations center, for on-premises, in cloud, or managed deployments for all but the smallest of businesses. The product is popular with government agencies, large enterprises, and SIs. It is favored by MSSPs for its fully multitenant architecture, and its ability to accommodate extremely high event throughputs and function in closed network environments.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 6: Huntsman's rating

Strengths

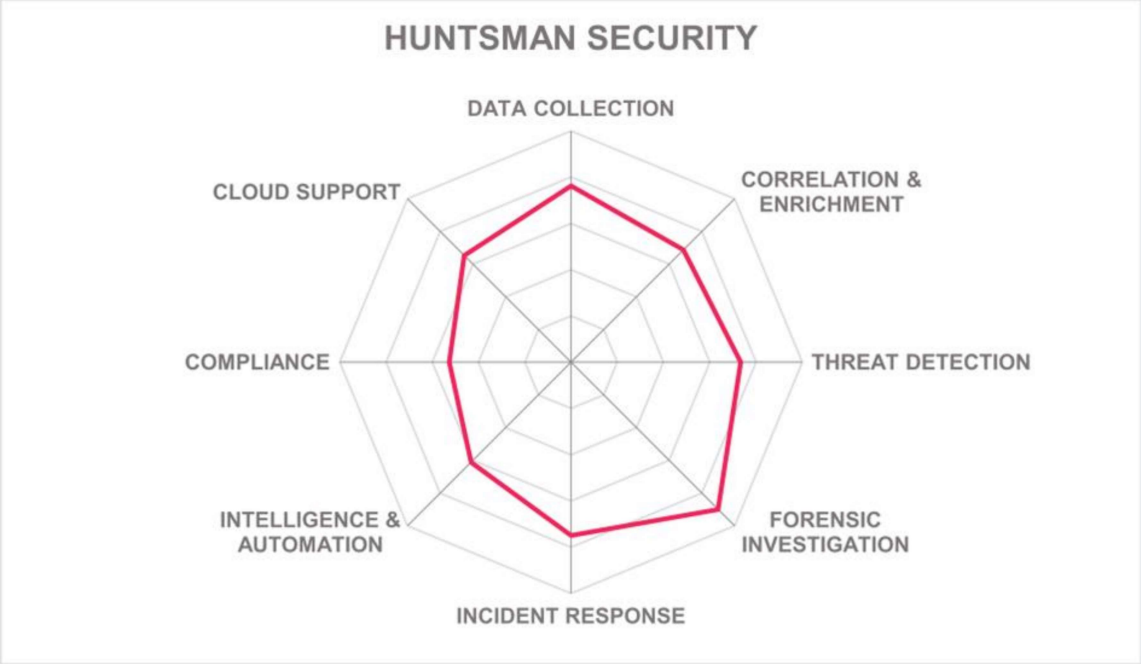
- Flexible licensing models and deployments options
- Special features and licensing plus strong multitenancy capabilities for MSSPs.
- Can function fully on closed networks without any internet connection.
- Available as a managed service if required.
- Can take data in from any source and does not require traditional network.
- Scalable storage.
- Alert triage and instant incident response with built-in case management capability.
- Easy access to data via UI.
- Good cloud support with bi-directional connectors.
- All event and alert details held within incidents, even when incidents are archived.
- Good correlation with ATT&CK framework via dedicated and interactive dashboard.
- Strong support for role-based access control with built-in RBAC functionality.

Challenges

- Limited cyber risk management integrations, but improvements on the roadmap.
- Traditional investigation screen with no node-graph capability.
- Full natural language search not available, but no query language skills required because Huntsman uses a point-and-click query interface.
- No automatic incident linking capability, although incidents can be linked manually.

- Solution is not independently certified to support compliance with any of the major security standards.
- Limited market presence outside the APAC region, UK, and Europe.
- Support offered only in English and Japanese, documentation only in English.
- Solution does not support OSI layer 7 traffic analysis.
- Huntsman does not provide its own threat intelligence.
- No automatic recommendations based on historic data.
- Solution does not provide risk models for various industry use cases.

Leader in



IBM Security – QRadar SIEM

IBM Corporation is a publicly listed multinational technology and consulting company founded in 1911 and headquartered in the US in Armonk, New York. With over 100 years of history, IBM has evolved from a computing hardware manufacturer to offer a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and cybersecurity.

IBM has a large global partner and channel network, with most customers in the mid-market and large enterprise segments located mainly in EMEA, followed by North America, APAC, and LatAm.

IBM's QRadar Suite is aimed at bringing together all the core capabilities needed to run a SOC on a single modular platform, namely SIEM, SOAR, EDR/XDR, Log Insights, and ASM. The suite is designed around the analyst experience with increasing levels of automation available. The open architecture of the platform means that customers can use any combination of IBM and third-party core SOC capabilities via federated access, and access them through the QRadar Suite's unified analyst experience or common set of functionalities (federated search, automated investigation, and recommended remediations) that are available across the suite.

The suite has simplified and flexible licensing that allows customers to choose between usage-based or enterprise-based licensing models for each of the suite's components, depending on their requirements. The metric for enterprise-based licensing is common across all components. It is based on the size of the environment being protected and is expressed in terms of managed virtual servers (MVS). The metric used for usage-based licenses is EPS for SIEM, number of users for SOAR and ASM, number of gigabytes per day for Log Insights, and number of endpoints for EDR. Because customers buy tokens called resource units, these can be translated into the common enterprise metric or any of the usage metrics, which means that customers can use a mix of models across the suite and can switch easily from one to the other for each of the components.

QRadar SIEM is available as software installed on premises, as physical and virtual appliances that can be deployed on premises or in a cloud of choice, as a managed service, and as SaaS offering. IBM security released QRadar cloud-native SIEM in December 2023 that has the cloud-native qualities of elasticity, resilience, speed, and scalability. It can run as a SaaS service, and is scheduled to be available in an on-premises or hybrid deployment in the second half of 2024.

The solution supports a comprehensive range of log sources, including OT, IoT devices, and mobile devices. It allows customers to configure custom log formats and develop custom connectors for log collection. There are no technical limitations to the number or size of collected logs. The solution supports capturing and analyzing network traffic, including virtualized infrastructures and OSI layer 7 traffic. It can also capture network traffic on a gateway and supports passive mode on SPAN/TAP. The solution supports all common protocols and services. It also supports collecting data directly from endpoints using APIs

and agents. An extensive range of operating systems and platforms are supported by agents, including AIX, Android, Bastion, Linux, mainframes, MacOS, Unix, and Windows. Agentless data collection is also supported, using the RPC and SSH protocols.

QRadar SIEM correlates real-time and historical security data from different sources, and collects and analyzes data from all sources, including cloud and on-premises in real time. The solution is backed by IBM's X-Force Threat Intelligence with support for external threat intelligence feeds. The solution supports the STIX/TAXII threat intelligence standards, and it is able to use information from IAM/IGA systems, UEBA systems, and business context information for security data enrichment. The solution is able to identify multiple events from different sources and times as part of a single security incident and bring all relevant information into a single incident for investigation.

Threat detection is supported by the solution's ability to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The solution provides relative risk scores for each incident/threat, and it includes functionality to identify ransomware behaviors. The solution provides risk models for various industry used cases, which can be customized. QRadar SIEM comes with OOTB integrations with half of the most common third-party behavior analytics products, but customers can take advantage of universal device support module (uDSM) functionality to build custom parsers visually. This means the solution can ingest, parse, normalize, and use log sources that do not have a DSM OOTB.

