

RSA NETWITNESS[®] ENDPOINT

Detect Unknown Threats. Reduce Dwell Time.
Accelerate Response.



KEY CUSTOMER BENEFITS:

- Gain complete visibility into all of your endpoints, regardless of whether they are on or off your network
- Continuously monitor endpoints and receive prioritized alerts in real-time
- Faster root cause analysis reduces time, scope, and cost of incident response
- Drastically reduce dwell time by rapidly detecting and identifying new and unknown threats
- More effective and faster prioritization to address real threats
- Increased resolution rate with reduced time-to-remediation for incidents
- More completely understand the full scope of the attack across endpoints and network with the RSA NetWitness Suite

PRODUCT OVERVIEW

Today's cyberattacks are unparalleled in sophistication and frequency, and the potential attack surface for organizations is only growing. Trusted endpoints no longer reside just within the organization's four secure walls. As workforces grow more mobile, they are increasingly used off-premises on untrusted networks and then brought back into the trusted environment. Endpoints – now more than ever – remain the most vulnerable attack vector, and today's threat actors are more tenacious than ever before.

Now, it's generally not a matter of "if" you'll be compromised, but rather "when", and the "when" more often than not includes threats that are **personalized, complex, and never-seen-before** in the wild. Complicating matters further, security solutions that traditionally rely on signatures or rules, such as antivirus software on endpoints, are simply unprepared for these new, more adaptable unknown threats. When the organization is inevitably compromised, security teams and incident responders quickly discover that they're...

- Unable to get real, deep visibility into all critical endpoint activity surrounding the compromise;
- Facing challenges in actually detecting those hidden, never-seen-before, and targeted threats;
- Confronted with thousands of alerts from traditional security solutions that complicate the quick detection, accurate analysis, and efficient response to the REAL threats to their organization.

The biggest question facing security teams worldwide is **"How do we effectively defend against something that's never been seen before?"**

RSA NetWitness Endpoint answers that question.

RSA NetWitness Endpoint is an endpoint detection and response tool that continuously monitors endpoints to provide deep visibility into and powerful analysis of all behavior and processes on an organization's endpoints. RSA NetWitness Endpoint doesn't require signatures or rules. Instead, leveraging unique endpoint behavioral monitoring and advanced machine learning, RSA NetWitness Endpoint dives deeper into your endpoints to better analyze and identify zero-day, new, and hidden threats that other endpoint security solutions miss entirely. As a result, incident responders and security teams gain unparalleled endpoint visibility allowing them to more quickly detect threats they couldn't see before, drastically reduce threat dwell time, and focus their response more effectively to protect their organizations.

RSA NetWitness Endpoint is a core component of the RSA NetWitness Suite, offering seamless integration with RSA NetWitness Logs and Packets and RSA NetWitness SecOps Manager, which helps SOC and IR teams gain insight into the full scope of an attack across both network and endpoint and receive actionable intelligence that streamlines threat analysis and response.



DEEPER DETECTION TECHNIQUES TO UNCOVER UNKNOWN THREATS

Do you trust your operating system? We don't. That's why RSA NetWitness Endpoint uniquely runs in kernel mode on your endpoints – without the use of signatures – to continuously monitor all processes, executables, and behavior to ensure that anything out of the ordinary is flagged for your security team. Because RSA NetWitness Endpoint doesn't rely on signatures or hashes and, instead, monitors and collects data on **all endpoint activity**, it rapidly detects new, completely unknown, and targeted attacks that other endpoint detection and response solutions miss entirely.

RSA NetWitness Endpoint has the ability to

- Continuously monitor all endpoint activity, allowing full visibility into what's happening on an endpoint – regardless of whether the endpoint is on or off the corporate network.
- Leverage a unique combination of capabilities to delve deep into the inner workings of endpoints and expose anomalous behaviors. RSA NetWitness Endpoint techniques include live memory analysis, direct physical disk inspection, network traffic analysis, and endpoint state assessment.
- Utilize an extremely lightweight endpoint agent to collect full endpoint inventories and profiles within minutes, with no discernible impact to end-user productivity. Endpoint data collection completes rapidly, with all data storage and the bulk of analysis occurring on the RSA NetWitness Endpoint server to ensure data integrity and drastically reduce resource impact.
- Automatically initiate a quick, targeted scan when unknown files, processes, etc. load on an endpoint, record data about every critical action (e.g., file or registry modifications, network connections) surrounding the unknown item, and communicate with the RSA NetWitness Endpoint server for further analysis.

RSA NetWitness Endpoint dives deeper into the endpoint to find those unknown, targeted threats that other solutions miss, enabling faster detection of a wider range of malicious endpoint behavior.

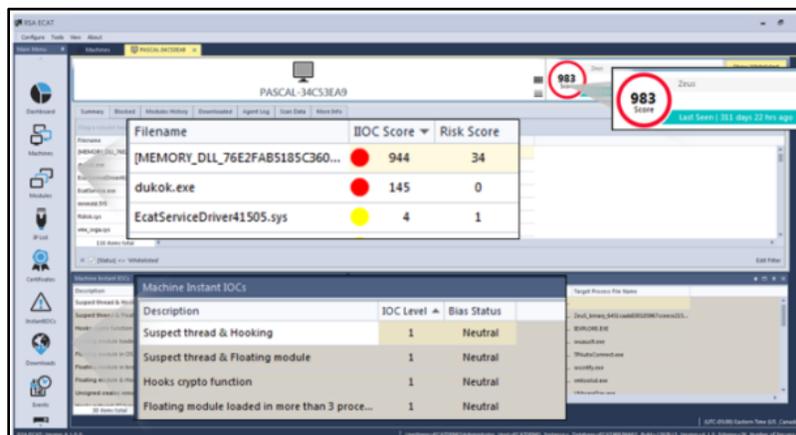


Figure 1 – RSA NetWitness Endpoint Console

QUICKLY IDENTIFY AND UNDERSTAND THREATS AT A DEEPER LEVEL

Typically, a security team is overburdened with more incidents than they can effectively process. When every second counts, it's imperative that the team can identify and prioritize the highest-risk incidents quickly. RSA NetWitness Endpoint helps security teams better understand threats with advanced analytical capabilities that optimize the identification and investigation of incidents.

