RSA NETWITNESS®
LOGS & PACKETS

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

Today’s threat actors from criminals to state actors continue to challenge Security Information and Event Management (SIEM) platforms. Meeting the increasingly sophisticated security demands of most enterprises is complicated by shortages of trained security staff. Threat actors have learned how to evade most static rules-based security parameters and penetrate perimeter-based security. As threat actors “live off the land” plotting the perfect moment to attack, SIEMs must detect all anomalies and access the risk – a nearly impossible task. Most SIEMs were designed to meet specific compliance and reporting requirements and not as analytical engines. Analysts are overwhelmed by the sheer volume of alerts from their SIEMS. Security operations team are looking for alternatives to prioritize alerts and assure that they are focusing on the most relevant alerts.

RSA NetWitness Logs and Packets goes beyond baseline SIEM capabilities. Designed for scale and heavy analytic loads, RSA NetWitness Logs and Packets will spot sophisticated attacks and will prioritize alerts.

With real-time sessionized data capture, indexing and correlation capabilities that can be extended across metadata from logs, packets, NetFlow and endpoints, The RSA NetWitness Suite assures that analysts can comprehensively investigate and reconstruct events (including email, websites and more) to understand the complete scope of an attack and reduce the business impact of attacks.

INVESTIGATION: SPEED AND VISIBILITY

The incredible speed in the RSA NetWitness analytics engine is delivered by the normalizing of events with the platform's log and packet parsing technology. The RSA NetWitness database provides faster access to data thanks to the unique metadata model. Parsers extract metadata from either logs or packet data and index the values under a set of common indexed meta keys. Parsers are available Out of the Box (OOTB) with the option for customers to create and/or edit their own. The parsers, feeds and application rules that process traffic generate metadata about the structure of the data and extract values from the individual sessions that can be searched for efficiently. This differs from traditional IDS/IPS solutions in that it is possible to find new unknown malicious activity compared to only finding previously identified malicious activity.

Relevant metadata is indexed, and any unparsed logs are “tokenized” and indexed to allow for rapid searching. It is possible to configure and selectively manage retention of raw and metadata. Short-term retention provides extremely fast access to the data. Longer-term retention allows for cost-effective storage while still providing indexed access for compliance purposes.

RSA NetWitness analytics engine enriches certain metadata with security and business context to create over 200 metadata keys which is much more than the typical SIEM. Through a powerful combination of Feeds, app rules
and parsers, and behavior analysis we can drive the creation of meaningful enriched metadata keys such as the Indicators of Compromise. The color-coded, highlighted, indexed metadata is why analysts are able to quickly detect threats, investigate the details and respond with confidence.

RSA NetWitness Logs and Packets data model delivers breath of visibility which facilitates speed of investigation. A consistent and intuitive workflow for analysts of all levels for incident response activities helps analysts make the right decisions.

WHY METADATA MATTERS
RSA NetWitness Logs and Packets captures and enriches full network packet data along with other data sources and creates a uniform metadata model across all data types. This is what delivers speed and visibility. RSA patented technology delivers differentiated speed for analysis by creating valuable metadata as follows at capture time:

- **Sessionize**: Sessionize raw packet data for all network traffic up to Layer 7 so it is faster to retrieve and reconstruct events if needed during the investigation stage.
- **Parse**: Extract the key elements from logs and packets. Associates raw data to normalized data so the security analyst can focus on the security investigation instead of data interpretation.
- **Data Enrichment**: Add risk and/or business context to each session.
- **Threat Intelligence**: Apply threat intelligence from multiple sources including RSA LIVE and correlate to the metadata at the time of capture to speed identification of sophisticated threat.
- **Indexing**: after indexing the result is a security focused custom database which accelerates analysis.

COMMAND AND CONTROL (C2) DETECTION
Command and control (C2) communications are active elements in most forms of malware and advanced threats. After establishing an initial foothold, lateral movement provides flexibility so that hackers can “live off the land” and expand their footprint. C2 activity exposes advanced malware activity. A threat actor can hide as long as they don’t try and move around the enterprise but once they do – they are visible and trackable. Early detection of lateral movement can expose threat actors before they can expand their foothold within the enterprise as they attempt to exploit vulnerabilities.

- **C2 detection is available for either or both logs and packets within the RSA NetWitness Suite with the Event Stream Analysis (ESA) modules.**
- **Rules combined with machine learning facilitates the identification and detection rates.**
RSA NetWitness Logs and Packets automates C2 detection across both logs and packets activity by having access to the right data, profiling attacker’s behavior and detecting anomalies utilizing machine learning.

**CONTEXT HUB**

Context Hub is a service that provides enrichment lookup capability in both the Respond and Investigations views. The service brings together contextual information from a variety of data sources so that analysts can make better decisions. It enables the quick look-up of both business and security context. Context Hub is hosted on the Event Stream Analysis (ESA) module. Metadata values with context will be highlighted so that analysts know there is more information available.

