RSA DATA DISCOVERY FOR RSA SECURITY ANALYTICS
Enabling Content Aware Security Investigations

AT A GLANCE
Gain Visibility into IT Assets
- Classify organization-wide IT assets with 170 out-of-the box expert data classification policies.

Simplify Investigations
- Use contextual IT asset information to quickly drill down to suspicious traffic.

Prioritize Alerts and Incidents
- Raise alerts based on criticality of IT assets involved in security analysis.

CONTENT AWARE INSIGHTS FOR RSA SECURITY ANALYTICS

Security attacks are becoming more targeted and sophisticated, and security teams are required to gain as much visibility as possible into the attacks and the corresponding business impact in order to effectively protect the organization’s most sensitive data. Furthermore, the attacks could come from external sources or from a malicious insider, both aiming to steal valuable data.

Security analysts investigating suspicious network traffic may not have the appropriate visibility into the business context or the types of data targeted by advanced attacks, and as a result are unable to correctly prioritize alerts for additional investigation and remediation.

RSA Data Discovery is a data classification tool for RSA Security Analytics that not only discovers IT assets such as data repositories (file servers, SharePoint servers, etc) and endpoints, but also identifies if sensitive data such as credit card data, privacy data, and intellectual property is residing in these assets. RSA Data Discovery feeds meta data information to RSA Security Analytics about IT assets containing critical information (such as regulatory data or intellectual property), so that organizations can quickly identify attacks on critical assets and enable security analysts to better prioritize investigations.

RSA Data Discovery is based on matured RSA Data Loss Prevention (DLP) content analysis technologies, where various sophisticated techniques, such as pattern and proximity analysis, derivative, and full signature analysis are used. This offering comes with more than 170 out-of-the-box expert information classification policies including policies for HIPAA, PCI, NERC, and EU Data Privacy that organizations can just turn on.

ENABLE CONTENT AWARE SECURITY INVESTIGATIONS
Using RSA Data Discovery for RSA Security Analytics, organizations can quickly identify and investigate advanced attacks involving both external sources and malicious insiders. Key benefits include:

- Simplified Investigations: Faced with a large number of suspect network sessions, the security analyst can use the contextual information of the IT assets to quickly drill down to suspicious network traffic involving IT assets with sensitive data.

- Prioritized Alerts and Incidents: Based on the data discovered on IT assets, RSA Security Analytics can prioritize alerts involving IT assets that contain sensitive data. For example, you can generate a high priority alert when outbound encrypted traffic is detected from an IT asset containing sensitive data going to an unknown destination server, which could be a malicious drop zone in another country or location.
• Report Generation: The reporting capabilities of RSA Security Analytics are further enhanced by the additional IT asset classification information presented by the RSA Data Discovery feed. A security analyst can generate security reports that also contain information classification for IT assets. These reports can be useful for both security investigations as well as tracking of assets having compliance or regulatory data.

For example, tasked with creating security reports concerning IT assets that have PII data, a security analyst can now generate reports about all suspected activity identified by RSA Security Analytics on IT assets containing PII data.