OVERVIEW

Information security has been a major challenge for organizations since the dawn of the digital era. Today, however, a number of factors have combined to make security more challenging than ever before:

- The rapid industry transition to virtualized and cloud-based infrastructure has effectively broken the traditional perimeter-based security approach. Years of security best practices are swept aside, as data and processes can now reside anywhere, inside or outside the organization.
- Attackers are employing tools, techniques and procedures (TTPs) that are more sophisticated and impactful than ever before. No longer the purview of “script kiddies” and amateurs, cyber threats have been commercialized for mass use, most recently taking advantage of exploits originating in nation-state intelligence organizations.
- Business leadership no longer regards cybersecurity as a “hygiene” activity to be left to the IT department. Breaches and data leaks are causing lasting financial and reputational harm to organizations in every region and industry, getting the attention of C-suite and board members. Managing cyber risk has been elevated to a core business responsibility, not just an IT problem.

RSA recognizes and understands these challenges, and offers evolved SIEM and threat defense tools and services that help organizations rapidly detect and respond to threats in this continuously evolving environment.

RSA NETWITNESS® PLATFORM

The RSA NetWitness Platform provides pervasive visibility across a modern IT infrastructure, enabling better and faster detection of security incidents, with full automation and orchestration capabilities to investigate and respond efficiently. RSA NetWitness Platform takes security “beyond SIEM,” extending the traditional log-centric, compliance-focused approach to security to include state-of-the-art threat analytics, including user and entity behavior analytics (UEBA), and visibility into cloud, network and endpoints.

Figure 1: RSA NetWitness Platform Architecture
RSA NetWitness Logs and RSA NetWitness Network provide security visibility across your infrastructure, from on-premises data centers to public cloud services. It captures real-time data from logs and network packets, as well as NetFlow data, and applies deep analytics, machine learning, UEBA and threat intelligence. Correlating alerts and indicators of compromise (IoCs) across an organization’s IT infrastructure empowers security analysts to detect and recognize threats before the attacker can cause the intended damage.

RSA NetWitness Endpoint provides visibility into IT endpoints at the user and kernel level, to flag anomalous activity, provide machine/endpoint suspect scores and block/quarantine malicious processes. It provides its own free-standing analytics server, or endpoint data can be integrated with RSA NetWitness Logs & Packets to provide unmatched visibility across your IT infrastructure. RSA also makes a free RSA Endpoint Insights agent available for licensed RSA NetWitness Platform customers, to offer endpoint data collection including Windows logs.

RSA NetWitness Orchestrator is a comprehensive security operation and automation technology that combines full case management, intelligent automation and orchestration, and collaborative investigation capabilities. RSA NetWitness Orchestrator enables security operations center (SOC) analysts to have consistent, transparent and documented threat investigation and threat-hunting capabilities by leveraging playbook-driven automated response actions, automatic detection and machine-learning powered insights for quicker resolution and better SOC efficiency. RSA NetWitness Orchestrator acts as the connective tissue—not only for the RSA NetWitness Platform but across a SOC’s entire security arsenal.

RSA NetWitness UEBA Essentials extends the breadth of analytics to identify advanced threats. Leveraging user, network and endpoint behavioral profiling powered by static rules, advanced correlation, machine learning intelligence and statistical analytics, RSA UEBA Essentials identifies deviations from normal user behaviors. Attack vectors such as compromised credentials, abuse or misuse of privileged user accounts, insider threat, brute force and account manipulation are among detection indicators included. RSA NetWitness UEBA Essentials is available via RSA Live to all RSA NetWitness Platform customers, and extend the analytic capabilities that empower RSA customers to rapidly identify today’s known and unknown threats.
RSA CYBERSECURITY SERVICES
In addition to market-leading security technology, RSA offers advanced professional services to help organizations design effective security systems and processes, and to respond to security incidents including data breaches.

RSA services utilize RSA NetWitness Platform (and other) tools when performing customer engagements. While RSA NetWitness Platform provides a powerful toolset for RSA professional services, their use of the platform creates a virtuous feedback loop, where continuous encounters with real-world threats inform both product development and threat intelligence activities.

RSA ADVANCED CYBER DEFENSE (ACD) PRACTICE
RSA Advanced Cyber Defense (ACD) Practice provides services to assess, design and implement an organization’s SOC strategy. ACD services focus on readiness and resilience, helping customers implement world-class security.

RSA INCIDENT RESPONSE (IR) PRACTICE
RSA Incident Response (IR) Practice provides services to help organizations detect and investigate incidents and breaches. IR services are designed to identify root causes and guide customers in developing containment and remediation plans.

VISIBILITY, PRODUCTIVITY AND BUSINESS-DRIVEN SECURITY
What makes RSA NetWitness Platform different from other security platforms? There are several factors, including RSA’s 36 years of leadership as a technology security company.

The power of RSA NetWitness Platform delivers advantages in three critical areas:

VISIBILITY
To effectively combat sophisticated attacks, you need pervasive visibility across both data sources (packets, NetFlow and logs) and threat vectors (endpoint, network and virtualized/cloud-based infrastructure).

