RSA

SOLUTION BRIEF

RSA NETWITNESS® NETWORK

VISIBILITY-DRIVEN THREAT DEFENSE

RSA

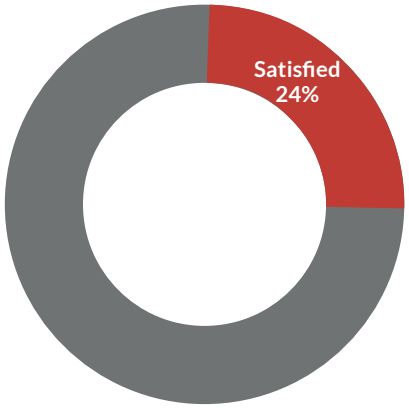
KEY CUSTOMER BENEFITS:

- *Gain complete visibility across enterprise networks*
- *Continuously monitor all traffic*
- *Faster analysis reduces risk exposure*
- *Reduce dwell time by rapidly detecting and identifying new threats*
- *Reduce risk exposure with deep insights*
- *Understand the full scope of attacks*

Today's cyber attacks are unparalleled in sophistication and organizations are failing to keep up. As dwell time continues to increase, organizations are struggling to identify and prioritize threats. Over 76% of organizations are dissatisfied with their current ability to detect and investigate threats using their current data and tools, according to a recent study by RSA titled Threat Detection Effectiveness Global Benchmarks 2016. But what options do they have? Most depend on perimeter-based security solutions. One solution is to capture data that provides visibility into the actions, movements and tactics of threat actors in order to increase the ability to defend against attacks.

OVERALL: LOW SATISFACTION FOR DETECTION AND INVESTIGATION

How satisfied are you overall with your ability to detect and investigate threats using your current data and tools?



Only **24%** of organizations are satisfied with their current ability to detect and investigate threats using their current data and tools.

Source: *RSA Threat Detection Effectiveness Global Benchmarks 2016*

RSA NETWITNESS® NETWORK

RSA NetWitness® Network exposes network data to enhance a security team's capabilities to detect and respond to today's advanced threats. RSA NetWitness Network provides immediate deep visibility for rapid detection, efficient investigation and forensics, in order to reduce dwell time. With unparalleled speed for real-time behavior analytics, RSA patented technology accelerates detection and investigation of threats as they traverse your network. RSA NetWitness Network provides real-time visibility into all your network traffic—on premises, in the cloud and across virtual environments. RSA NetWitness Network enables threat hunting with streamlined workflows and integrated, automated investigation tools that analysts use to hunt and monitor the timing and movements of threat actors. Through a unique combination of behavioral analytics, data science techniques and threat intelligence, RSA NetWitness Network detects known and unknown attacks that put organizations at risk.

RSA

RSA NETWITNESS NETWORK HIGHLIGHTS

ADVANCED THREAT DEFENSE
Gain greater visibility, detect threats sooner, and focus response more effectively

INTUITIVE INVESTIGATION & FORENSICS
Comprehensive Investigation Tool-Kit for forensic analysis

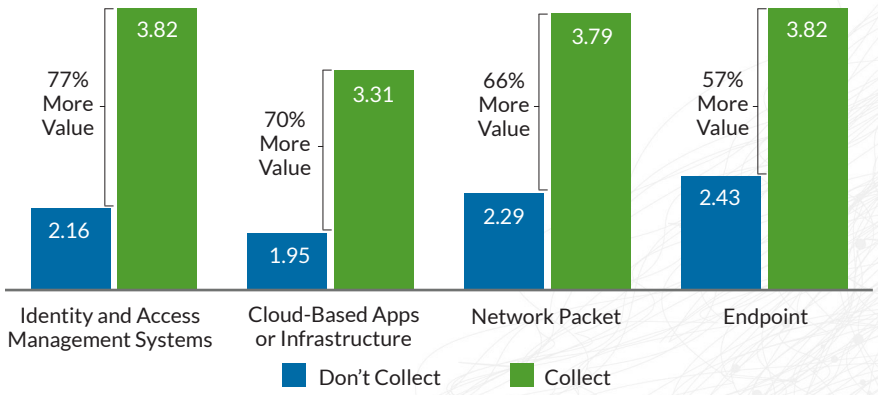
ACCURATE HUNTING WITH CONTEXT & THREAT ANALYTICS
Real time capture and enrichment of network data guides the hunter

DEEPER UNDERSTANDING OF THE FULL SCOPE OF AN INCIDENTS
SEE what happened with reconstruction capabilities leveraging network visibility

You Don't Know What You Don't Know

Organizations that collect specific types of data find increased value compared to those who don't.

How Valuable is this data source in helping you detect threats?
(Average Rating, Scale of 1 to 5)



Source: *RSA Threat Detection Effectiveness Global Benchmarks 2016*

One option to improve threat detection is to capture data that provides visibility into the actions, movements and tactics of threat actors in order to increase the ability to defend against attacks. Network Packets is one of the top 3 data sources that organizations have seen as valuable for detecting threats. The RSA NetWitness Network solution provides visibility and analytics for network packets to improve threat detection.

