# RSA Live and RSA Live Connect

## Actionable Content and Intelligence to Detect and Respond to Threats

## OVERVIEW

In today's threat environment, threat actors evolve their tactics rapidly to evade static security controls and signature-based detection solutions. Threat actors are using open-source methodologies where attacker Tactics, Techniques and Procedures (TTPs) are publicly available and it is simple for them to study, change and improve the TTPs for their benefit. Threat actors are effectively collaborating to design and share new strains of hacking services, botnets, malware and exploits.

Against this backdrop, organizations need to collaborate and share actionable content and intelligence to detect and respond efficiently and effectively to security threats. RSA Live provides actionable content and threat intelligence reducing the time to detect, assess and respond to security incidents.

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

Analysts can view, provide input and leverage the content and threat intelligence in RSA Live from both RSA NetWitness Logs and Packets and RSA NetWitness Endpoint. RSA Live changes the security paradigm by illuminating only the most persistent security information relevant to an organization, and providing it continuously to enable prioritization for detection and response.

## SOURCES OF CONTENT & INTELLIGENCE

RSA Live Content and Threat Intelligence are sourced from multiple sources as follows:

- 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

## TYPES OF CONTENT & INTELLIGENCE

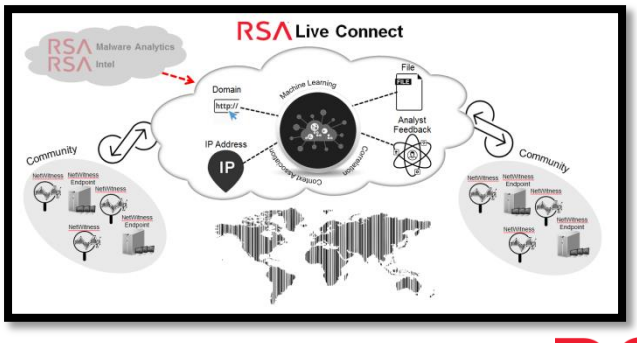
The types of Threat Intelligence and Content in RSA Live are as follows:

- **Threat Intelligence Feeds** consist of APT Domains, Suspicious Proxies, Malicious Networks, Threat Blacklists and Zero-Day Identifiers.
- **Event Stream Analysis (ESA) Rules and Alerts** provide advanced analytics across disparate event streams to detect and alert hidden threats such as Privileged escalations, Lateral Movements, Windows Suspicious Admin Activity and others.
- **Correlation Rules** enable detection of Data Exfiltration, Identity and Access Anomalies, Unusual Connections, Endpoint / Network Activity Anomalies, Reconnaissance Activities.
- **Reports** that provide a view of an organization's Compliance Posture, Network Activity, IT Operations, Suspicious Behavior and User Activity.
- **Parsers** for both Logs and Packets that convert raw data to metadata so raw data can be indexed for fast query.

## RSA Live Connect

RSA Live Connect is a community driven, cloud hosted, threat intelligence service. RSA Live Connect collects, analyzes and assess crowd sourced threat intelligence from various sources including RSA NetWitness Logs and Packets and RSA NetWitness Endpoint.

Using RSA Live Connect, analysts can peer into the intelligence during an investigation. The initial version of RSA Live Connect has suspicious IP addresses sourced from RSA Malware Analytics Cloud and RSA Incident Response Team. These IP addresses are characterized as either having suspicious communication or source of malware.



## RSA NetWitness Logs and Packets → Live Connect

During an investigation, an analyst can peer into RSA Live Connect and get an indication of why the IP Address is suspicious as follows:

- Risk Reason – Suspicious domain, Suspicious communication, Malware source or 3rd party Blacklist
- % of Users that found the IP Address risky
- Community statistics with how many analysts investigated this IP address

Additionally, each analyst can provide their opinion of the IP address, is it safe or risky?


## RSA NetWitness Endpoint → Live Connect

Using RSA NetWitness Endpoint, analysts can opt-in to see the reputation of a file in RSA Live Connect. The analyst can see details as file hash, Timestamp, Analyst score, First time seen, Related IOCs, Total analysts viewed, Related IPs and BIOS category.