
NETWITNESS
DETECT AND RESPOND TO ANY THREAT, ANYWHERE
See everything. Fear nothing.
www.netwitness.com

In the current ever-expanding landscape, cyber risk and business interruption are the risks the companies fear most, reflecting the importance of today's digital economy, the evolving threat from ransomware and extortion, as well as geopolitical rivalries and conflicts increasingly being played out in cyber space.

# The below challenges make the scenario more complex:

## Usability

High turnover drains senior expertise from the SOC, steepening the learning curve and prejudging team's ability to respond to alerts.

## Visibility

Expanded use of agent-less devices exponentially increases unknown traffic.

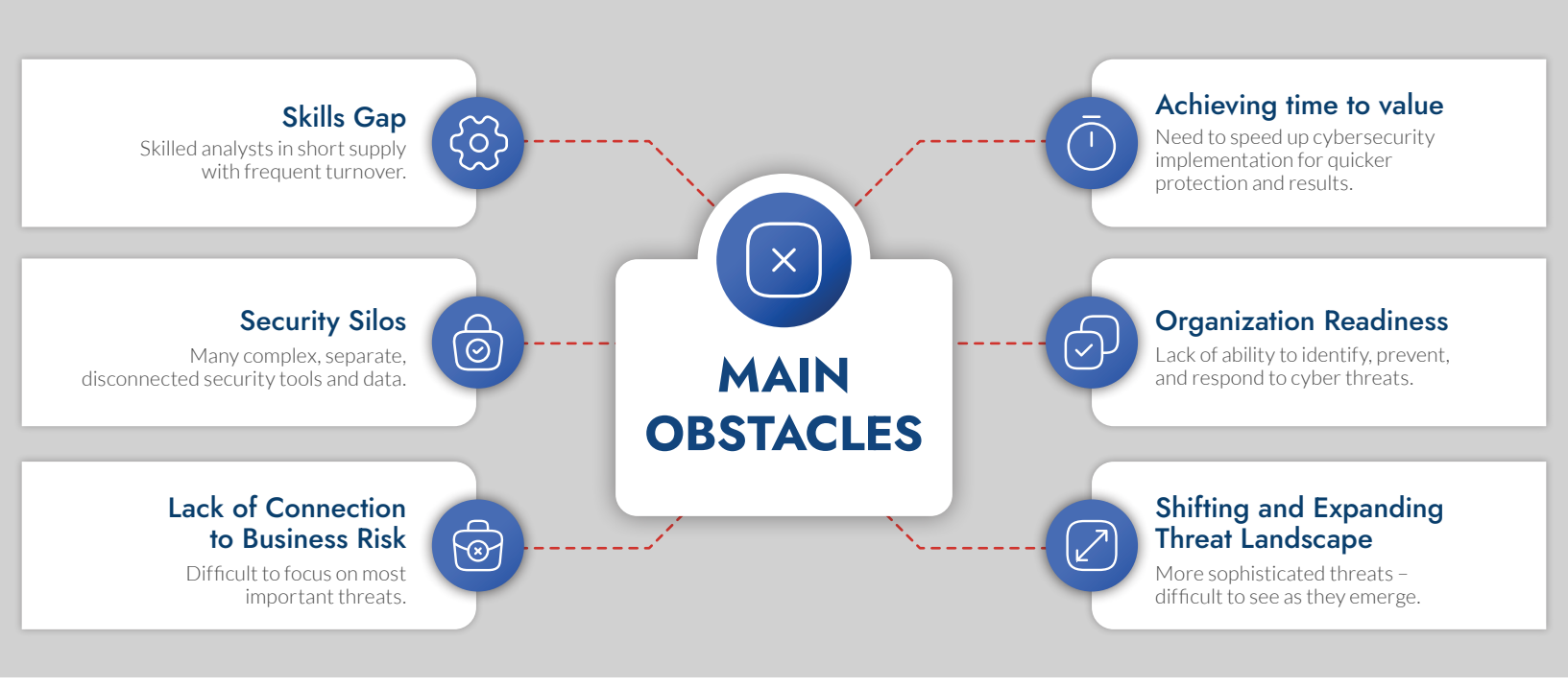
Technology continues to encrypt more traffic and data reducing the visibility.