The solution can prioritize alerts based on risk scores, it can prioritize groups of related alerts based on combined risk scores, and it can correlate alerts for each user or entity to calculate a risk score. The platform also provides automatic triage of alerts and recommendations based on historical data, but it does not provide automatic remediation of common threats. It is also possible to pivot to related events, entities, or users to better understand relationships between them and to estimate the impact. Queries can be built by clicking on search terms, but full natural language search capabilities have been identified as a key AI use case and are still under development. IBM is also working on functionality to translate search queries from one query language to another. IBM QRadar Incident Forensics tool allows companies to index and search captured network packet data (PCAPs) and includes a feature that can reconstruct that data back into its original form. This reconstruction feature applies to data and files, including email messages, file and picture attachments, VoIP phone calls and websites. Customers can also import existing Yara and Sigma Community rules into the tool for extended use cases, and use those rules for matching and flagging malicious content.

The solution includes a centralized interface for collaboration across all organizational units, and full lifecycle management for the creation, tracking, and management of incidents. It also supports visualization of network flows and integrates with SDN/SDCI tools. The solution includes minimal remediation capabilities, allowing users to write scripts that do specific actions in response to particular events. Greater remediation capabilities are available through QRadar SOAR within the QRadar Suite. QRadar SIEM provides functionality to discover shadow IT, and it can collect logs from shadow IT directly. Alerts are mapped to the ATT&CK framework, and the solution enables users to prioritize the ATT&CK techniques they believe are the most relevant to the organization.

The solution offers automation capabilities for various parts of incident response workflows, and it supports the automation of actions that involve third-party products. QRadar SIEM does not implement a visual designer for automation workflows, does not offer a catalog of pre-built playbooks for common scenarios, and does not offer a catalog of actions or other building blocks for playbooks. Workflows/playbooks do not support conditional logic or manual approvals. However, all these are available in QRadar SOAR. The solution uses supervised and unsupervised ML detection models, and also uses DL algorithms. ML is used for a wide range of purposes, including prioritization of alerts based on historic responses by analysts. IBM provides support in tuning inputs for ML/DL algorithms, and the solution provides ML-based analytics, but these do not include predictive analytics.

QRadar SIEM supports compliance with a comprehensive range of security standards, including FIPS 197, FIPS 140-2, PCI-DSS, HIPAA/HITRUST, US Section 508 IT accessibility standard, SBOM, and STIG hardening. The solution itself has certified compliance with ISO/IEC27001 and is in the process of acquiring US FedRAMP certification. It does not have AICPA's SSAE 18 SOC 2 Type 2 certification. The solution supports a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, and incident responders. It provides support for multiple groups, with the ability to restrict access on a need-to-know basis to enable segregations based on departments and geographic locations. QRadar SIEM’s support for multitenancy means that MSSPs and organizations can provide SIEM services to multiple organizations from a single, shared deployment and restrict access based on input sources and using security profiles and user roles to manage privileges. The solution offers guaranteed data/metadata residency for the EU, US, and UAE, and provides the option of keeping customer data entirely on premises.

The cloud-native edition of QRadar SIEM was released for general availability in December 2023. Multi-cloud deployments are supported, the solution covers logs from cloud services and applications, cloud infrastructure is supported by agents, and connectors are provided for a wide range of services under Microsoft Azure, GCP, and AWS. The solution comes with more than 600 OOTB data source modules (DSMs) for parsing third-party tools and security tools. The solution also provides integrations with a wide range of cloud-based business applications, and it provides functionality to connect to a CASB to collect logs from cloud-based shadow IT. Customers can also customize the Universal Cloud REST API protocol to collect events from various REST APIs, including data sources that do not have a specific DSM or protocol.

IBM QRadar SIEM caters to companies of all sizes, but is particular suited to mid-market and large enterprises looking for flexibility in deployment and licensing models as well as the ability to have a tightly integrated set of SOC capabilities on a single platform with a unified analyst experience or the flexibility to mix IBM with third-party core SOC capabilities, but still benefit from the QRadar common user experience.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 7: IBM Security's rating

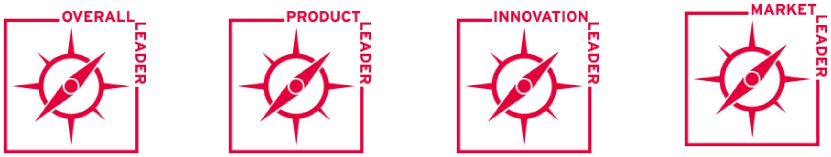
Strengths

- Modern SecOps approach that is analyst focused and AI-supported.
- Unified analyst experience across modular QRadar Suite.
- Flexible licensing models according to customer needs.
- Flexible and rapid deployment supported by automation.
- Fast and federated search capabilities.
- Strong forensics tools and capabilities.
- ML-based anomaly detection for zero-day threats and true anomaly detection.
- Supports a wide range of OOTB integrations and custom integration tools.
- Auto correlation of insights between network and logs.
- Built-in native SIGMA support.
- Support services available in a wide range of languages.

Challenges

- Full natural language search capability not available, but under development.
- Does not include some basic automation capabilities, including automatic remediation of common threats, relying instead on a SOAR solution for these such as QRadar SOAR or a third-party SOAR product.
- Workflows/playbooks do not support conditional logic or manual approvals natively.
- No generative AI capabilities, but this is under development.

Leader in




IBM SECURITY
DATA COLLECTION
CORRELATION & ENRICHMENT
THREAT DETECTION
FORENSIC INVESTIGATION
INCIDENT RESPONSE
INTELLIGENCE & AUTOMATION
COMPLIANCE
CLOUD SUPPORT

Logpoint – Logpoint Converged SIEM

Logpoint is a private global cybersecurity software company founded in 2003 in Copenhagen, Denmark, where the company is headquartered. Logpoint has offices across North America, Europe, and Asia. The majority of customers are medium-sized companies located in EMEA, followed by North America, APAC, and LatAm.

Logpoint Converged SIEM combines the company's SIEM, SOAR, and UEBA capabilities with its endpoint agent, AgentX, for all customer endpoints to import large quantities of data and enable response actions. UEBA is an optional add-on, along with Logpoint Business-Critical Security (BCS) for SAP to extract SAP data and connect it with any SIEM. Other add-ons include additional searchable and archive storage, premium support, and managed playbook services.

The solution is available as software installed on-premises, software installed on physical and virtual appliances, as a cloud service in public or private clouds, and as a managed service. Any combination of the above is also available.

On-premises SIEM licensing is based on the number of nodes or devices. SaaS licensing based on the number of employees. There are three SaaS packages for 50MB, 150MB, and 500MB per employee per day. On-premises and SaaS licenses include one concurrent SOAR user. This means multiple users can share the license with only one user accessing the system at a time. Additional SOAR licenses are available on a per concurrent user basis. UEBA licensing is based on the number of entities being tracked. BCS licensing is based on the number of users.

The solution supports a comprehensive range of log sources, including OT, IoT, and mobile devices. The solution is designed to normalize data into a single common taxonomy, which enables data ingestion from any source that can transmit logs through a common data exchange protocol. It is possible to configure custom log formats and develop custom connectors for log collection. There are no technical limitations to the number or size of collected logs. Logpoint's largest customers exceed 2TB per day. The solution supports capturing and analyzing network traffic, including virtualized infrastructure but not OSI layer 7 traffic directly. The solution also cannot capture network traffic on a gateway and does not support passive mode (SPAN/TAP). The solution supports the majority of common protocols and services, and it allows for the collection of data directly from endpoints using agents and APIs. Most operating systems and platforms are supported by agents, except Android, Bastion, and mainframes. Agentless log collection is supported using RPC, SSH, syslog, WEF, HTTP(S), WMI, Snare, and Nxlog.

