NETWITNESS

DATA SHEET

The Netwitness® Platform

See Everything. Fear Nothing.

Overview

Today's shortage of qualified security experts is a global challenge for all enterprises. Having the right information at their fingertips is crucial for security analysts. Companies are confronted with thousands of alerts from multiple security solutions, and a myriad of tools across multiple screens. This can lead to delays in detection, and failure to respond to the real threats to their organization.

The **NetWitness® Platform** empowers security teams to detect and understand the full scope of a compromise, because it analyzes data and behavior across an organization. Business and security context enriches data from logs, packets, endpoints, NetFlow, and IoT devices. The NetWitness Platform transforms the data into more useful information through real-time enrichment with business context and threat intelligence delivered from a variety of sources. The Platform utilizes a unified taxonomy across all data sources to accelerate the detection of both known and unknown threats.

The **NetWitness Platform** is designed for analysts who are responsible for protecting valuable assets and networks. The accessibility of both business and security context throughout the user interfaces enables prioritization and results in faster threat detection and response. Whether it is business context such as asset criticality, user information from identity solutions, or threat intelligence, relevant information is easily accessible and highlighted for the analyst.

Analysts are at the core of every security team or organization's defense strategy. The NetWitness Platform empowers them with the following capabilities:

- Automated analytics and sophisticated tools to make every analyst better at what they do.
- Intuitive workflows to help alleviate pressures from security skills shortage.

One of the biggest challenges facing security teams worldwide is "How do we effectively prioritize threats?"

The NetWitness Platform answers that question of prioritization paralysis with intuitive interfaces for both initial Response workflow and detailed Investigation. Analysts can smoothly transition between triage activities and investigative activities to immediately gain a more comprehensive view of the metadata behind the incident. Analysts of all levels can increase their productivity with the flexibility to dive into any incident within Respond workflow or from the Investigation workflow.

Key Analysts Benefits

- Gain complete visibility across your network
- Alleviate pressures from security staff shortages with intuitive workflows
- Focus on the threats that really matter with relevant context
- Faster root cause analysis reduces time and cost of incident response and investigation
- Drastically reduce dwell time by rapidly detecting and investigating threats
- Increase resolution rate with reduced time-to-remediation for incidents
- Completely understand the full scope of attacks across logs, packets, endpoints, NetFlow and IoT devices with the NetWitness Platform

Security and business context accelerate threat prioritization

The Context Hub incorporates business and threat information that helps to identify and prioritize threats. The Context Hub provides an enrichment data lookup capability in both the Respond and the Investigation views to expose context data on demand. The sources for enrichment data include asset criticality directly from Archer, Microsoft Active Directory, and threat intelligence sources; Respond or incident management; custom lists; Endpoints and various options for customers to incorporate their own external enrichment data. Context Hub enables relevant threat information such as whitelists, blacklists or custom watchlists to be imported and exported. In addition, Context Hub is integrated with RSA Live Connect service so that a RSA **Live Connect** Risk Assessment, in the form of a Risk Badge (Unsafe, High Risk, Suspicious, Safe, or Unknown, can show the risk level assigned to the entity by RSA Live Connect and other sources of risk factors.

Archer	Incorporate asset criticality with asset information
Microsoft Active Directory	Feed user behavior analysis and protect high-profile individuals and user roles
Respond	Correlate with related incidents and alerts to see patterns and the full scope of an attack
Custom Lists	Trigger from detail in any CSV file to provide further context
NetWitness Endpoint	Complete the picture with information from NetWitness Endpoint including machines, processes, files, etc.

As a result, incident responders and security teams gain unparalleled insights, allowing them to prioritize threats quickly and drastically reduce threat dwell time by focusing their response more effectively to protect their organizations.

A force multiplier for security analysts and incident responders

The **NetWitness Platform** concentrates and synthesizes relevant information for easy access by analysts. Toggling between a myriad of disparate tools can be frustrating and confusing, making it easy for an analyst to miss something. By creating visual clues and integrating tools such as a storyline and nodal diagrams for events, the respond process is streamlined. External tools, look-ups and screens are eliminated and therefore reduce the headaches of toggling between multiple tools. The NetWitness Platform interfaces are designed to reduce both eye strain and the cognitive load on analysts.

Based on insights from hundreds of Incident Response situations, the NetWitness Platform is designed to streamline triage by providing all the relevant information on a single screen. Each component is designed to add value to and simplify the workflow. Correlated metadata and relevant business context is highlighted and made available to help the analysts to make better decisions. The result is that the workflows facilitate the development of analysts and help improve the productivity of the entire security team.

