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.

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 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.

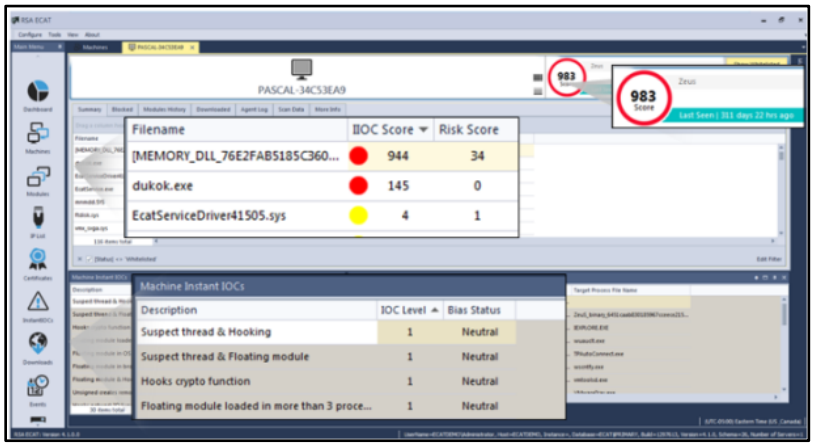

Figure 1 – RSA NetWitness Endpoint Console

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. Utilizing an intelligent risk scoring algorithm that combines advanced machine-learning techniques with a wide array of behavioral indicators of attack, powerful aggregated whitelisting and blacklisting capabilities and curated, real-time intelligence from RSA Experts, the intelligence community, and the RSA community, 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.

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 quickly gathers all of the most critical data needed for a forensic investigation and instantly identifies 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. 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. Integrations with the rest of the RSA NetWitness Suite allow organizations to see and understand the full scope of an attack across network and endpoint telemetry and then optimize their security operations for response.

RSA NETWITNESS ENDPOINT – RESPOND IN MINUTES, NOT MONTHS

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