The Logpoint Converged SIEM correlates real-time and historical security data from different sources, and collects and analyzes data from all sources, including on-premises and cloud. The solution does not come with its own threat intelligence sources, but it supports external intelligence feeds using a translation framework that normalizes TI from disparate sources into a single representation. The solution also supports STIX/TAXI and MISP. For security data enrichment, the solution is able to use information from IAM/IGA systems, UEBA

systems, and business context information. The solution is also able to identify multiple events from different sources and times as parts of a single security incident.

Threat detection is supported by the solution's ability to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The solution provides relative risk scores out of 100 for each threat/incident and creates alerts when the UEBA risk score exceeds the defined threshold. The solution also includes functionality to identify ransomware behaviors. It also provides risk models for various industry use cases, which can be customized. The solution provides few OOTB integrations for third-party behavior analytics products, but Logpoint develops support for any commercially available product free of charge.

The solution can prioritize alerts based on risk scores, it can prioritize groups of related alerts based on combined risk scores, and it can correlate alerts for each user or entity to calculate a risk score. The solution also provides automatic triage of alerts, automatic remediation of common threats, and automatic recommendations based on historic data. The solution supports natural language searches of collected data and enables users to pivot to related events, entities, or users to better understand the relationship between them and to estimate the impact. The solution's forensic capabilities are strengthened by the single taxonomy that makes cross-device analytics possible.

The solution offers a centralized interface for collaborating across all organizational units, and full lifecycle management for the creation, tracking, and management of incidents. The solution includes direct remediation capabilities and visualization of network flows. Logpoint currently does not have any planned integrations with SDN/SDCI solutions. Alerts are mapped to the ATT&CK framework, and the solution enables users to prioritize the ATT&CK techniques they believe are the most relevant to the organization.

The solution offers automation for various parts of incident response workflows, and it supports the automation of actions that involve third-party products. A visual designer for automation workflows and playbooks is included, the platform offers a catalog of pre-built playbooks for common scenarios, and it provides a catalog of actions or other building blocks for playbooks. Workflows/playbooks support conditional logic and manual approvals. The platform uses supervised and unsupervised ML detection models, and also uses DL algorithms, particularly to capture the collective knowledge of the SOC team as it interacts with the system. ML is used for a wide range of purposes, including prioritization of alerts based on historic responses by analysts. Logpoint provides support in tuning inputs for ML/DL algorithms and the solution provides ML-based data analytics, but this does not include predictive analytics to prevent future attacks.

The solution supports compliance with a range of regulations, including ISO/IEC 15408, PCI-DSS, and HIPAA/HITRUST. The solution itself has certified compliance with ISO/IEC 15408 and AICPA's SSAE 18 SOC 2 Type 2, while it is still in the process of getting ISO/IEC 27001 certification. The SIEM is also NATO certified, achieving the Common Criteria EAL3+ certification in 2015 and 2020. The solution supports a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, and incident responders, as well as providing support for multiple groups, with to ability to restrict access on a need-to-know basis to enable segregations based on departments and geographic locations. The solution

supports automatic compliance reporting against standards customer organizations need to meet, it enables customers to keep data entirely on premises, and it offers guaranteed data/metadata residency for the EU and the US, but not the UAE.

The solution is built on cloud-native architecture, but it does not support multi-cloud deployments. Logpoint SaaS is currently hosted on a single Tier 1 IaaS provider. It covers logs from cloud services and applications, and cloud infrastructure is supported by agents. Connectors are provided for a comprehensive range of services under Microsoft Azure, GCP, and AWS. It also provides OOTB integrations for a limited number of cloud-based business applications, and can connect to a CASB to collect logs from cloud-based shadow IT.

Logpoint Converged SIEM is suited to companies of all sizes looking for SIEM, SOAR, UEBA and the ability to respond to threats in business-critical systems in a single solution, particularly medium-sized companies seeking ML-based guidance and automaton to reduce the mean time to recovery (MTTR), and large enterprises and MSSPs with complex requirements requiring native multi-tenant capabilities and support for distributed environments.

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 8: Logpoint's rating

Strengths

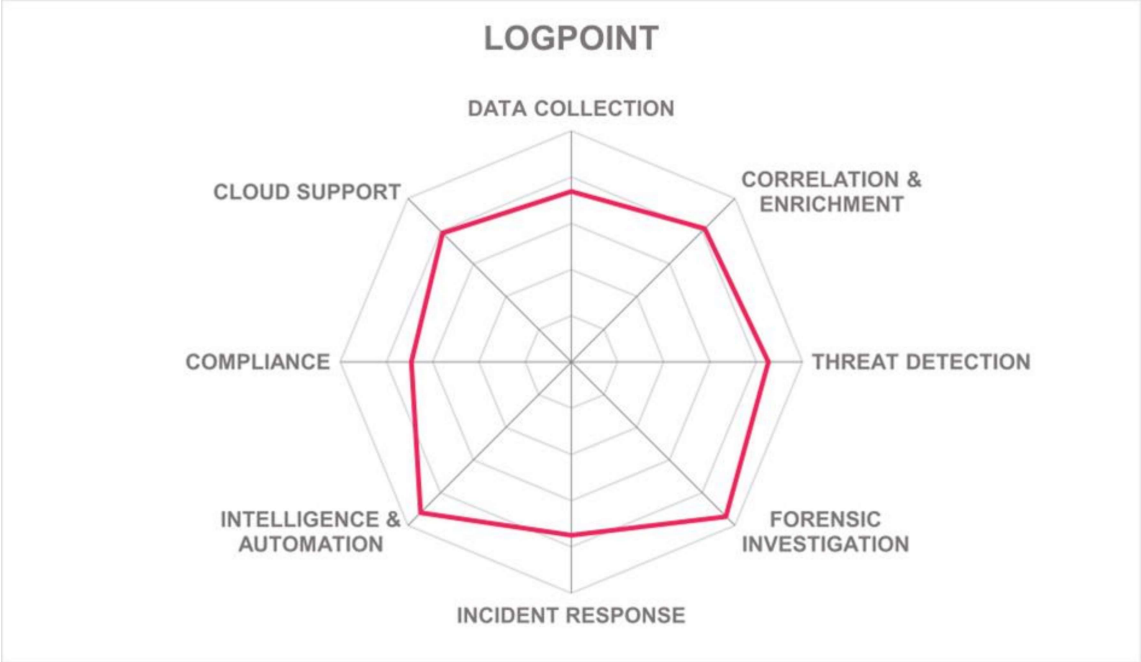
- Converged SIEM analyzes data to produce actionable knowledge.
- ML models provide guidance on the next steps.
- AgentX for high-volume data collection and response actions.
- Flexible deployment options.
- Simple, predictable licensing model that includes SOAR for one concurrent user.
- Good data collection capabilities.
- Detection and response logic continually fine-tuned by expert team.
- Strong automation capabilities aimed designed to reduce MTTR.
- Solution backed by threat research team and customer success engineers.
- Good reporting capabilities.
- Strong focus on privacy and data protection according to regulations like GDPR.
- Support services available in six languages.

Challenges

- AgentX not available for MacOS, but this is on the roadmap.

- Does not support direct OSI layer 7 traffic analysis.
- Limited number of OOTB integrations with third-party behavior analytics products.
- Does not support multi-cloud deployments.
- Limited OOTB integrations for cloud-based business applications.

Leader in



NetWitness – NetWitness SIEM

NetWitness was established in 1997 and is headquartered in the US in Bedford, Massachusetts, and has evolved from a packet capture solution vendor into a pure-play security operations company with a strong security heritage, offering a single, modular open architecture platform to detect, investigate, and respond to threats across complex environments.