## Efficiency

As budgets decrease and complexity of threats increase there's pressure to do more with less.

Cybersecurity budgets lack sufficient funds to cover all needs.

## To achieve comprehensive threat detection and response, we must first acknowledge and overcome the numerous obstacles that stand in our way.




**Inadequate threat detection and response measures can result in a catastrophic data leak, which can have devastating consequences for a critical infrastructure.**

NetWitness is the most comprehensive, yet flexible, unified threat detection, investigation, and response platform to deliver unparalleled visibility, robust contextualization, and automated, actionable insights that empower security teams to tackle the most complex, sophisticated attacks.

# The NetWitness Open Platform

## Which delivers across four major focus areas:

**Intuitive**
Seamless and easier adoption, less complexity.

**Automated**
Drive bi-directional integrations. Push/pull data to achieve more automation in the SOC.

**Intelligent**
Leverage the power of analytics, ML and AI.

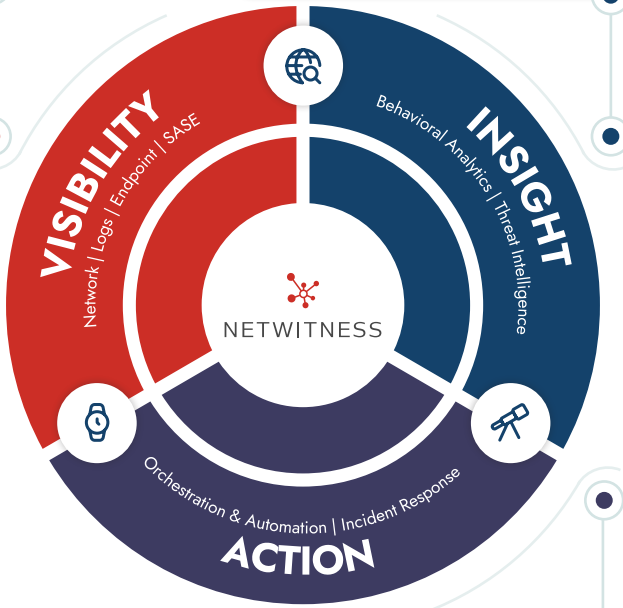
**Efficient**
Doing more with less, reduced footprint, compression, bundling.

### See every attack

Deep visibility across the entire infrastructure and scalability from on-premise to multi-cloud.

