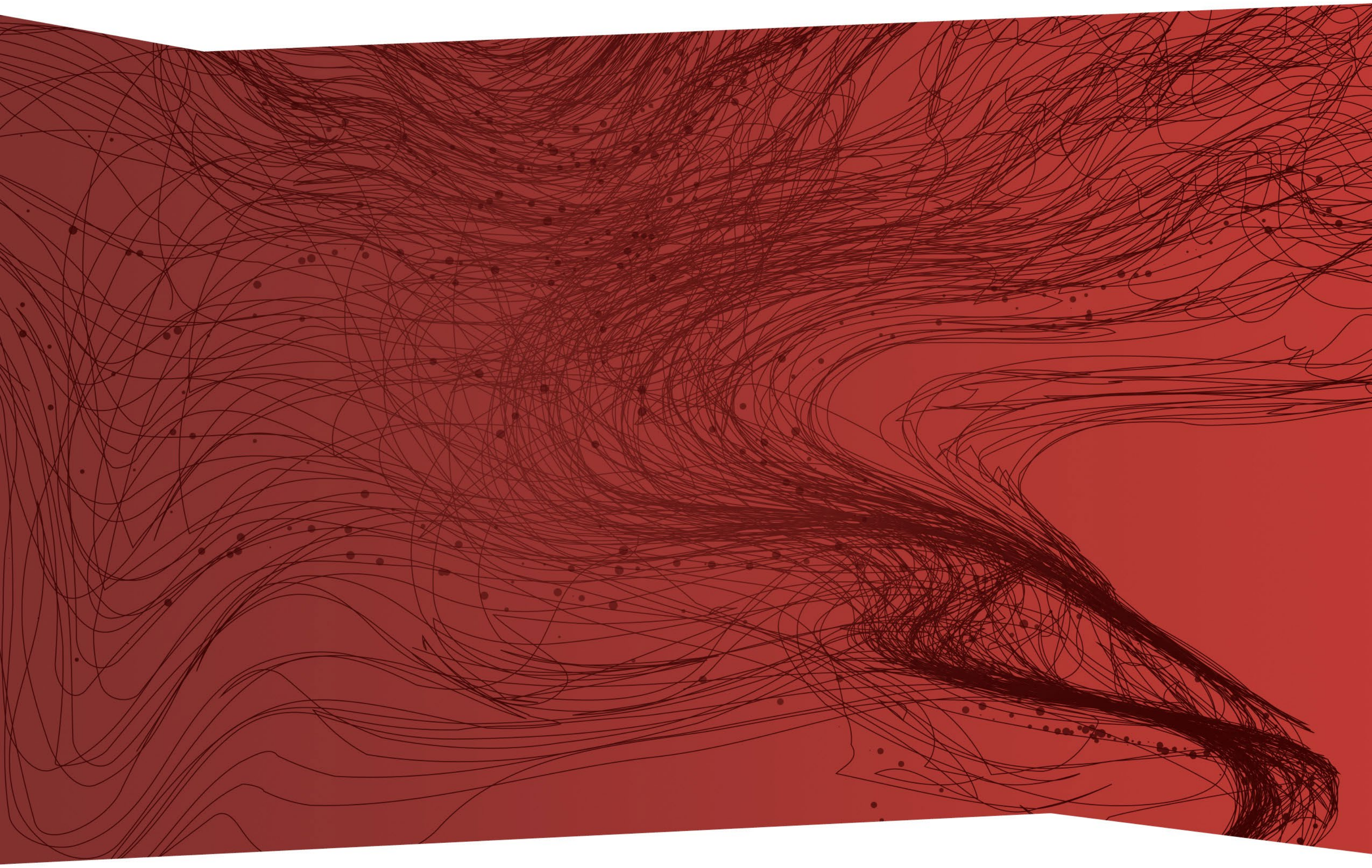


DATA SHEET

# RSA NETWITNESS® ENDPOINT

## DETECT UNKNOWN THREATS. REDUCE DWELL TIME. ACCELERATE RESPONSE.

## KEY CUSTOMER BENEFITS:

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

## 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 are:

- 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 that evaded preventive technology like next-generation antivirus.
- 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 threats on an organization's endpoints. Instead of signatures or rules, it leverages unique, continuous behavioral monitoring and advanced machine learning to dive deeper into endpoints to better analyze and identify zero-day, hidden, and non-malware attacks 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 and offers seamless integration with both RSA NetWitness® Logs and Packets and RSA NetWitness® SecOps Manager. The RSA NetWitness Suite interweaves business context and risk with the most advanced cybersecurity capabilities to help security operations and incident response teams more rapidly respond to the threats that matter the most to the organization and mitigate negative business consequences.

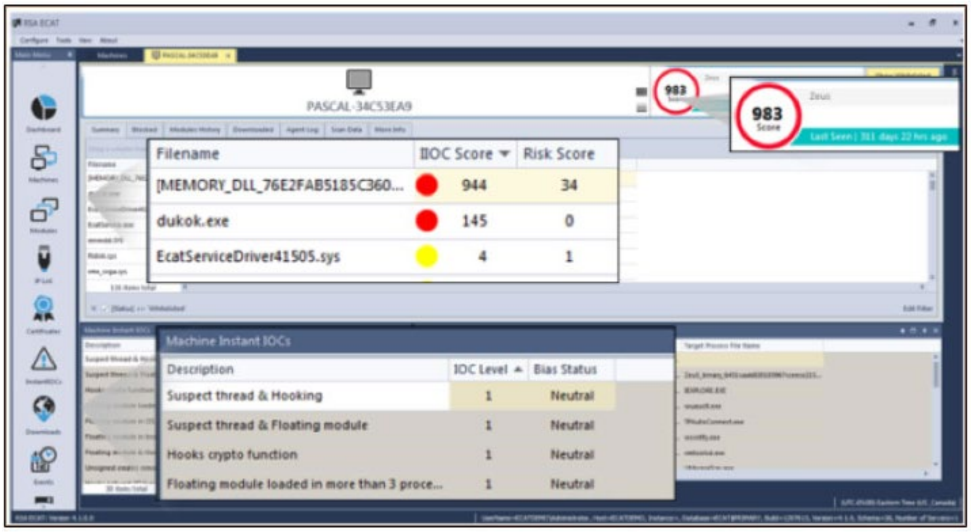
## DEEPER DETECTION TECHNIQUES TO UNCOVER UNKNOWN THREATS

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. RSA NetWitness Endpoint can run alongside existing antivirus or next-generation antivirus products. However, because RSA NetWitness Endpoint doesn't rely on signatures or hashes and, instead, monitors and collects data on ***all endpoint behavior and activity***, it can rapidly detect brand new, unknown, targeted, and non-malware attacks that other endpoint security solutions will miss completely.

**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, suspicious user behavior detection, 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 and more 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 on the endpoint, enabling faster detection of a wider range of malicious behavior.



| Filename | IIOC Score | Risk Score |
|---|---|---|
| [MEMORY_DLL_76E2FAB5185C360... | ● 944 | 34 |
| dukok.exe | ● 145 | 0 |
| EcatServiceDriver41505.sys | ● 4 | 1 |

Machine Instant IOCs

| Description | IOC Level | Bias Status |
|---|---|---|
| Suspect thread & Hooking | 1 | Neutral |
| Suspect thread & Floating module | 1 | Neutral |
| Hooks crypto function | 1 | Neutral |
| Floating module loaded in more than 3 proce... | 1 | Neutral |

*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 threats.

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 for malware, live memory attacks and exploits, PowerShell and "file-less" attacks, and even user-initiated suspicious behaviors along with aggregated threat intelligence, RSA NetWitness Endpoint assesses the threat risk of an endpoint and provides a clear visual indication of that potential endpoint threat level, 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 reputation and 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 Research and other trusted intelligence sources to help security teams understand and investigate more efficiently.

