SOLUTION BRIEF

RSA NETWITNESS® PLATFORM

OVERVIEW OF CAPABILITIES FOR FEDERAL AGENCIES

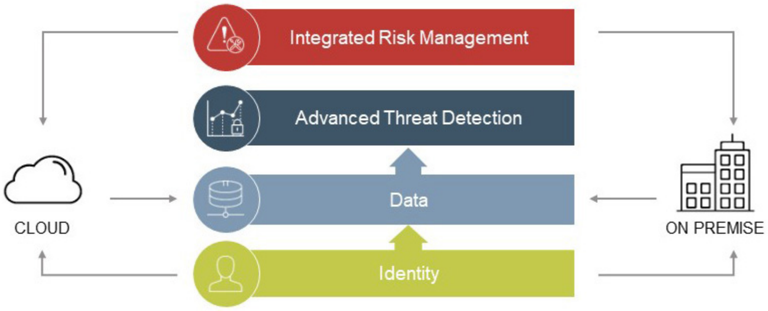


Figure 1. RSA in Action

Federal security teams need to evolve to stay in front of attackers and the latest threats, but in recent years this has become much more difficult. Attackers continue to advance and use sophisticated techniques to infiltrate government systems. Our adversaries spend significant resources performing reconnaissance to learn about Federal IT. They use this knowledge to develop techniques specifically designed to bypass the security tools being used.

Tools, Tactics and Procedures (TTPs) are the ways the attackers work to target, exploit and compromise organizations. In recent years, attacker TTPs have become more sophisticated, mimicking normal user behavior, making them very hard to detect through preventative, perimeter based security controls. The NIST Cyber Security Framework has recognized this reality and established as best practice a better balance across prevention ("Protect") and Detection and Response as the basis for advanced threat management.

RSA NetWitness aligns with this best practice, providing pervasive visibility with real-time behavior analytics to detect and investigate the sophisticated attacker TTPs. It delivers capabilities across:

- Data Sources – Full Packet Capture, NetFlow and Logs
- Threat Vectors – Endpoint, Network and Cloud
- Analytics Engines – User and Entity Behavioral Analytics (UEBA)
- SOC Orchestration – Orchestration and Automation (O&A)

The unique RSA NetWitness architecture captures and enriches data sources with security context in real-time. Additionally, threat intelligence is applied to the enriched data to identify high risk indicators as APT domains, suspicious proxies or malicious networks. This method of processing large data sources in real-time provides analysts with security insight into their entire environment; on-premise to cloud.

Analysts can now detect and investigate sophisticated attacks and truly understand the attacker TTPs. RSA NetWitness captures full network packet data. This means an attack can be completely reconstructed by your security operators – giving them the insight they need to both understand the attacker TTPs and implement an effective remediation plan. RSA helps you stop your agency's adversaries from achieving their objectives.

NETWORK MONITORING AND FORENSICS

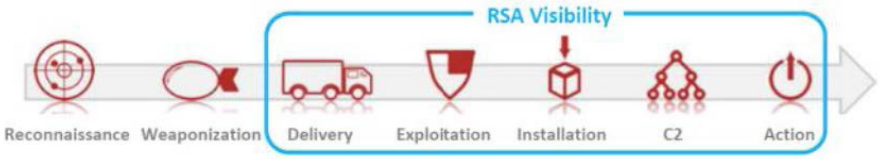
RSA NetWitness captures and enriches full network packet data alongside other data types, such as logs, NetFlow and endpoint. It processes the data types at time of capture as follows:

- Data enrichment – Associates normalized and intuitive metadata to raw data so the security analyst can focus on the security investigation instead of data interpretation.
- Apply threat intelligence – Threat intelligence is applied and correlated to the raw data at time of capture to quickly identify sophisticated attacks early.
- Parse and Sessionize Raw Packet Data – Raw packet data is parsed and sessionized at capture time so it's faster to retrieve and reconstruct the event during an investigation.

The ability to process network data in real-time enables agency security operations teams to detect malicious activity earlier in a breach event. IT security teams will also be able to investigate and remediate incidents both more effectively and more rapidly.

RSA VISIBILITY

By using RSA NetWitness, a security operations team will have full visibility across the kill chain as shown below.



THE EVOLVED SIEM

SIEM solutions have been around for many years and they were designed primarily for two objectives:

1. Collect, analyze, report and store log data from hosts, applications and security devices to support security policy compliance management and regulatory compliance initiatives
2. Process and correlate – in real time – event data from security devices, network devices and systems to identify security issues that pose the biggest risk to an organization

While most SIEM solutions have met objective number 1, a large majority of these solutions struggle to meet objective number 2. These SIEM solutions do not have the scale and real-time analytics capabilities for identifying issues that can compromise an organization before an attacker achieves their objective.