The company is owned by the private equity firm, Symphony Technology Group (STG), and is transitioning into a fully independent company with a new leadership team, having been part of RSA since 2011, under the ownership of EMC, which eventually merged with Dell. RSA, including NetWitness, Archer, and SecureID, was acquired from Dell in 2020 by STG, which decided to split the group into three independent businesses.

NetWitness has sales teams in 22 countries, but is mainly channel based, with resellers and/or distribution partners in 60 countries, providing a worldwide sales and fulfilment function, and global support and implementation services.

As part of the NetWitness Platform, NetWitness SIEM sits alongside the company's NDR and EDR modules, which all share the same backend using a unified data model. They are also all backed by automation and in-house, real-time threat intelligence capabilities.

The solution is primarily targeted at governments and large enterprises in highly regulated and critical infrastructure industries with complex cybersecurity requirements, such as financial services, telecoms, energy, healthcare, and transportation, as well as the retail and technology sectors, including MSSPs, which make the solution accessible to smaller organizations.

NetWitness offers flexible deployment methods, with the SIEM module using a tiered throughput-based licensing model. There are separate charges for UEBA, hardware, storage, AI detection, EDR, and advanced SOAR, where these options are selected.

The solution supports a wide range of log sources, including OT, IoT devices, mobile devices, SASE network solutions, AWS AppFabric, and Windows and Linux. The solution allows customers to configure custom log formats and develop custom connectors for log collection. There are no technical limitations to the number or size of collected logs. The solution supports capturing and analyzing network traffic, including virtualized infrastructure and OSI layer 7 traffic. It can also capture network traffic on a gateway and supports passive mode (SPAN/TAP). The solution supports all common protocols and services, and collecting data from endpoints using APIs and agents, which will run on Linux, mainframes, MacOS and Windows. AIX and UNIX support is agentless. A wide range of protocols are supported in agentless mode.

NetWitness SIEM correlates real-time and historical security data from different sources, and collects and analyzes data from all sources, including cloud and on-premises in real time. The solution is backed by NetWitness threat intelligence, including input from a community-based threat intelligence crowdsourcing platform, with extensive support for external threat

intelligence feeds. The solution supports STIX/TAXII threat intelligence standards. NetWitness SIEM is able to use information from IAM/IGA systems, UEBA systems, and business context information for security data enrichment. The solution is able to identify multiple events from different sources and times as part of a single security incident, and bring all relevant information into a single incident for investigation.

In terms of threat detection, the solution is able to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The solution can provide relative risk scores for each incident/threat. Risk scores and models are all customizable and tunable. Identification of ransomware behaviors can be done using the NetWitness Malware Analysis, Threat Analysis, Endpoint Insight products, which are optional extras to the SIEM module. The solution includes risk models for various industry use cases, which are customizable. The solution provides no OOTB integrations for third-party behavior analytics products, but can forward security events to them, and NetWitness is working on integrations.

The solution can prioritize alerts based on risk scores, it can prioritize groups of related alerts based on combined risk scores, and it can correlate alerts for each user or entity to calculate a risk score. However, the solution does not provide automatic triage of alerts, remediation of common threats, or recommendations based on historic data. Decision-making support and basic SOAR functionality are provided by the built-in NetWitness Orchestrator (NWO). Search functionality for collected data is reasonably good, but NetWitness SIEM does not yet include full natural language search, which is under development. The solution does enable users to pivot to related events, entities, or users to better understand the relationship between them and to estimate the impact. The NetWitness UI displays the nodal graph representation of entities and their relationships with others.

NetWitness SIEM provides good incident response capabilities, including a centralized interface for collaborating across all organizational units, and full lifecycle management for the creation, tracking, and management of incidents. The solution supports nodal graph representation and reconstruction of network flows, and there is support for direct remediation capabilities with NWO. The solution has integrations with SDN/SDCI solutions, but it does not include functionality to discover shadow IT or collect logs from shadow IT directly. The solution is able to help customers to prioritize the ATT&CK techniques they believe are the most relevant to the organization.

Automation capabilities are available for various parts of incident response workflows via NWO, which enables IR teams to coordinate multiple streams of activity, drive decision-making, escalate cases automatically, automate investigation processes, record all case information, expedite artefact collection, get instant team-based updates, and automate actions that involve third-party products. NWO also has a visual drag-and-drop UI to define playbooks, provides a wide range of built-in automation playbooks, and offers a catalog of actions or other building blocks for playbooks. Advanced SOAR capability is available as an optional extra from OEM partner, ThreatConnect. Workflows/playbooks support conditional logic and manual approvals. The solution uses supervised and unsupervised ML detection models but not DL algorithms. ML is used for a wide range of purposes, including prioritization of alerts based on historic responses by analysts. NetWitness does not provide

support for the tuning of inputs for ML/DL algorithms. The solution includes ML-based analytics, but it does not enable predictive analytics to predict and prevent future attacks.

The platform supports compliance with FIPS 140-2, NIST 800-57, PCI-DSS, and HIPAA/HITRUST, but not FIPS 197 and US FedRAMP. NetWitness SIEM has achieved ISO/IEC 27001 compliance, and an application for certification for compliance with AICPA's SSAE 18 SOC 2 Type 2 is in progress. The solution supports a reasonable set of roles, including admins, security analysts, SOC managers, incident responders, and content developers, but not including security and solution engineers, CISOs, and data integrators. The solution can support multiple groups, with the ability to restrict access on a need-to-know basis to enable segregations based on departments and geographic locations. NetWitness SIEM supports automatic compliance reporting against standards as well as audit logging and report scheduling. It also allows customers to keep sensitive data entirely on premises if required, offering guaranteed data/metadata residency for the EU, US, and UAE.

Looking at cloud support, the solution is built on cloud-native architecture, supports multi-cloud deployments, and can collect logs from cloud services and applications. Cloud infrastructure is supported by agents, and connectors are provided for a wide range of services under Microsoft Azure, GCP, and AWS. It also provides functionality to connect to a CASB to collect logs from cloud-based shadow IT, but OOTB cloud service/business application integrations are relatively limited.

NetWitness SIEM provides a comprehensive and flexible unified threat detection, investigation, and response platform for the largest and most security conscious organizations, providing visibility and context as well as automated, actionable insights. As a highly integrated and unified platform, NetWitness is a solution best suited for large enterprises looking for a security operations solution from a single vendor.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 9: NetWitness's rating