RSA NetWitness Endpoint can

- Rapidly score and flag suspicious endpoint activity and behavior for further investigation. Utilizing an intelligent risk scoring algorithm that combines advanced machine-learning techniques with a wide array of behavioral indicators of attack and aggregated intelligence, RSA NetWitness Endpoint prioritizes incidents and provides a clear visual indication of the potential threat level of endpoints, helping security teams more easily triage alerts, focus investigations, and optimize their time.
- Drastically reduce incident white noise by comparing the current endpoint to a defined "gold image" and leveraging powerful aggregated whitelisting capabilities delivered by Reversing Labs.

- Conduct multiple checks of file legitimacy to determine if a file is malicious, including checking file certificates and hashes as well as employing OPSWAT Metascan to scan against multiple antivirus and antimalware engines.
- Provide aggregated intelligence from the security experts at RSA and other trusted intelligence sources to help security teams understand and investigate more efficiently.
- Leverage RSA Live Connect for crowdsourced, community-based threat intelligence from peers to identify and respond to threats more quickly.
- Retrieve copies of executable files from the endpoint – both automatically and on an ad hoc basis – for additional analysis. RSA NetWitness Endpoint Server maintains a global repository of all files found, allowing security teams to have all the data they need at their fingertips to reduce investigation time as well as provide added context of *all* machines' behavior related to an attack.
- Easily incorporate YARA rules, import STIX data, create RSA NetWitness Endpoint rules, and permit security analysts to customize any of the 300+ behavioral indicators provided by RSA out-of-the-box to deliver the most customizable experience.

IMPROVE RESPONSE TIME. REDUCE THE IMPACT OF A BREACH.

A critical aspect of effective remediation is understanding how far a targeted attack has spread across your network. RSA NetWitness Endpoint provides this broad visibility and arms security teams with targeted response capabilities to swiftly remediate incidents across all endpoints in the enterprise.

RSA NetWitness Endpoint enables security teams to

- Quickly gather all of the most critical data needed for a forensic investigation. Unlike other solutions, RSA NetWitness Endpoint runs in kernel mode and can easily pull full process and memory dumps, view the Master File Table (MFT), and see all modified and deleted files and registry entries.
- Instantly identify all endpoints infected with any threat, enabling immediate understanding of the scope and breadth of the malware infestation. This allows security teams to respond more effectively and completely eradicate the threat across all infected endpoints.
- Block threats with greater precision on all endpoints. With RSA NetWitness Endpoint, security teams can blacklist malicious files and then block and quarantine them with one action across all infected endpoints in the enterprise. Additionally, the RSA NetWitness Endpoint Agents on all endpoints will remember the blacklisting and prevent future execution on any endpoint.
- Leverage the REST API to send endpoint data to in-house or third-party security solutions and integrate into service management systems or security operations management platforms such as RSA NetWitness SecOps Manager.

RSA NETWITNESS ENDPOINT SOLUTION COMPONENTS

COMPONENT	DESCRIPTION	NOTES
RSA NetWitness Endpoint Agent	Software agent that resides on the endpoint (i.e., server, laptop, desktop, VM, VDIs)	Supported Operating Systems: Windows (XP, Vista, 7, 8, 10) Windows Server (2003 SP2, 2008, 2008 R2, 2012, 2012 R2) Mac OS X (10.8, 10.9, 10.10) Linux (Red Hat Enterprise Linux 6.x, 7.x; CentOS 6.x, 7.x)
RSA NetWitness Endpoint Server	Server used to control and communicate with the agents via the management console. Microsoft SQL Server is required. Multiple server architecture is optional.	Supported versions of Microsoft SQL: Microsoft SQL Server 2008 R2 Microsoft SQL Server 2012
Roaming Agents Relay (RAR)	The RAR is an optional server that provides visibility into and communication with endpoints that are disconnected from a corporate network.	Can be deployed as a cloud service
RSA Live	Threat intelligence delivery system that delivers multiple intelligence feeds from both RSA FirstWatch and the most trusted and reliable providers in the security community.	Requires RSA Live account.
File Reputation Service	Provides access to a large whitelisting database, updated in real-time, to offer the most current file validation information.	Requires RSA Live account.

OPSWAT Metascan	Optional third-party application supported by RSA NetWitness Endpoint, which, when enabled, scans all files downloaded by RSA NetWitness Endpoint against multiple antivirus engines, configurable by administrator.	
YARA Engine	Optional component that allows for static analysis with open-source YARA rules	
RSA NetWitness Endpoint REST API Server	Optional component that allows configuration and usage of the RSA NetWitness Endpoint REST API by customers, partners, and third-party developers.	Installed by default with RSA NetWitness Endpoint Server. Support for JSON and XML data formats

SUPPORT

RSA's world-class global support organization can enhance your security solution with a comprehensive support plan that provides important security alerts, valuable upgrades, and access to expert advice. RSA provides the resources you need to quickly and proactively resolve product-related issues and questions to ensure business continuity. For more information about RSA Support and Services, see the [RSA Support page](#).

Warranty information can be found at <https://community.rsa.com/docs/DOC-40403>.

NEXT STEPS

To learn more, visit Dell.com/DataSecurity or contact us at DataSecurity@Dell.com.