**RSA LIVE**

RSA Live is a platform and service where RSA shares content such as Feeds, Logs and Packet Parsers, Rules, Reports and Threat Intelligence with RSA NetWitness Logs and Packets customers. Customers can receive quick time to value and accelerate the time to detect, assess and respond to security incidents by leveraging RSA Live.

RSA Live Content and Threat Intelligence are sourced from multiple sources, including the following:

- RSA R&D and Engineering
- RSA FirstWatch Threat Intelligence Team
- RSA FraudAction Team
- RSA Incident Response (IR) Team
- RSA Malware Analytics Cloud
- 3rd Party Sources – Public and Commercial
- RSA Customer Community

**RSA LIVE CONNECT**

To counter the tight hacker community which collaborate openly, RSA Live Connect enables organizations to utilize and operationalize crowd sourced threat intelligence from the RSA Community. Analysts gain time-sensitive insights from their peers into emerging threats that target their enterprises. Analysts can provide anonymous risk assessments of threat intelligence at any stage.

**RSA NETWITNESS LOGS: GO BEYOND COMPLIANCE**

Ideally organizations could capture all logs. Collecting and analyzing everything is a great strategy for vendors to sell more. Unfortunately, the reality is that it collecting everything provides a false sense of security since we know that humans become overwhelmed and many alerts from logs have been missed or ignored in critical security situations in the past due to them being hidden in the noise. Collecting logs is not enough. Analysts need tools
that help prioritize log reports by structuring information in a way that is easy and fast to highlight more relevant alerts and correlate across alerts.

RSA NetWitness Logs solution creates metadata to identify what is most relevant and important for analysis. Unlike other SIEMS, RSA NetWitness Logs parses, enriches and indexes logs at capture time delivering differentiated speed for alerting and analysis.

COMPLIANCE
RSA NetWitness Logs is a network security monitoring and forensics tool that collects, analyzes, reports on and stores log data from a variety of sources to support security policy compliance and regulatory compliance initiatives.

- RSA NetWitness Logs deliver SIEM capabilities for the compliance use cases with pre-built templates for the regulations such as SOX, PCI or HIPAA.

DISCOVERY
Some of the most vulnerable organizations are those that are growing quickly, adding new environments due to mergers and acquisitions. RSA NetWitness Logs automatically identifies log sources when you have limited staff to manually classify. Unlike other log collectors which require manual configuration, RSA NetWitness Logs has automated this task.

- The Event Source Integrator (ESI) tool helps users to easily create parsers for new, unsupported or custom event sources. ESI provides for automation of the incorporation of new log sources.

BEYOND LOGS
As part of RSA NetWitness Suite: RSA NetWitness Logs integrates seamlessly with RSA NetWitness Packets and/or RSA NetWitness Endpoint which extends the detection capabilities beyond just logs.

RSA NETWITNESS PACKETS
The Power of the RSA NetWitness Packets is in the visibility and speed that it delivers for detection and investigation.

POWER OF PACKETS: PARSERS
Packet parsers identify the application layer protocol of sessions seen by the packet Decoder (see components), and extract metadata from the packet payloads of the session. Every packet parser is able to extract metadata from every session. For example, a webmail session will be parsed by both an HTTP parser which identifies the session as HTTP and extracts metadata from HTTP headers, and by a MAIL parser which extracts email-related metadata from message headers. Further, if the session were to contain an executable file, its presence would be detected by a Windows executable parser. The logic contained in the RSA NetWitness parsers is far more versatile than your typical regex-based signatures.
POWER OF PACKETS: INSTANT REPLAY
Event Reconstruction is enabled by the power of the details captured by packets and delivers ultimate visibility to what really happened. Events that can be reconstructed include emails, web content, IM conversations, text, hex, and packets. This is like Instant Replay – or having a security camera constantly monitoring relevant activity in your network. A reconstruction for emails will allow analysts to see the email header, who it was sent to, the sender and the entire body including all malicious components. This delivers depth of visibility.

POWER OF PACKETS: HUNTING
Hunting within the RSA NetWitness dataset is accomplished by analyzing intrusions, reverse-engineering malware, analyzing traffic generated by malware and other attacks, then selecting metadata generated by RSA NetWitness based on this type of behavior. Content and tactics have evolved from the experience of the RSA IR team from numerous investigations and aid an analyst to quickly navigate the dataset by combining many aspects of behavior into a single piece of metadata. This cuts down on the number of drills needed to find the sessions with the desired behavior, enhancing performance of the platform and reducing the effort needed to find malicious behavior. This has allowed the IR team and other users to discover incidents without any prior knowledge or notification that the organization was under a targeted attack. The IR team has also used these methodologies and content to discover many incidents where the attacker wasn’t even using malware, but authenticated access, also called Living off the “LANd”.

HUNTING PACK: The Hunting pack is prepacked content designed to help analysts quickly hunt for enablers and indicators of compromise or anomalous network activity by dissecting packet traffic within the RSA NetWitness Packets and populating specific metadata keys with natural language values to expedite investigations.