RSA NetWitness goes beyond the baseline SIEM capabilities. With scale and analytic capabilities, RSA NetWitness will spot sophisticated attacks in real-time. Additionally, the unique correlation across logs, packets, NetFlow and endpoint enables analysts to comprehensively investigate and reconstruct the event. RSA NetWitness UEBA provides comprehensive detection for unknown threats based on behavior, without the need for analyst tuning. RSA NetWitness Orchestrator is an intelligence-driven security operations platform that gives teams the ability to leverage threat intelligence, automation, and orchestration directly from one platform.

This means that security analysts can investigate the attacker TTPs at each stage of the cyber kill chain:

- **Delivery** – Targeted e-mail attachment, embedded links
- **Exploitation** – Opening of targeted malware of the endpoint, installation and hooking into the system
- **Command and Control (C2)** – Malware beaconing
- **Action** – Data exfiltration, lateral movement, disruption

Attacker TTPs are fully reconstructed with RSA NetWitness, helping security operations teams deploy and execute an effective remediation.

CORRELATE, DETECT AND RESPOND IN REAL TIME

RSA NetWitness provides a powerful analytics and alerting engine that enables correlation across multiple event types. It can ingest and analyze metadata from log, packet, NetFlow, and endpoint sources. This can happen with rules delivered out of the box, by creating custom rules using the underlying event processing language, or using the rule builder wizard. This capability helps analysts gain visibility and alert on the attacker TTPs as they move across the kill chain.

The real-time behavioral analytics engine can automate detection of attacker TTPs early in the attack lifecycle. RSA NetWitness® UEBA is a purpose-built, big data-driven, user and entity behavior analytics solution integrated as a central part of the RSA NetWitness Platform. By leveraging unsupervised machine-learning algorithms, across a large breadth of use cases, RSA NetWitness UEBA provides comprehensive detection for unknown threats based on behavior, without the need for analyst tuning.

Let's look at how this plays out in an attack scenario. RSA NetWitness helps operators correlate a series of attacker actions and a combination of anomalous activities by users and other entities as possible leading indicators of Command and Control (C2) communications. This requires further investigation and ultimately a defensive activity (or counter strike) to stop the attacker. In this scenario, RSA NetWitness automates C2 detection by accessing the right data, profiling attacker TTPs and detecting anomalies utilizing behavior analytics.

Say an attack includes efforts by the adversary to move laterally in an environment: RSA NetWitness can automatically detect this activity too. Credential-related monitoring activity (e.g.: suspicious login activity and explicit logins) can help your agency detect and prosecute this harmful activity.

Once alerts are triggered, the RSA NetWitness Orchestrator provides the response workflow to assign, triage, investigate and remediate the incident.

SECURITY OPERATIONS ORCHESTRATION

A Security Operations Center (SOC) is comprised of people, process and technology. Effective orchestration of people, process and technology increases the effectiveness of the overall SOC program. Investing in technology and considering how the three aspects of the SOC work together is of fundamental importance. Orchestration and framework-based benchmarking can increase the return on investment and maximize the value of resources in a SOC implementation, reducing the time taken to respond to incidents.

RSA NetWitness Orchestrator is an intelligence-driven security operations platform that gives teams the ability to leverage threat intelligence, automation, and orchestration directly from one platform. The RSA NetWitness Orchestrator is centered on the idea that intelligence and operations are built on a mutually beneficial, cyclical relationship. Automation and orchestration informed by threat intelligence makes your pre-existing technology investments and your entire security team, including threat intel, security operations, and incident response professionals, more efficient and more effective.

By leveraging RSA NetWitness Orchestrator, your agency can be sure that your SOC is leveraging advanced technology to drive an effective, predictable and consistent process for threat detection and response.

ABOUT RSA

RSA Security Solutions help organizations reduce the risks of operating in a digital world. Through visibility, insights, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, reduce the mission risk associated with IP theft, fraud and cybercrime.

For more information about RSA, please go to rsa.com.

ARCHITECTURE

The RSA NetWitness architecture is designed so that customers get security insight in real time when detecting and investigating incidents. As such, at capture time, data sources are sessionized and security enriched at wire speeds.

Additionally, analytics such as behavior analysis are performed as streams of data sources are captured in real time. This means that events are being analyzed in real time, speeding the detection and alerting of anomalous activities.

From an investigation perspective, retrieval and reconstruction of sessions is also accelerated as the raw data is parsed and indexed. This allows security analysts to retrieve the raw data quickly and reconstruct sessions.

The architecture consists of three functional components: capture, analysis and server. The architecture is modular to allow agencies to scale the RSA NetWitness deployment based on capture or analysis performance requirements. RSA NetWitness can be deployed in both physical and virtual environments.

RSA