### Expose the full scope of every attack

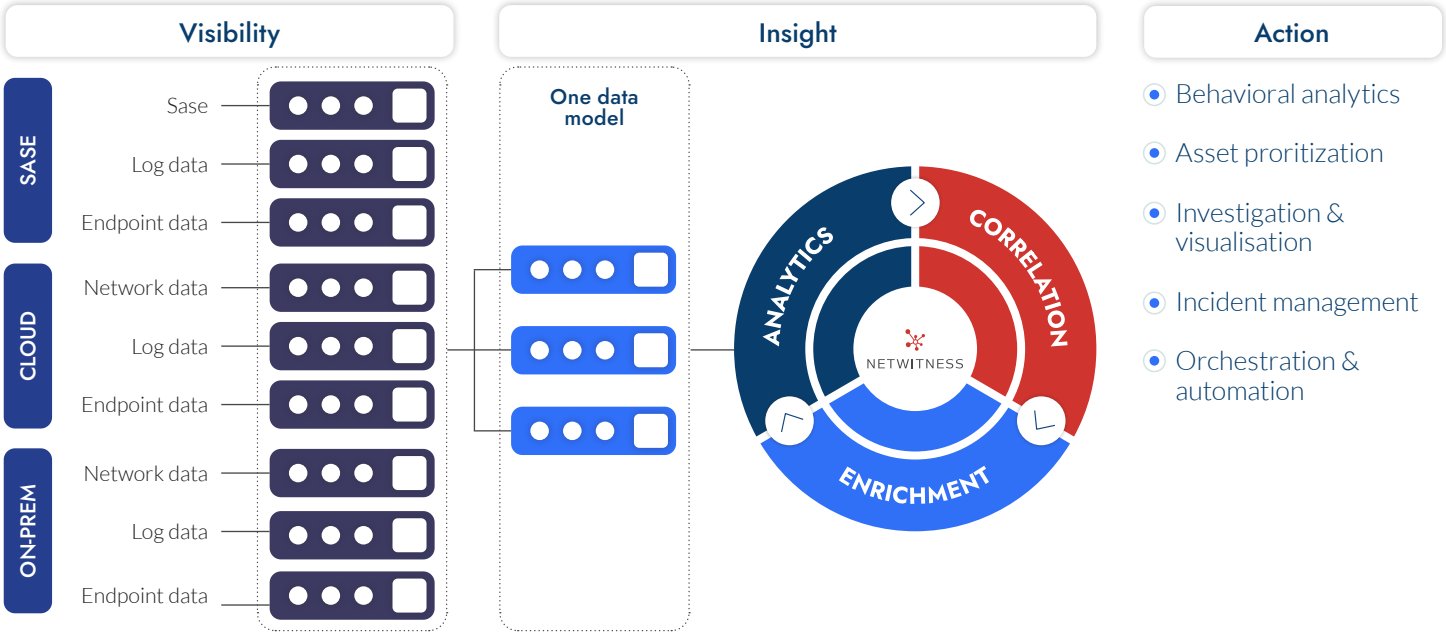
Comprehensive platform enriching, machine learning and behavior data analysis to detect anomaly and identify unknown pattern.




### Respond to every attack

Orchestrate and automate action to quickly address response and threat management.

# The Architecture




Threat intelligence

| | | | |
|---|---|---|---|
| One platform that gives attackers nowhere to hide | Open to integrate third party components | Modular approach | One data model |

# What makes NetWitness Platform different?

A modular, intelligence-driven threat detection and response platform that works with multiple key security data planes, provides insightful context and analysis, in a unified data architecture and interface.

Drive bi-directional integrations. Push/ pull data to achieve more automation in the SOC.

Automatic Threat Intelligence, Business and Technical Context.

Multi-Layered Threat Detection and Behavioral Analytics.

Effective investigation through complete session Reconstruction and Forensics.

Unified Data Architecture, Visualization, Investigation and Threat Hunting.

# NetWitness Services

## NetWitness Professional Services

Draw on hands-on, deeply experienced specialists to optimize the effectiveness of your NetWitness solutions

## NetWitness Cyber Defense Services

Continuously improve your ability to detect, investigate and respond to threats and to maximize the value received from NetWitness and other security solutions

## NetWitness Education Services

Draw on extensive live, virtual and on-demand training options to extract the most power from NetWitness

## NetWitness Incident Response

Quickly find the source of, and remediate, an urgent threat by engaging NetWitness' Incident Response Team which will

1. Promptly investigate and assess the dynamics of the malicious actions preparing for a strategic remediation
2. Identify all the evidences linked with the attack allowing the evaluation of its magnitude
3. Empower the customer with all needed recommendation and actions to successfully expel the malicious actor
4. Provide post-incident monitoring to prevent any attacker come back

# History of NetWitness

**Network Detection and Response since 1996**

We were the first to do NDR and continue to excel at it.

**SIEM since 2000**

We evolved SIEM for true detection and response within logs.

**Endpoint Detection and Response since 2007**

Originally invented for a Northern American military, EDR became part of our official offering in 2012.

**Extended Detection and Response 2017**

## See Everything. Fear Nothing.

Next steps towards achieving comprehensive cybersecurity.

**Book a deep dive:**

**Request a Demo**
www.netwitness.com

**Get in touch to learn more about NetWitness:**
email us

NETWITNESS