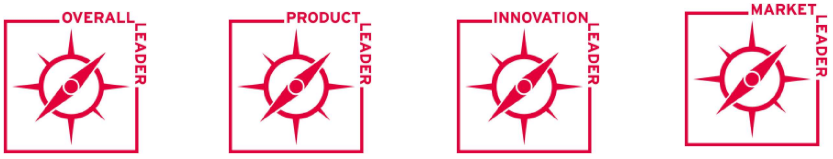
Strengths

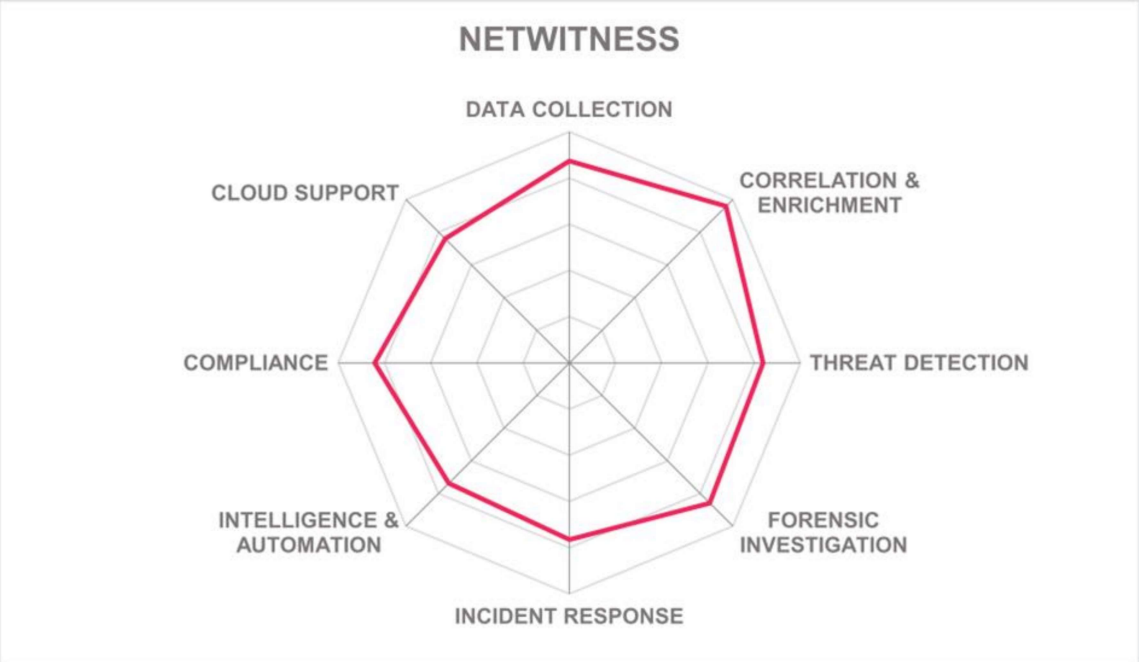
- Single unified platform with centralized configuration and content management.
- Flexible deployment options.
- Based on open platform architecture.
- Simple licensing model.
- Supports all use cases.
- Geared for complex security environments, including air-gapped systems.
- Can correlate all relevant security information into a single incident for easy investigation, enabling users to see a lot of information quickly and easily.
- Built-in NetWitness Orchestrator for providing basic automation capabilities.
- Can work across on-premises, cloud, and hybrid, with plans to expand to SASE.
- Good graphic representation of attack progression.
- Wide range of parsers.
- Good integration with third-party vendors with extensive set of APIs.
- Solution supported by real-time internal and external threat intelligence.
- Support services and documentation available in five languages.

Challenges

- No OOTB integrations for third-party UEBA products, but this is on the roadmap.
- No automatic triage of alerts, remediation of common threats, or recommendations based on historic data, but NetWitness is adding native remediation support from version 12.4 onwards.
- No natural language search functionality yet, but NetWitness is working on it.
- Does not provide predictive analytics to predict and prevent future attacks.
- Relatively limited OOTB cloud service/business application integrations.

Leader in




NETWITNESS
DATA COLLECTION
CORRELATION & ENRICHMENT
THREAT DETECTION
FORENSIC INVESTIGATION
INCIDENT RESPONSE
INTELLIGENCE & AUTOMATION
COMPLIANCE
CLOUD SUPPORT

Securonix – Unified Defense SIEM

Securonix is a private security analytics and operations management vendor, headquartered in the US in Addison, Texas near Dallas, with other US offices in Los Angeles, California and Jersey City, New Jersey. It also has offices in Neuss, Germany for EMEA, a UK office in London, and APAC offices in Bengaluru and Pune, India, and Singapore. The company dates back to 2008 and was incorporated in 2015.

Securonix has a large global partner network and supports mainly small, medium, and mid-market enterprises, with most customers in the mid-market segment, predominantly in North America, followed by EMEA, APAC, and LatAm.

The Securonix Unified Defense SIEM is available as SaaS and a managed service and has three main licensing packages, which all include Snowflake storage and use EPS as the main pricing component. The first, Unified SIEM Basic, is aimed at MSSPs and small to medium businesses looking for SIEM and log management. The second, Unified Defense SIEM Standard, is aimed at mid to large enterprises looking for SIEM and UEBA. The third, Unified Defense SIEM Advanced, is aimed at mature MSSPs and mid to large enterprises looking for advanced SIEM and UEBA. Add-on modules such as Autonomous Threat Sweeper (ATS), Securonix Investigate, and Threat Coverage Analyzer can be added to any package for an additional cost.

The solution supports a comprehensive range of log sources, including OT, IoT devices, and mobile devices, and allows customers to configure custom log formats for collection as well as develop custom connectors for log collection. There are no technical limitations to the number or size of collected logs. The solution supports capturing and analyzing network traffic, including virtualized infrastructure and OSI layer 7 traffic, but it cannot capture network traffic on a gateway and does not support passive mode (SPAN/TAP). The solution supports some of the most common protocols and services, but this list is not fully comprehensive. It supports collecting data directly from endpoints using APIs and agents. Agents will run on AIX, Linux, MacOS, and Windows. Agentless log collection is supported using SSH, WMI, SCP, SFTP, HTTPS, NFS, and SMB/CIFS.

The Securonix platform correlates real-time and historical security data from different sources, and collects and analyzes data from all sources, including on-premises and cloud in real time. The solution comes with its own threat intelligence sources as well as supporting external intelligence feeds, using any of seven standards for the delivery and integration of threat intelligence feeds. For security data enrichment, the solution is able to use information from IAM/IGA systems, UEBA systems, and business context information. Finally, the solution is able to identify multiple events from different sources and times as parts of a single security incident using tiered threat models.

Threat detection is supported by the solution's ability to establish behavioral baselines and detect anomalies and outliers in security data, which includes comparing normal profiles with current and historical events. The solution provides relative risk scores for each incident/threat using a risk engine. It also includes functionality to identify ransomware behaviors by detecting any anomalous/sudden changes to files, any rare entities accessing a

large number of files, and many other anomalous actions in files. The solution provides risk models for various industry use cases, which can be customized, and includes a dashboard showing the risk scores of users and entities. However, the solution provides no OOTB integrations for third-party behavior analytics products.

The platform can prioritize alerts based on risk scores, it can prioritize groups of related alerts based on combined risk scores, and it can correlate alerts for each user or entity to calculate a risk score. The platform also provides automatic triage of alerts, remediation of common threats, and recommendations based on historic data. There is an easy-to-use search function for collected data, but Securonix is still working on full natural language search. The platform does enable users to pivot to related events, entities, or users to better understand the relationship between them and to estimate the impact. Securonix Investigate provides on-demand context at investigation time, allowing analysts to query TI sources and internal context channels such as chat and collaboration tools, while Securonix Autonomous Threat Sweeper proactively searches for IoCs/TTPs related to new threats.

The platform provides good incident response capabilities, including a centralized interface for collaborating across all organizational units, and full lifecycle management for the creation, tracking, and management of incidents. The platform supports incident simulation for testing and improving existing workflows, and includes direct remediation capabilities, but does not include visualization of network flows. Securonix currently does not have any planned integration with SDN/SDCI solutions. The platform provides functionality to discover shadow IT and collect logs from shadow IT directly. Alerts are mapped to the ATT&CK framework, and the platform enables users to prioritize the ATT&CK techniques they believe are the most relevant to the organization.

Looking at intelligence and automation, the platform offers automation for various parts of incident response workflows, and it supports the automation of actions that involve third-party products. A visual designer for automation workflows and playbooks is included, the platform offers a catalog of pre-built playbooks for common scenarios, and it provides a catalog of actions or other building blocks for playbooks. Workflows/playbooks support conditional logic and manual approvals. Unsupervised and supervised ML and DL detection models are used for a wide range of purposes, including prioritization of alerts based on historic responses by analysts. Securonix provides support in tuning inputs for ML/DL algorithms, and the platform provides ML-based analytics, including predictive analytics.