Modern IT infrastructures simply don’t follow the classic data center model. Virtualization and cloud strategies create real benefits, including lower costs and higher flexibility. Unfortunately, these things tend to make security much more challenging. It’s a dynamic tension that falls upon the SOC to manage.

RSA NetWitness provides the needed visibility into all components of your IT infrastructure, not just the traditional parts. Unlike companies that focus on logs, or network, or endpoints, or cloud, RSA NetWitness sees the full environment.

Why is this so important? Modern sophisticated threats are designed precisely to defeat traditional, perimeter-based defenses. They attack different resources and hide among normal traffic. Even if a risk event is
triggered in one control, it’s increasingly likely that an attack features the use of multiple data sources and threat vectors.

Pervasive visibility is the raw material for effective threat hunting. This allows analysts to see the full scope of an attack, and to respond decisively.

**PRODUCTIVITY**

RSA NetWitness Platform is designed to optimize the productivity of SOC personnel of all skill levels, from new security analysts to the most experienced threat hunters. It starts with the pervasive visibility discussed above; that’s the raw material upon which a world-class SOC is based.

The paradox is that collecting so much data exacerbates a primary problem of modern IT: the ever-increasing amount of data generated by applications and security controls makes it nearly impossible to find the threats hiding within.

RSA NetWitness Platform solves this problem with powerful analytic capabilities. Its modular architecture handles massive amounts of raw data, enriching it with security context at time of capture. It then applies a set of sophisticated analysis tools, including machine learning, UEBA and public as well as RSA community threat intelligence. This process correlates disparate events and alerts into discrete investigations, automatically scoring each according to the likelihood that they represent an attack or exploit.

This empowers security analysts to do their jobs better and faster. Level one analysts can quickly work through the prioritized investigation queue, distinguishing between benign alerts and true threats. They can tune the system to ignore alerts and processes that generate false positives, greatly increasing productivity.

*Figure 2: RSA NetWitness Platform "Respond" Visualization Screen*
Threat hunters become much more productive as well, with a rich toolset and an intuitive user experience that presents the information visually, and lets them drill down or pivot on any data point. In this manner, threat hunters can quickly evaluate and understand the full scope of an attack, and respond with confidence.

As a byproduct of its threat detection and response capabilities, RSA NetWitness Platform enables security personnel to report on all security activity, both in the form of standard compliance reports as well as incident response outcomes. With governments worldwide enacting laws requiring breach notification and risk evaluation, having the power to show exactly what an attack exposed can be the difference between a public breach announcement and a contained incident.

RSA NetWitness Orchestrator is a force multiplier for SOCs to standardize, scale, measure and continuously adopt security operations in an ever-expanding threat landscape environment. It automates repetitive incident response tasks, adds context-rich metadata and empowers security analysts to respond faster with higher efficiency and reduce MTTR to a compromise.

BUSINESS-DRIVEN SECURITY
The focus on visibility and productivity makes RSA NetWitness Platform a great choice for any organization looking to deploy a world-class threat detection and response capability. Business context is the third major differentiator.

The constant drumbeat of publicly exposed exploits and breaches makes it clear how expensive and damaging they can be. Business leaders now understand that IT risk is one of the most critical risks to be managed.

RSA believes that the most effective security strategy is business-driven. RSA NetWitness Platform reflects this by uniting business risk and IT risk with a common language and framework, and integrating business risk data into the threat detection process.

For example, RSA NetWitness Platform features the ability to integrate asset criticality data from various sources including RSA Archer®. Good risk management leverages the fact that a CISO’s laptop is more critical to an organization than a web server that hosts a company’s cafeteria menus. By integrating this type of risk-based assessment into the data being fed through the analytics engine, risk scores can reflect both the threat being seen and its effect on the organization if it succeeds.

This approach provides the bridge to the long-standing problem that IT and risk teams don’t typically collaborate closely. RSA NetWitness Platform automates the process and puts focus on the threats that carry real business risk.

There are additional benefits to a business-driven approach, because it opens up the threat detection and response data set to drive other IT controls. For
example, RSA NetWitness Platform can use data to trigger identity platforms such as RSA SecurID®. If unusual login or data transfer activity is detected from a particular user account, indicating possible credential compromise, RSA NetWitness Platform will be able to command the identity platform to activate step-up authentication. Any malicious activity is stopped in its tracks, while legitimate use is not affected.

SUMMARY
Organizations are experiencing a rapidly changing threat environment, and they need tools and services that can keep up with the changes. RSA NetWitness Platform is designed to offer the maximum amount of visibility, with automated analysis and prioritization, and in context of the real business risk of a threat. In this way, RSA NetWitness users can be sure they are seeing, and responding to, the threats that matter to their organizations.

For more information about RSA NetWitness Platform, visit rsa.com/DoMore or contact your RSA Channel Account Manager or Authorized Distributor.