



RSA NETWITNESS® PANORAMA

Unifying pervasive network monitoring and log data for a complete view of potential threats

Solution Brief



OVERVIEW

Today's security threats are dynamic, multi-faceted and highly complex initiatives oftentimes drawn out over long periods of time. The current security tools are simply not designed to identify and investigate these types of advanced threats. In order to defend against these challenges security analysts and IT professionals require a comprehensive and interactive view into their entire infrastructure.

RSA NetWitness® Panorama, a new module in the RSA NetWitness family, delivers innovation in security analytics through the fusion of hundreds of log data sources with external threat intelligence. Combined with existing RSA NetWitness network monitoring products, Panorama can now provide enterprises with extraordinarily broad and robust high-speed visibility into the critical information needed to help detect targeted, dynamic and stealthy attack techniques.

WHAT IT IS AND HOW IT WORKS

RSA NetWitness Panorama may be deployed in three ways: as an extension to RSA NetWitness installations to combine the diverse information contained in log files with the deep content of full traffic capture; alongside RSA enVision® SIEM for fast security analytics across the volumes of log data collected by enVision SIEM; or as a standalone log-analytics module—with or without other third party SIEM tools. The module can either consume syslog data directly or gather richer data via direct feeds from the RSA enVision SIEM platform to provide even greater context for investigations and incident response.

RSA NetWitness Panorama's comprehensive security event log collection, leveraged in the RSA NetWitness Investigator and Informer modules, delivers an innovative fusion of security intelligence that offers correlation and analysis of the large volumes of network and system data needed for effective threat detection.

Informer is a NetWitness module for reports and alerts created for the ongoing monitoring of elements from an active investigation, and the detection of anomalies and analytics (reports, alerts) to assist with specific aspects of security investigations. With NetWitness Panorama's infusion of event log data, Informer applies the same rigorous reporting and alerting logic of raw network data to log data, enabling users to rapidly build multi-layered reports for distribution to security teams and management to address a myriad of problem sets.

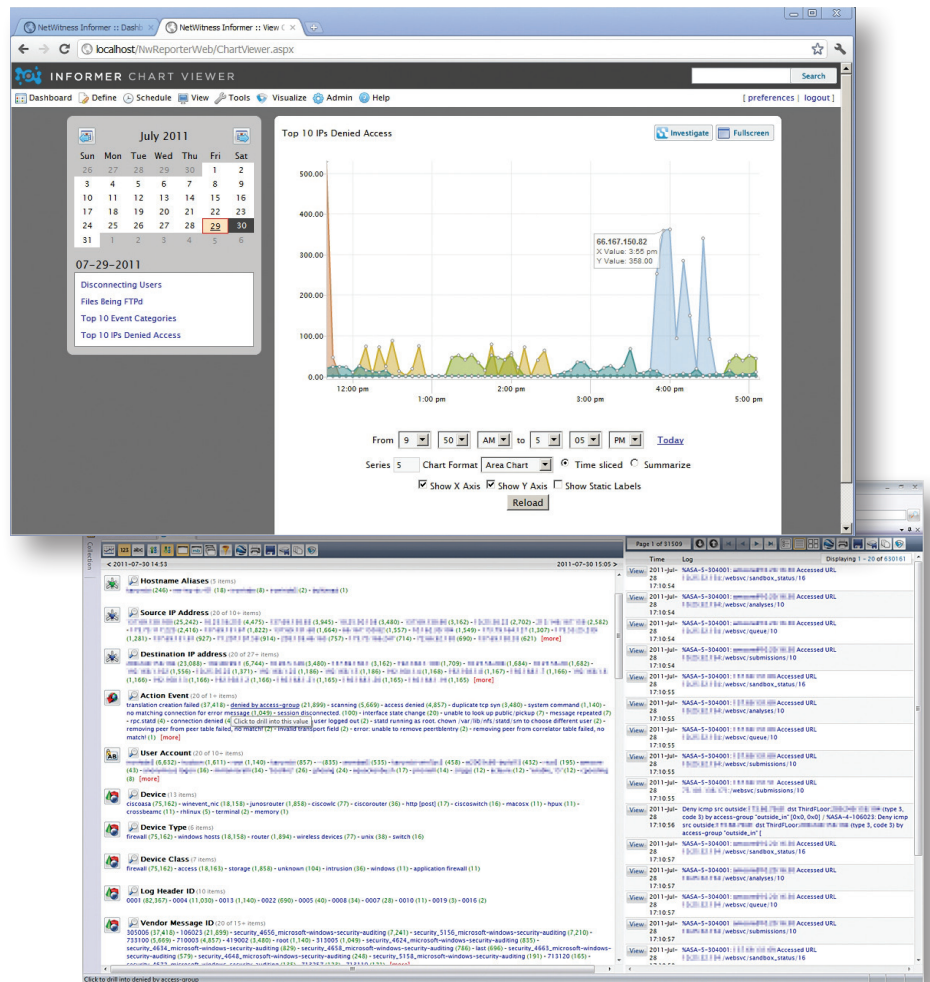
NetWitness Investigator provides free-form contextual analysis of raw network data captured and reconstructed by the NetWitness enterprise security platform. Panorama and Investigator correlate log events in real-time during analysis, as well as provide an intersection of log and raw network packet data, previously unavailable in a single product. This enables new log formats to be easily consumed and modeled into a single unified infrastructure of threat intelligence. From Google earth displays and time-line views to raw log data analysis, NetWitness helps security organizations to focus valuable staff on high-risk issues and adapt and adjust policies, procedures and investments in order to manage the risks of their virtual and physical environments. And by integrating NetWitness Investigator Enterprise with NetWitness Live, log data can now be correlated with real-time threat intelligence, enabling users to monitor suspect activity contributed by the global security community to better track advanced and emerging threats.