The platform supports compliance with FIPS 140-2, NIST 800-57, PCI-DSS, HIPAA/HITRUST, and AICPA's SSAE 18 SOC 2 Type 2, as well as reporting for all major regulations, including the EU’s GDPR. The Securonix solution itself is compliant with ISO/IEC 27001 and is currently undergoing US FedRAMP certification. The platform supports a comprehensive set of roles, including admins, security engineers, CISOs, SOC managers, and incident responders, as well as providing support for multiple groups, with the ability to restrict access on a need-to-know basis to enable segregations based on departments and geographic locations. The platform also includes a compliance dashboard for real-time monitoring of compliance issues. Alerting and case management are integrated to generate notifications of any high-risk compliance violations. The platform offers

guaranteed data/metadata residency for the EU, US, and UAE, but does not provide the option of keeping customer data entirely on premises.

In terms of cloud support, the solution is built on cloud-native architecture, supports multi-cloud deployments, covers logs from cloud services and applications, cloud infrastructure is supported by agents, and connectors are provided for a wide range of services under Microsoft Azure, GCP, and AWS. It also provides integrations for a good range of cloud-based business applications, and provides functionality to connect to a CASB to collect logs from cloud-based shadow IT.

The Securonix Unified Defense SIEM provides a comprehensive unified threat detection and incident response (TDIR) platform with built-in SOAR, UEBA, and Snowflake storage for small, medium, and mid-market enterprises looking for proactive cyber defense capabilities.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 10: Securonix's rating

Strengths

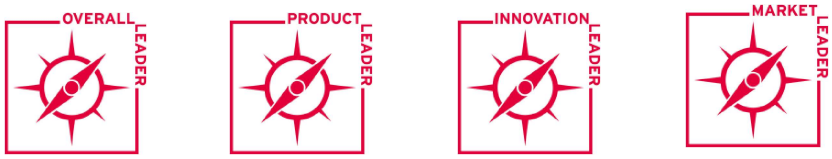
- Unified threat detection and incident response (TDIR) with built-in SOAR.
- Strong threat modelling capability.
- New Snowflake-based data lake for improved scalability and search performance.
- Strong analytics capabilities.
- Autonomous Threat Sweeper and Investigate provide good proactive defense.
- Threat Content as a Service capability, and optional Threat Coverage Analyzer.
- Good user interface with a clear summary view, easy navigation, and logical layout.
- ChatGPT integration provides support for analysts' queries.
- Support services available in nine languages.
- The platform supports incident simulation for testing and improving existing workflows.

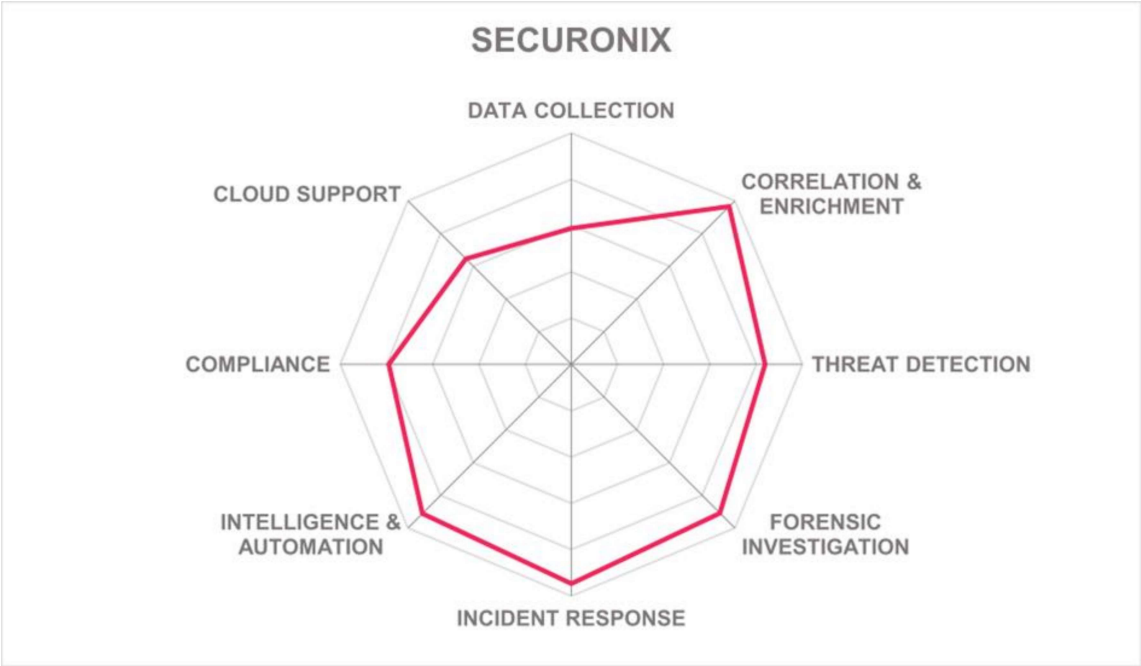
Challenges

- EPS-based pricing, but vendor is considering a shift to data-based pricing to increase predictability and reduce cost.
- Available only as a cloud-based service or a managed service, not on-premises.
- Full NLP and federated search are not yet available, but they are on the product roadmap.
- Few OOTB integrations for third-party behavior analytics products.

- Documentation available only in English.

Leader in





Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors may not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment, or maybe a fast-growing startup that may be a strong competitor in the future. Other companies listed here are considered I-SIEM platform vendors but did not participate in this report.

Anomali

Anomali is a private US cybersecurity company, founded in 2013 as ThreatStream, before rebranding in 2016. The company is headquartered in Redwood City, California, with other offices in major cities, including Belfast, Northern Ireland; London, UK; Singapore; and Dubai.

Why worth watching: The Anomali Platform is suitable for all organizations, especially large enterprises, banks, and government organizations requiring fast and retrospective searches for IoCs and the ability to know who is targeting them and how to enable a more proactive approach to security.

AT&T Cybersecurity

AT&T Cybersecurity (formerly AlienVault) is a developer of commercial and open-source services to manage cyberattacks, and it is one of the world's largest MSSPs. It was founded in 2018 and is headquartered in the US in San Mateo, California, and is a subsidiary of the multinational telecommunications company, AT&T.

Why worth watching: AlienVault Unified Security Management (USM) Platform includes SIEM (log and event management, event correlation, and reporting) plus security monitoring technologies, including asset discovery, network and host IDS, FIM, cloud monitoring, IR, vulnerability assessment, continuous threat intelligence, and a unified management console. It provides threat detection, compliance, and IR in one integrated platform.

Blumira

Blumira is a cybersecurity provider that was founded in 2018 and is headquartered in the US in Ann Arbor, Michigan. The company focuses on helping SMB and mid-market companies detect and respond to security threats, while meeting compliance and cyber insurance requirements. Products include endpoint visibility, automated response, XDR, and cloud SIEM.

Why worth watching: Blumira's Automated Cloud SIEM is aimed at making advanced detection and response easy and effective for small and medium-sized businesses to

accelerate the prevention of ransomware and data breaches. The solution is designed for rapid deployment and easy integration with existing technology stacks to help SMBs struggling with complex solutions and a lack of time, skills, and resources. Blumira also offers an all-in-one XDR platform that combines SIEM with endpoint visibility, detection, and automated response.

Datadog

Datadog is a company that develops a monitoring and analytics platform for technology stacks. It was founded in 2010, is headquartered in the US in New York City, New York, with offices around the world and regional headquarters in Boston, Massachusetts; Dublin, Ireland; Paris, France; Singapore; Sydney, Australia, and Tokyo, Japan. Products cover infrastructure, applications, digital services, logs, and security, including Cloud SIEM.