ADVANCED THREAT DEFENSE

GAIN GREATER VISIBILITY, DETECT THREATS SOONER AND FOCUS RESPONSE MORE EFFECTIVELY

With unparalleled speed for real-time behavior analytics, RSA patented technology accelerates detection and investigation of threats as they traverse your network. By collecting and analyzing network packets, organizations gain deep visibility into the nature of traffic on their enterprise networks.

RSA

Alleviates Analysts' Alert Fatigue

Enriches network data with threat intelligence and contextual information about your business so that your analysts can quickly identify high-priority threats and reduce false positives.

Simplifies Threat Detection and Investigation

Hunt for threats without ever having to look at a PCAP again. RSA NetWitness Network offers intuitive data visualizations and nodal diagrams—in addition to a complete set of automated detection, investigation and forensics tools—to transform every analyst into an experienced threat hunter.

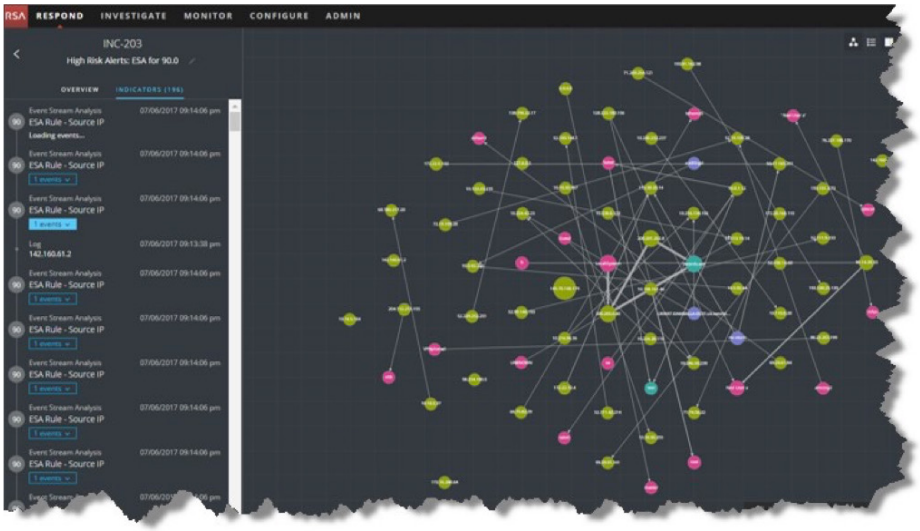


Figure 1: RSA NetWitness Comprehensive Nodal View of Incidents

INTUITIVE INVESTIGATION & FORENSICS

COMPREHENSIVE INVESTIGATION TOOLKIT FOR FORENSIC ANALYSIS

When every second counts, RSA provides the tools an analyst needs to quickly investigate incidents and reduce risk. Network data from packets is enriched with business and identity context in addition to threat intelligence, which then provide a consolidated and comprehensive view that reveals the insights an analyst needs in order to follow the trail left by threat actors.

ACCURATE HUNTING WITH CONTEXT & THREAT ANALYTICS

REAL-TIME CAPTURE AND ENRICHMENT OF NETWORK DATA GUIDES THE HUNTER

A critical aspect of hunting is having the tools you need available. RSA provides content in Hunter Packs to get your analysts started down the right path.

DEEPER UNDERSTANDING OF THE FULL SCOPE OF AN INCIDENT

SEE WHAT HAPPENED BY LEVERAGING NETWORK VISIBILITY

Comprehensive and Continuous Network Monitoring

Monitors all data from any network, including virtual networks, as well as packets from public clouds such as AWS. Because it enriches packet data

RSA

at capture time, RSA NetWitness Network provides the immediate, deep network visibility required to accelerate detection, investigation and forensics.

Eases Management of Network Data

Pervasive visibility facilitates administration and analysis of data across distributed and virtual environments, enabling rapid detection, investigation, reporting and management of all network data. From the intuitive nodal views to the extensive and robust tools available for investigation, the tasks that an analyst has to perform are all available within one platform so that an organization can understand the full scope of attacks and the risks they pose.

TRUSTED TECHNOLOGY

RSA NetWitness solutions received the Common Criteria certification for product security and are certified for U.S. Department of Defense Information Network UC APL.

SCALABLE PLATFORM

RSA NetWitness Network is an integral part of the RSA NetWitness Platform, an enterprise-grade, modular and flexible platform that meets the needs of customers as they evolve their security strategies. In addition to RSA NetWitness Network, the RSA NetWitness Platform consists of RSA NetWitness Logs, RSA NetWitness Endpoint, RSA NetWitness UEBA Essentials. Together, these solutions deliver the industry's most complete visibility across logs and network and endpoint data, helping to expose the full scope of attacks and make security analysts more efficient and effective through automation and advanced analytics.

03/18, Solution Brief, H17073.