POWER OF PACKETS: INCIDENT RESPONSE AND BEYOND
The unprecedented view into network traffic provided by RSA NetWitness Packets is not only effective for Incident Response capabilities, but can also be used to validate the appropriate enforcement of your security policies and/or uncover areas where these policies and procedures may require improvement. The platform helps organizations improve tactics and evolve the skills of their analysts.

ESA: CORRELATE, DETECT AND RESPOND IN REAL TIME
The Event Stream Analysis (ESA) module is a powerful analytics and alerting engine that enables correlation across multiple event types. ESA can consume and analyze metadata from log, packet, Netflow, and endpoint sources using rules. There are out of the box or by creating custom rules. ESA helps analysts gain visibility and create custom alerts based on their environment.
**RSA NETWITNESS SUITE**

The RSA NetWitness Suite delivers the only unified solution that helps security teams understand the full scope of an attack — across endpoints, networks, and the cloud. Combining insights from RSA NetWitness Endpoint into endpoint behavior and activity with the rich set of network packets and log data from RSA NetWitness Logs and Packets allows analysts to gain unmatched visibility into everything happening in their environment, allowing them to investigate more completely, and respond more definitively.

**VISIBILITY**

The RSA NetWitness Suite captures and enriches data sources with security and business context in real-time delivering unparalleled visibility and forensic capabilities. RSA NetWitness Suite enables enterprises to not only connect incidents in real time but also to relate them across a long time horizon which means threats can be observed and understood and counter strategies put in place.

Pervasive visibility via monitoring across:

- Data Sources – Logs, Full Packet Capture, NetFlow, and Endpoints
- Threat Vectors – Endpoint, Network, and Cloud

![Figure 1 - Overview of RSA NetWitness Suite, with both RSA NetWitness Logs and Packets and RSA NetWitness Endpoint and RSA Live](image)

**ARCHITECTURE**

The architecture consists of three functional components: capture, analysis and server. It is a modular architecture allowing customers to scale the RSA NetWitness Logs and Packets deployment based on capture or analysis performance requirements. RSA NetWitness Logs and Packets can be deployed in both physical, cloud and virtual environments.
VISIBILITY INTO THE CLOUD

For AWS customers, the RSA NetWitness Logs and Packets components are available as AMIs and can be deployed completely within the AWS cloud or in a hybrid manner to collect, encrypt, monitor and store both packets and logs from AWS and the VMs running in AWS. In order to collect packets it is necessary to incorporate Gigamon’s Visibility Platform for AWS.

For Azure customers, the RSA NetWitness Logs solutions components can be deployed completely within the Azure cloud or in a hybrid manner to collect, encrypt, monitor and store logs from Azure and the VMs running in Azure.

RSA NetWitness solutions are scalable and modular to that help enterprises secure their ever expanding perimeter-less networks.

RSA NETWITNESS SUITE DEPLOYMENT OPTIONS

RSA NetWitness Logs may be deployed as follows:

- Standalone Logs SIEM solution.
- As a logs analytics module to compliment other 3rd party SIEM tools and enhance threat detection.
- Integrated with other components within the RSA NetWitness Suite - Packets or Endpoint - to enable a single integrated view of threat information across logs, packets and endpoint sources.

RSA NetWitness Packets may be deployed as follows:

- Standalone Packets solution.
- As a packets analytics module to compliment other 3rd party SIEM tools and enhance threat detection across logs and packets.
- Integrated with other components within the RSA NetWitness Suite - Logs or Endpoint - to enable a single integrated view of threat information across logs, packets and endpoint sources.

Whether it is just for logs or extended to packets and endpoints - The RSA NetWitness Suite provides a single, scalable system which serves as the centerpiece of your security infrastructure with differentiated breadth and depth of visibility for rapid threat detection and response.
# RSA NETWITNESS SUITE COMPONENTS

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA NetWitness Server</td>
<td>Web UI and management server, which serves as primary user interface.</td>
</tr>
<tr>
<td>Decoder</td>
<td>Captures and stores raw data. Decoders are specific to Logs or Packets. Create metadata from raw data capture and enriches with security and business context.</td>
</tr>
<tr>
<td>Concentrator</td>
<td>Stores and indexes metadata for fast queries and retrieval of raw data capture.</td>
</tr>
<tr>
<td>Broker</td>
<td>Facilitate queries across a multi-site deployment. Facilitate scale.</td>
</tr>
<tr>
<td>Event Stream Analysis (ESA)</td>
<td>Real-time correlation and analysis engine across logs, packets, endpoints and NetFlow.</td>
</tr>
<tr>
<td>Archiver</td>
<td>Long term retention and compression of log data for compliance reporting.</td>
</tr>
<tr>
<td>Virtual Log Collector (VLC)</td>
<td>Virtual or Cloud instance of a log collector for remote sites to forward logs to the Decoder.</td>
</tr>
</tbody>
</table>

## 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](https://www.rsa.com/en-us/products/threat-detection-and-response/siem-and-beyond).

## NEXT STEPS