Why worth watching: Datadog cloud-native Cloud SIEM provides real-time threat detection across operational and security logs to deliver threat detection and investigation capabilities for dynamic, cloud-scale environments. The solution enables developers, security, and operations teams to leverage detailed observability data to accelerate security investigations in a single, unified platform.

Devo

Devo is a cloud-native logging and security analytics company (formerly known as Logtrust) that was founded in 2011 by a team of security experts and data scientists, and is headquartered in the US in Cambridge, Massachusetts.

Why worth watching: The Devo Security Data Platform integrates SIEM, SOAR, and UEBA, and features AI-driven decision making to deliver autonomous threat detection and incident response (TDIR) quickly, at scale, and at lower cost. The platform is powered by Devo's HyperStream technology, a cloud-native data processing engine that ingests and queries customer data at speed and at scale to deliver real-time visibility and high-performance analytics. Devo is aimed at supporting human-machine collaboration to augment security teams, and to enable better insights and faster outcomes.

DNIF

DNIF is a security analytics vendor established in 2002 and based in Mumbai, India. Before 2017, the company operated in the managed detection and response business, gradually developing its own data analytics technology to power it. In 2017, the company introduced DNIF HyperScale SIEM – an integrated platform that is engineered to run security operations at a massive scale, suitable for large enterprises and MSSPs.

Why worth watching: DNIF's solution combines SIEM, behavior analytics, orchestration, automation, and response capabilities in a single platform that is easy to deploy and operate without involving a team of engineers, but it is ready to deal with the petabyte-scale data collection to ensure complete coverage and full visibility into a company's security posture.

Elastic

Elastic is a public software company founded in 2012 and headquartered in the US in Mountain View, California. The company is primarily known as the developer of the open-source Elastic Stack, which combines the Elasticsearch search engine and Kibana data visualization framework with powerful data ingestion and processing capabilities.

Why worth watching: Elastic Security is suitable for all sizes of organizations in all sectors, particularly those in the public, financial, and technology sectors, looking for a SIEM solution with strong security analytics capabilities, AI support for analysts, and fast, federated, and collated search capabilities across large data sets and distributed data sources.

Fortra

Fortra (formerly HelpSystems) is a private US cybersecurity and automation company founded in 1982 and based in the US city of Minneapolis, Minnesota, providing a growing range of solutions through acquisitions.

Why worth watching: Fortra Event Manager is designed to prioritize security risks in real time, reduce alert fatigue by identifying and escalating critical security events to enable quick and effective response, record all security events and document investigations into security events, and tailor reports to meet an organization's requirements. Event Manager is aimed at organizations of all sizes, including a free version for small businesses.

Graylog

Graylog is a log management and security analytics software company based in the US in Houston, Texas. It was founded in 2009 as an open-source project in Hamburg, Germany.

Why worth watching: Graylog Security is built on the Graylog platform, has a modern UI, high logging bandwidth, and includes SIEM, security analytics, incident investigation, asset enrichment, and anomaly detection. The solution is designed to provide easy-to-use, affordable, and proactive threat detection, incident analysis, investigation, response, and compliance reporting.

LogRhythm

LogRhythm is a global security intelligence company that was founded in 2003, and is headquartered in the US in Boulder, Colorado. The company specializes in SIEM, log management, networking, and user behavior and security analytics. With offices in all geographic regions, LogRhythm has a substantial global presence, including a wide network of MSSP partners. The company offers a broad portfolio of security solutions beyond log management, including SIEM, UEBA, SOAR, as well as NDR and XDR products.

Why worth watching: LogRhythm provides an open cloud-native SaaS SIEM platform that includes security analytics and incident response capabilities, and it caters to organizations

of all sizes. The platform is designed to integrate easily with other cloud services and on-premises applications, automatically onboarding new data sources. The platform enables organizations to automate incident response and investigative workflows, and to conduct red team exercises and penetration tests, with out-of-the-box threat content mapped to the ATT&CK framework that supports custom threat detections. Log data is normalized and enriched through LogRhythm's patented Machine Data Intelligence (MDI) Fabric to improve searchability and analytics across disparate log sources.

Logsign

Logsign is a private cybersecurity company, specializing in security intelligence and security operations center solutions. Originally founded in Turkey in 2010, the company is headquartered in The Hague, Netherlands, with offices in Istanbul, Turkey, and Mumbai, India, with a marketing team in San Francisco, California.

Why worth watching: The Logsign Unified Security Operations Platform can be used for all sizes of organization, but it is best suited to medium to mid-sized organizations looking for a high level of integration between SIEM, SOAR, UEBA and threat intelligence in a single, easy-to-use platform that is deployed on premises or as a managed service.

Logz.io

Logz.io is a provider of cloud-native observability and security solutions founded in 2014 and headquartered in Tel-Aviv, Israel. The platform is designed as a universal solution for both DevOps and security specialists, based on a cloud-native architecture and powered by multiple open-source technologies.

Why worth watching: Logz.io Cloud SIEM is a cloud-native SaaS security monitoring and analytics platform with a multi-cloud, multi-tenant architecture and unlimited scalability. The platform is built for scale and combines the best-of-breed open-source monitoring tools in a fully managed cloud service, backed by dedicated security analysts and SIEM best practice expertise. The company offers a SIEM solution without the technical debt of legacy tools. With an API-first approach, it is suitable for companies that want to integrate SIEM functionality into existing toolchains.

ManageEngine

Headquartered in Pleasanton, California with development and operations in Chennai, India, ManageEngine is the enterprise software division of Zoho Corporation, an international software development company founded in 1996. ManageEngine offers solutions for a range of markets, including IT service and IT operations management, with IT security remaining a strong priority from inception.

Why worth watching: ManageEngine Log360 is a tightly integrated suite of specialized tools for log management and network security monitoring that are integrated into a single management console. Log360 provides a unified SIEM solution with integrated DLP and

CASB capabilities. Log360 does not reach full feature parity with enterprise-grade SIEM products from market-leading vendor, but it compensates by providing several complementary security and compliance features, including EDR, DLP, SOAR, and proactive and reactive analysis of an organization's security posture across all layers of its IT infrastructure.

Microsoft

Microsoft is a multinational technology company founded in 1975 and headquartered in the US in Redmond, Washington. After rising to dominate the personal computer software market with MS-DOS and Microsoft Windows operating systems, the company has expanded into multiple markets, including desktop and server software, consumer electronics and computer hardware, mobile devices, digital services, and cloud computing. Microsoft is the world's largest software company and one of the top corporations by market capitalization.

Why worth watching: Microsoft Sentinel, formerly known as Azure Sentinel, is a cloud-native SIEM and SOAR platform with UEBA capabilities AI support for enriching detection and investigation that delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Thanks to its native integrations into Azure cloud services, Microsoft's endpoint management and security tools, and threat intelligence, Sentinel offers a high degree of efficiency and ease of deployment. Sentinel also has built-in connectors to the broader security and applications ecosystems for non-Microsoft solutions. Microsoft offers substantial freedom of customization for the platform, by allowing customers to integrate other Azure services, enabling advanced analytics and threat hunting, own machine learning models, custom automations, and external threat intelligence.

OpenText

A Canadian enterprise information management software company founded in 1991 and headquartered in Waterloo, Ontario that nearly doubled its size in February 2023 with the acquisition of British multinational software company Micro Focus, making OpenText one of the fastest growing cybersecurity companies with a focus on information management and accelerating digital transformation.

Why worth watching: OpenText's acquisition of Micro Focus included the acquisition of several cybersecurity software products, including ArcSight, one of the pioneering security analytics and intelligence platforms. Under Micro Focus, ArcSight was honed into a layered security analytics platform, offering a complete security operations solution, including SIEM, UEBA, SOAR, and threat hunting capabilities on a unified platform with common storage, a shared data model, and a unified interface.

