RSA

SOLUTION BRIEF

RSA NetWitness® Platform for Threat Defense

Overview

Attacks are constantly evolving to evade preventative controls, penetrate the perimeter and infect an organization's assets. Security operations teams lack the complete, visibility-enhancing and automated technology to both detect and respond to today's advanced threats. Instead, they have silos of information, data collection and data storage systems bolted together that create more work and complexity for analysts. Because of this bolted-together system, security operations teams are increasingly overwhelmed with more systems, more screens and more alerts than they have time to view.

The layered defense strategy that organizations have taken is over-reliant on logs and preventative controls. Since companies have no choice but to allow some traffic to pass through all layers of defense in order to do business, traffic needs to flow through preventative controls. Logs only tell part of the story of what traffic makes it through. Log-centric SIEMs can only report on what the preventative controls have identified. As organizations add more preventative controls, the amount of data and events generated can overwhelm even the most mature security teams. This leads to even more noise, increasing the likelihood that the signal (clues about an attack) will get lost.

Malware and other threats that have gone inside the network without being detected by preventative controls and have managed to infect assets, force security operations teams to experience long dwell times before noticing an intrusion and acting on it. This gives attackers time to exfiltrate data, and can cause major business damage.

Change in mindset required

Attack prevention strategies alone are futile, and relying on one-time security inspection gating and allow-or-block decisions doesn't work. When bad things without known signatures are let in past these one-time inspection controls (most notably antivirus, intrusion prevention systems and secure web gateways) or rule-based detection technologies, the executable or network connection is assumed to be good. Indeed, if it was malicious, once let in, most enterprises lack

the visibility to detect and respond to the breach, allowing the bad guys to infect systems, grab credentials and move laterally to other systems.

This is a significant change in mindset for information security. If you assume bad entities will inevitably get past one-time gating assessments of threat prevention, then the goal of threat defense at this point must shift from block-or-allow decisions to continuous visibility and analysis across the network and on the endpoint for the rapid detection and response if and when something malicious happens—minimizing the attacker's ability to infect other systems and cause damage.

RSA NetWitness Platform for threat defense

RSA NetWitness Platform for threat defense enables organizations to detect threats that have bypassed preventative controls by leveraging data far beyond log-centric SIEMs, from across the network and deep on endpoints. Real-time visibility into network traffic across all internal (east-west), internet-bound (north-south), virtual infrastructure and cloud computing environments, paired with deep, process-level endpoint visibility, enables RSA NetWitness Platform for threat defense to detect intrusions as they are happening. Multiple types of behavior analytics detect anomalies across the network, suspicious activities of machines and users, as well as abnormal activities across applications—no matter where they reside. Once detected, a prioritized and automated response to the full scope of the attack helps defend against today's and tomorrow's threats.

RSA NetWitness Platform for threat defense key capabilities include:

- **Single, unified platform for all your data**
  This is the only solution that combines threat detection analytics and automated response with network and endpoint telemetry, investigation and threat intelligence capabilities to defend against threats.

- **Integrated threat and business context**
  By adding business context to analysis, organizations can prioritize threats based on the potential impact to their businesses. In addition, intelligence gathered from industry research and crowdsourced from our customer base and the organization's own data is fully aggregated and operationalized at ingestion to better detect the unknowns that are prime indicators of compromise.

- **Automated user behavior analytics**
  Our unique Advanced Analytics Engine looks for potentially malicious issues across disparate data sets as well as correlates data across full network packets and endpoints—all prime attack vectors for today's advanced threats. By analyzing all these data sources together and searching for attack behaviors, and applying user and entity behavior analytics (UEBA), RSA NetWitness Platform can dramatically speed threat detection and response. RSA NetWitness UEBA Essentials extends the power of the RSA NetWitness Advanced SIEM by targeting threats that manifest themselves in user and entity behavior.

- **Rapid investigations**
  The RSA NetWitness Platform for threat defense provides an advanced analyst workbench to triage alerts and incidents including an interface designed specifically for security investigations. Utilizing deep insight into data from across the infrastructure allows analysts to natively and visually reconstruct a network attack or data exfiltration in its entirety. The platform empowers analysts to connect incidents over time in order to expose and better understand the full scope of an attack.

- **Automation and orchestration**
  Automation and orchestration enables security operations center (SOC) analysts to have consistent, transparent and documented threat investigations and threat hunting capabilities by leveraging playbookdriven automated response actions, automatic detection and machinelearning powered insights for quicker resolution and better SOC efficiency.

- **Flexible, scalable architecture**
  By offering a wide range of flexible deployment options, the RSA NetWitness Platform for threat defense can scale incrementally according to an organization's needs and security priorities. Whether deployed as a single appliance or dozens, partial or fully virtualized deployments, onpremises or in the cloud, RSA NetWitness Platform for threat defense can support it all.

- **End-to-End security operations**
  The RSA NetWitness Platform for threat defense is the only platform that unifies network telemetry and endpoint telemetry along with advanced threat intelligence and SOC runbooks and management to fully operationalize security operations programs from end to end.

RSA NetWitness Platform for threat defense provides organizations the capability to analyze and alert on threats that have bypassed their preventative controls as they cross their networks and attempt to infect their endpoints with more accurate and rapid detection and automated response.

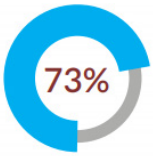
RSA NetWitness Platform for threat defense utilizes intelligent metadata from across your network and endpoints to identify anomalies in behavior. This exposes hidden and unknown attacker behaviors, such as remote access tools, hidden tunnels, backdoors, credential abuse and lateral movement.

Through a unique combination of network traffic analysis, behavioral analysis, endpoint analysis, data science techniques and threat intelligence, RSA NetWitness Platform for threat defense detects known and unknown attacks and automates response. It exposes the full scope of an attack by providing unparalleled network and endpoint visibility, connecting incidents over time and delivering deeper insights from both automation and machine learning.

Detecting intrusions is a critical requirement of any security operations team. It is time that the defense is armed to fight back against today's attack. That is where RSA NetWitness Platform for threat defense comes in. See every move the intruder makes—from when they cross preventative controls to their attempts in infecting your assets.

RSA NetWitness Platform for threat defense is the threat detection and response solution that gives you the fastest path to fully understand, then ultimately eradicate, threats that have bypassed preventative controls prior to business impact, regardless of the attack vector.

- Know that you have visibility across all network traffic and endpoint process in order to detect and respond to threats before they can damage the business
- Find active intrusions inside your network as they attempt to infect endpoints.
- Have confidence that you have the right understanding of the full scope of the threat.
- Persistently track threats across all phases of attacks, without blind spots.
- Minimize business impact by quickly responding and automatically taking action.
- Create a more efficient and effective security team—without adding staff.



of organizations rate their threat detection capabilities as inadequate

Source:
RSA Cybersecurity Poverty Index 2016

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.