NETWITNESS

# NetWitness® Insight

## Automated Asset Discovery and Security Prioritization

To defend the enterprise, security analysts must monitor billions of network sessions and millions of IP addresses in search of threats and anomalies. Massive data sets drive alert fatigue and increase the challenge to quickly identify and block the threat. Organizations need an automated and reliable way to cut through the data and noise to protect those assets that matter most.

## Reduce mean time to detect and respond

NetWitness® Insight empowers security teams to determine what assets matter most, providing the knowledge and context they need to better defend the enterprise. By automatically and continuously pulling network metadata, NetWitness Insight passively discovers, profiles, categorizes, characterizes, prioritizes, and tracks all assets, improving detection quality while simplifying analysts' search.

With NetWitness Insight, organizations discover and have visibility into assets, including ones they did not know they had. Assets are categorized by network profile and prioritized by risk level based on activity and exposure ranks. The addition of asset contextual enrichment, usage baselines, and the detection of new or altered assets empowers the cybersecurity team to truly understand their network and where to focus their stretched resources.

### Key Features

- Proprietary, patented, unsupervised learning techniques
- Dynamic, statistical risk scoring technique
- Deep packet visibility with historical forensics enriched by automated asset discovery and contextual information
- All native, server-less SaaS technology
- Passive asset discovery and categorization
- Efficient, scalable architecture

## Scalable, high-performance cloud security

- Gain a comprehensive picture of your network behavior with a complete inventory of your assets.
- Create a baseline understanding of your network's security profile within hours.
- Prioritize your efforts with rankings that identify assets most at risk.
- Confidently and quickly make decisions on the priority and criticality of an investigation.
- Save time and money with SaaS. No hardware or IT investments required, eliminating additional capital and administrative costs.

## NetWitness Insight for a Complete Picture of Network Assets

| | |
|---|---|
| **Asset Discovery and Characterization** | NetWitness Insight inventories the true data that lives on your network and turns it into something actionable. It uses custom learning techniques to investigate the entire network to identify all assets. Each asset is described by a set of custom categorical labels and aggregate statistics that reflect its observed network behavior during a given measurement window: the network category (e.g., HTTP, DNS, SMTP) and type (e.g., Server, Client, FewClients, Undefined). The number of services, clients and external clients are captured as aggregate discrete values summarizing the totality of traffic reaching the asset. |
| **Asset Prioritization and Ranking** | To help analysts quickly focus on risks that matter the most, NetWitness Insight performs a variety of ranking functions to identify important assets based on different criteria, including an Activity Rank (a popularity ranking), and an Exposure Rank, which reflects the network risk calculated by the number of services and clients (internal/external) connecting to the asset and directionality (traffic flowing in or out of the network to the asset). |
| **Asset Categorization and Contextual Enrichment** | Asset categorization provides analysts a point of reference describing how an asset behaves over time, yielding a rapid way to determine if an asset category has remained constant or not. To characterize assets, NetWitness Insight constructs a network profile for each asset by analyzing all the protocols, clients, directionality, and type of traffic associated with it. This data provides a multitude of criteria to use as contextual data points to understand how to triage an asset in relation to the potential threats. |
| **Passive Asset Discovery and Categorization** | NetWitness Insight's proprietary, patented, unsupervised algorithm continuously pulls network metadata from NetWitness Network and passively discovers, profiles, categorizes, characterizes, prioritizes, and tracks all assets. |
| **Asset Tracking and Detection of Alteration** | By tracking the behavior of an asset over time, NetWitness Insight provides analysts with context spanning multiple days, empowering them to make quick and accurate decisions about the significance of a threat to a given asset. Any significant variation in the behavior from a baseline of all assets can induce a change in the network category and can trigger an alert. |

## NetWitness Professional Services — Committed to Your Success

NetWitness offers the services to support the ongoing success of security operations teams. These range from SOC design, implementation, and training, to managed detection and response (MDR) and major incident response (IR). IR Retainer Services ensure rapid response in the event of a major attack or breach.

**Ready to learn more? Visit www.netwitness.com**



NETWITNESS