- Leverage RSA Live Connect for crowdsourced, RSA-community-based threat intelligence and hash reputation from peers to aid security analysts in identifying and responding to threats more efficiently.
- Retrieve copies of executable files from the endpoint – both automatically and on an ad hoc basis – for additional analysis. RSA NetWitness Endpoint Server preserves forensic artifact integrity by maintaining 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.
- Easily pivot back and forth with RSA NetWitness Logs and Packets to empower security analysts to dive deeper into all data sources across endpoints, networks, and the cloud and, ultimately, better understand the full scope of an attack.
- Transform deep endpoint visibility into powerful metadata, used by ALL RSA NetWitness Suite components, that is seamlessly incorporated into the Investigate and Respond workflows of the Suite to streamline analyst investigations. By using a common metadata language across endpoint, logs, and packets, analysts can more easily gain deeper insights into everything happening in their environment, allowing them to investigate more effortlessly, and respond more definitively.

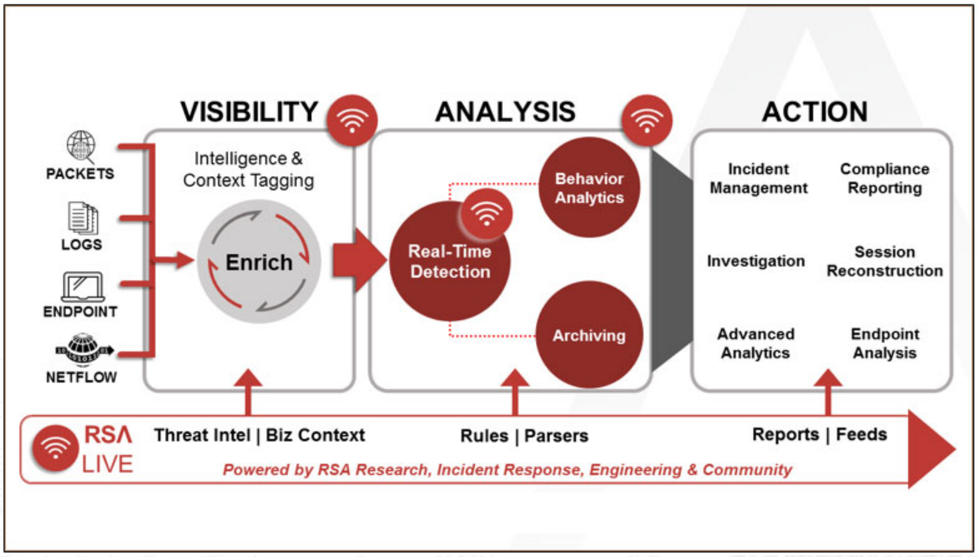


*Figure 2 – Overview of RSA NetWitness Suite, with both RSA NetWitness Endpoint and RSA NetWitness Logs and Packets*

## 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.
- Isolate an infected endpoint on the network via Machine Containment, allowing the security analyst to safely investigate and better understand the nature of the attack on the endpoint in a live environment (instead of an easily-thwarted sandbox environment) without the risk of lateral movement or continued communication with the threat actor.
- 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.
- Integrate RSA NetWitness Endpoint and endpoint data along with RSA NetWitness Logs and Packets (and other third-party security solutions) into RSA NetWitness SecOps Manager for optimized management of all security operations.

## 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:<br>**Windows** XP, Vista, 7, 8, 10.x<br>**Windows Server** 2003 SP2, 2008, 2008 R2, 2012, 2012 R2, 2016<br>**Mac** 10.8 – 10.13 (High Sierra)<br>**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:**<br>Microsoft SQL Server 2008 R2<br>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 Research and the most trusted and reliable providers in the security community. | Requires RSA Live account. |
| RSA Live Connect | Opt-in, community-based threat intelligence sharing platform that provides access to metrics on hash reputation, dates, and proportions of decisions made by security analysts in the RSA NetWitness Endpoint 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

For more information about RSA NetWitness Endpoint, visit https://www.rsa.com/en-us/products-services/threat-detection-and-response/netwitness-endpoint or contact your RSA Channel Account Manager or Authorized Distributor.

Published in the USA 07/17 DATA SHEET | H14904.4

Dell EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.