Panther Labs

Panther Labs is a venture-backed cybersecurity company that specializes in detection and response. It was founded in 2018 and is headquartered in the US in San Francisco, California.

Why worth watching: Panther v10 is an open-source cloud-native SIEM platform designed to meet the needs of cloud-first organizations. It is self-hosted, runs on top of native AWS services, and is designed to operate at scale, to process an infinite amount of data, to be easy to deploy, and to be used by experienced and inexperienced security practitioners.

Rapid7

A public global cybersecurity solutions provider founded in 2000 and based in the US city of Boston, Massachusetts, with offices across the US and in Canada and Australia supporting customers in 144 countries.

Why worth watching: Rapid7's Insight Platform provides a high degree of flexibility, enabling customers to combine multiple security solutions according to their current requirements, yet expand as their needs grow, still maintaining uniform visibility, management, and analytics across all products. For customers experiencing a cybersecurity skills shortage, Rapid7 also offers a number of managed security services.

Seceon

Seceon is a cybersecurity company that provides AI-supported security solutions to MSPs, MSSPs, and Enterprises. The company was founded in 2014 and is headquartered in the US in Westford, Massachusetts. Seceon’s products include its Open Threat Management (OTM) platform and its aiSIEM, aiXDR and aiMSSP platforms, which are built on OTM platform.

Why worth watching: Seceon’s aiSIEM is designed to avoid the pitfalls of traditional SIEMs and meet the requirements of cyberattack threats, techniques, and tactics. The platform is aimed at delivering continuous compliance monitoring, high fidelity threat detection, validated IoCs, and manual and automated response capabilities.

SolarWinds

SolarWinds is an American IT management software provider, founded in 1999 and headquartered in Austin, Texas, with offerings that cover a range of IT areas. The company’s product portfolio includes network management, systems management, database management, IT security, IT help desk, and cloud services.

Why worth watching: SolarWinds Security Event Manager (SEM) is designed to collect and correlate log data from thousands of devices to identify compliance violations and to mitigate emerging security threats. The solution can analyze real-time data from a wide range of sources, including routers, switches, servers, applications, and user endpoints. It includes more than 300 built-in report templates for regulatory compliance, including PCI-DSS, SOX, and HIPAA.

Splunk

Splunk is a software company founded in 2003 and is headquartered in the US in San Francisco, California. In September 2021, Cisco announced plans to acquire Splunk, which produces solutions for searching, monitoring, and analyzing any kind of machine-generated data. With its worldwide market presence and a strong ecosystem, Splunk is often considered a de facto standard for operational analytics and intelligence solutions. In 2009, the company introduced Splunk Enterprise Security - a dedicated security analytics platform.

Why worth watching: Splunk's strong market visibility makes it the first choice for any kind of operational or security analytics for many organizations, especially when a large number of readily available integrations, applications and APIs are required. The company's technology ecosystem is extensive. Cisco’s acquisition of Splunk is expected to be completed by the end of Q3 in 2024. Combined, Cisco and Splunk will become one of the world's largest software companies. The combination of these two companies is designed to drive the next generation of AI-enabled security and observability.

Sumo Logic

Sumo Logic is a cloud-native data analytics company based in the US in Redwood City, California. Founded in 2010, the company focuses on developing and operating an elastic cloud platform for collecting and analyzing enterprise log data. Sumo Logic offers a range of operational, security, and business intelligence solutions that are entirely cloud-based and maintenance-free.

Why worth watching: the company's Cloud SIEM solution is, as the name implies, an entirely cloud-based SaaS offering with a flexible pricing model and unlimited scalability. The solution's multi-tenant architecture allows customers to benefit from the "crowd wisdom" via anonymized threat analytics and recommendations.

Trellix

Trellix is a relatively new brand formed from the acquisitions and reorganizations of FireEye, and the McAfee enterprise and security service edge (SSE) businesses by Symphony Technology Group (STG). Trellix is a privately held cybersecurity company and is based in the US city of San Jose, California. The company launched in January 2022 with the combined security heritage, customer base, and assets from its parent organizations, including endpoint, network security, data leakage prevention (DLP), and SIEM components.

Why worth watching: Trellix Enterprise Security Manager is designed to provide near real-time visibility into the activity on all of an organization's systems, networks databases, and applications to detect, correlate, and remedy threats across the IT infrastructure. The solution integrates security tools and augments them with next-generation SIEM, SOAR, threat intelligence, and UEBA capabilities to enable security teams to conduct alert management, search, analysis, investigations, and reporting.

Trustwave

A global cybersecurity and managed security services company that is an independent subsidiary of multinational telecommunications company Singtel Optus group. Trustwave was founded in 1995, is headquartered in Chicago, Illinois in the US, and provides a range of cybersecurity services,

Why worth watching: Trustwave's Co-Managed SOC service is designed to go beyond traditional managed SIEM capabilities by helping organizations plan, build, and run their SIEM and security operations teams with greater efficiency. The service includes global alert monitoring, triage, and intelligence-led in-depth investigations, and is aimed at helping organizations to leverage their existing security investments, eliminate active threats, and augment in-house security operations teams to increase productivity and free up resources. In October 2023, the company introduced Trustwave Managed SIEM for Microsoft Sentinel aimed at maximizing an organization's Microsoft E5 investment, particularly those without a robust cybersecurity team.

Wazuh

Wazuh is a cybersecurity platform that provides unified XDR and SIEM protection for endpoints and cloud workloads. It was founded in 2015, is headquartered in the US state of California, and is used by numerous enterprises, including a Fortune 10 tech company.

Why worth watching: Wazuh is a free and open-source comprehensive security platform that provides unified XDR and SIEM protection for endpoints and cloud workloads. Wazuh charges for services and support. The solution is composed of a single universal agent and three central components: the Wazuh server, the Wazuh indexer, and the Wazuh dashboard. Users can deploy the agent to computers, virtual machines, and containers, and install it on most operating systems. Wazuh components abide by the GNU General Public License, version 2, and the Apache License, Version 2.0 (ALv2). There is also a SaaS version.

Related Research

Leadership Compass: Intelligent SIEM Platforms (2022)
Leadership Compass: Security Orchestration Automation and Response (SOAR) (2023)
Leadership Compass: Managed Detection and Response (2023)
Leadership Compass: Data Security Platforms (2023)
Leadership Compass: CIEM & Dynamic Resource Entitlement & Access Management (DREAM) platforms (2022)
Leadership Compass: Network Detection and Response (2021)
Leadership Compass: Fraud Reduction Intelligence Platforms (2021)
Leadership Compass: CIAM Platforms (2020)
Market Compass: SOC as a Service (2022)
Advisory Note: 2022 IAM Reference Architecture
Advisory Note: Architecting your Security Operations CentreLeadership Brief: Find Your Route from SIEM to SIP and SOAR
Leadership Brief: Responding to Cyber Incidents
Leadership Brief: Incident Response Management
Leadership Brief: Security Fabric: A Methodology for Architecting a Secure Future
Architecture Blueprint: Architecting your Security Operations Centre
Executive View: Micro Focus ArcSight
Executive View: ManageEngine Log360
Executive View: Exabeam Security Management Platform
Executive View: IBM Cloud Pak for Security
Executive View: IBM QRadar Advisor with Watson
Executive View: IBM QRadar Security Intelligence Platform
Executive View: Securonix Cloud SIEM and UEBA
Executive View: LogRhythm Security Intelligence Platform

Copyright

KuppingerCole Analysts supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole Analysts AG, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.