Log management and SIEM technologies are important elements of incident and threat management processes, but have been constrained by the lack of a common lexicon, scalability, and the agility to adapt to the ever-changing threat landscape. RSA enVision SIEM is a powerful tool for real-time correlation, alerting, security event monitoring, compliance reporting and analysis of log data as part of the security process. And, by providing native, cross-environment visibility and threat-informed analytics across log data, RSA NetWitness Panorama technology offers an unprecedented view of organizational activity across even more of the IT infrastructure.

NetWitness Panorama's innovative high-speed security analytics of log data makes the data an active part of security operations. Those innovations include:

- Interactive data-driven analysis of over 200 different enterprise log formats, leveraging RSA enVision content definitions
- Award-winning, patented, drill-down analysis that works over network sessions and log data
- Mature threat intelligence combined with log data for better context of threats, automating a key part of the information sharing process around threats
- Data presented the way expert security analysts investigate advanced threats, enabling more insightful analysis
- Scalability and speed to enable fast, actionable log analytics
- In side-by-side deployments, a high speed connector from enVision SIEM to the Panorama module enables richer data feeds into Panorama

RSA NetWitness Panorama delivers visibility and analysis of log data



PANORAMA IN ACTION

Global Enterprises are often hindered by the lack of comprehensive network visibility and the variety of network and security data sources required for effective incident response management and investigation. Current approaches to gaining such comprehensive visibility are challenged to scale to the size of the data sets involved, creating the possibility for poor performance which can result in proliferation of the threats.

NetWitness Panorama used with NetWitness NextGen provides complete visibility into network traffic and enterprise logs in a single, scalable system, enabling deep situational awareness and agility across large and diverse network data sets. By combining these network and log security insights into a reusable and normalized data framework, security staff and management are able to rapidly and effectively respond to sophisticated threats and events, particularly those related to vectors associated with advanced threats, such as behavior of external/internal network elements, hosts, users, custom applications and non-network based entities.

Panorama leverages exactly the same, proven and highly scalable N-Tier architecture used for network traffic recording and indexing—for more than 200 devices and common log formats. Without this architecture, enterprises are forced to deploy disparate systems that are often susceptible to inadequate design, a lack of big-data scalability and, as point solutions, are incapable of providing the contextual network views needed to respond to enterprise needs.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2011 EMC Corporation. EMC2, EMC, RSA, the RSA logo, enVision and NetWitness are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products or services mentioned are trademarks of their respective companies.

h9008-netwp-sb-0811

www.rsa.com

