NETWITNESS

DATA SHEET

NetWitness® Detect AI

Cloud-native machine learning for rapid detection of sophisticated threats

The digital attack surface continues to expand rapidly and grow increasingly complex and disjointed. This makes it harder for security teams to protect every asset from every threat vector, from commodity malware to state sponsored exploits and zero-day threats. Existing security monitoring technologies don't seem to offer much relief. They still produce too much data, too much noise, too many false alerts for overburdened security teams to sift through.

NetWitness Detect AI is a cloud-native SaaS offering that uses advanced behavior analytics and machine learning to quickly reveal unknown threats and provide high-fidelity actionable threat detection. NetWitness Detect AI frees security teams to focus on actionable alerts by automatically flagging the risky behaviors and suspicious anomalies that can signal the highest risk threats.

Advanced analytics and high-fidelity threat detection using the power and scale of the cloud

NetWitness Detect AI applies advanced analytics and machine learning to data captured by NetWitness Platform to deliver actionable threat detection against emerging and sophisticated attacks. The beauty of the solution is four-fold: it begins working to identify suspicious behaviors immediately; the machine learning algorithms require no manual tuning; and because it's SaaS, the hardware and ongoing management requirements are minimal, and it scales to meet your organization's needs and use cases.

High-fidelity threat detection

NetWitness Detect AI's machine learning algorithms automatically and continually get smarter about your organization's user and entity behaviors. NetWitness data scientists tune and update the algorithms regularly so that it always provides accurate threat monitoring without requiring rules, signatures or manual analysis.

Relief for security analysts

NetWitness Detect AI uses an innovative risk scoring model to alleviate analysts' alert fatigue by zeroing in on the highest risk indicators within noisy data environments.

Quick, easy deployment

NetWitness Detect AI requires minimal to no additional hardware, which dramatically simplifies installation and ongoing management of the solution. Administrators and analysts don't need to manually tune algorithms, and with native SaaS benefits, stability is never an issue.

Key features

- Innovative, dynamic statistical risk scoring model produces high-fidelity alerts with meaningful insights
- Intelligent peer grouping of anomalies provides additional context for understanding suspicious behavioral activity
- Massively scalable native SaaS application is capable of processing billions of daily events
- Patented unsupervised machine learning and behavioral analytics drives advanced and highly automated threat detection

Key benefits

- Reduces mean time to detect and respond with advanced analytics and machine learning that work right out of the box
- Frees up valuable time that analysts can spend investigating real business threats based on precisely tuned alerts
- Reduces your reliance on expensive hardware and data scientists
- Lowers your organization's risk profile by addressing a wide range of analytics use cases important to business leaders, including insider threats, employee misuse, sophisticated external attacks and more

Provides fast time-to-value

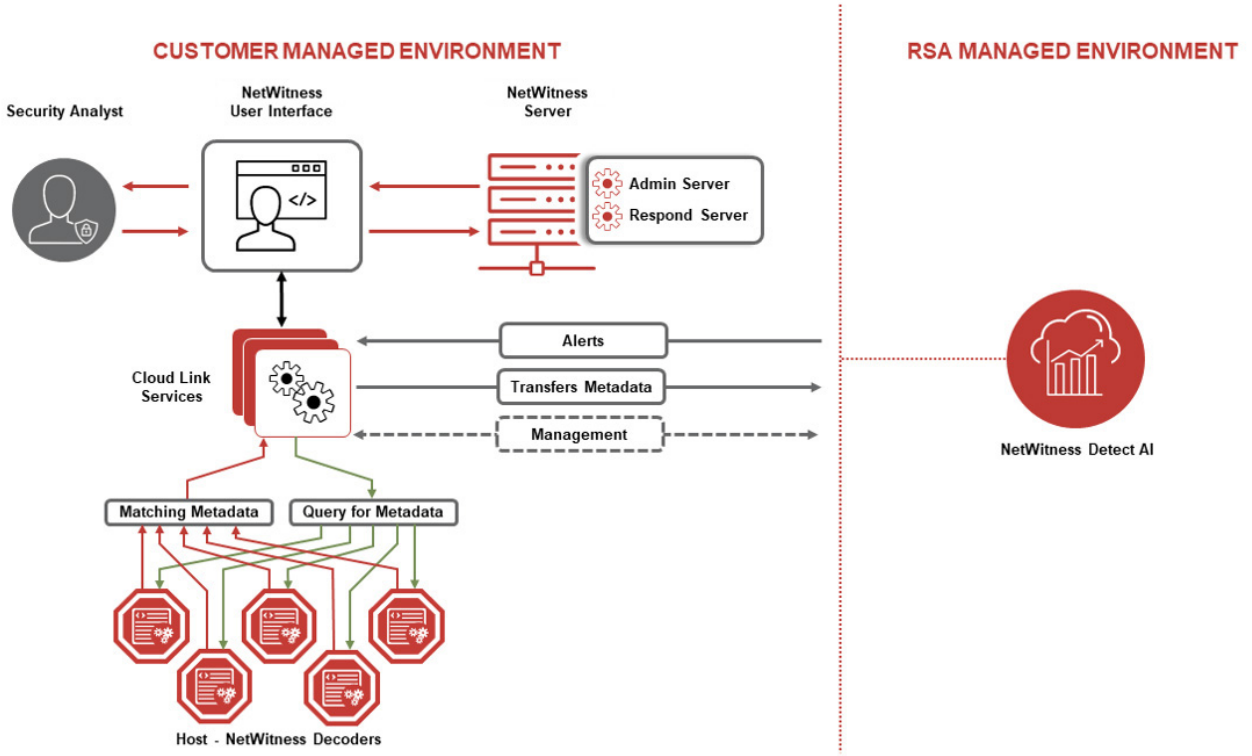
NetWitness Detect AI begins processing data the moment you turn it on. Within hours, it shows baseline behaviors so analysts can quickly understand anomalies. Within days, the system generates meaningful, high-fidelity and actionable alerts.

Zero-touch advanced threat detection for the fastest incident resolution

NetWitness Detect AI is a cloud-native, big-data driven, advanced analytics and machine learning solution, and it's an integral part of the NetWitness Platform. It leverages unsupervised statistical anomaly detection and data science to provide comprehensive, automated detection of unknown threats.

As a cloud-based SaaS solution with native scalability, NetWitness Detect AI delivers fast time-to-value. There's minimal setup, limited infrastructure requirements, and administration is simple. The solution augments your existing security team to provide rapid detection at every step of the attack lifecycle. Its powerful machine learning engine and the breadth of use cases it supports helps organizations quickly identify and decisively respond to unknown threats and unusual behaviors.

NetWitness continuously tunes the machine learning algorithms, allowing NetWitness Detect AI to get smarter the moment you turn it on and reveal anomalous behaviors quickly, accurately and without constantly demanding analysts' attention. NetWitness Detect AI accelerates the full attack investigation lifecycle and leads to more efficient and complete incident response.



This high-level architecture of NetWitness Detect AI demonstrates the data flow and management components between customer and NetWitness environments

Learn more about NetWitness Detect AI at **rsa.com/detect-ai**

NETWITNESS
An RSA Business