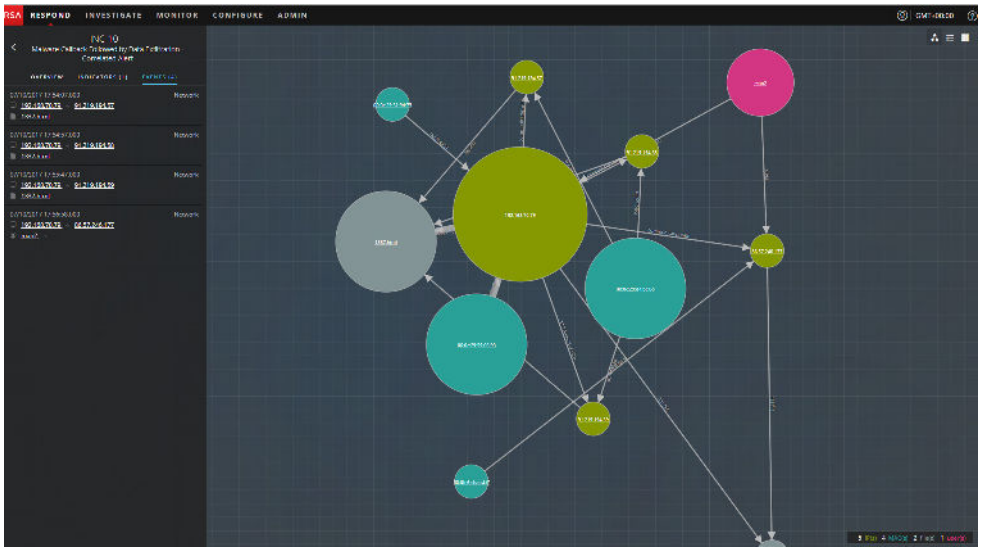

Figure 1 – The NetWitness Platform RESPOND Interface Nodal View

Identify and understand threats at a deeper level

The flexible analyst interfaces are designed for analysts of all levels. It is a swim-at-your-own-level scenario. Analysts have access to tools to go as deep as their skill set enables. The exposure to investigation tools facilitates learning within the platform. Agents can select an incident and then begin to triage in Respond or they can transition to Investigate workflow for a deeper dive. Alternatively analysts can choose to go directly into the Investigate workflow.

Once an incident is selected the Respond workflow provides the Incident Details screen where an “Overview”, “Indicators” and “Events” views are available. The Indicators view provides a Storyline of the incident with a Nodal diagram or list view displaying relationships. All related alerts and indicators that generated the Incident are shown. The related indicators can include: Source/Destination IP, Hostname, Username, Domain Name, and Filename for the Indicator that triggered an alert. The Storyline is arranged in chronological order and helps the analyst understand the full scope of the Incident by identifying other alerts/indicators that may be related but not part of the Incident. From the Storyline, an analyst should be able to begin understanding what assets or elements of the environment might be affected by this Incident.

The NetWitness Platform highlights relevant information with an Interactive Nodal Diagram (in Figure 1 that shows relationships to provide visual insights. The nodal nature incorporates the intensity of connections and the occurrence frequency is revealed by the size of the node. The Nodal diagram paints a picture of what elements (metadata are involved, and the activity and historical information is described in an easy-to-follow and comprehensive manner in the Storyline (Indicators component. Analysts can "hover" and/or "click" to reveal the next level of detail and reveal additional relationships. With a visual mapping of what is happening in their environment, analysts are able to respond faster to a wider range of incidents. While analysts still have visibility into the granular details of alerts and indicators within an incident, the nodal diagram provides a quick and easy way for them to visualize what happened during an incident. In addition, they can interact with the nodal diagrams and reveal additional relationships which facilitate interpretation.

Analysts can leverage RSA Context Hub for security and business context and RSA Live Connect for crowdsourced, RSA-community-based threat intelligence and hash reputation from peers to aid security analysts in identifying and responding to threats more efficiently.

As analysts investigate an Incident and begin to understand the context of the threat, they can transition to the Investigate interface to explore the raw security data. Within Investigation, analysts can analyze key metadata, view session reconstructions, and explore the raw log events. Coupling the ability to deep dive into the source data, with visibility to related supporting Incident information allows the analyst to understand and explore the full scope and severity of an Incident while revealing relationships that might not be apparent without the visibility available in the NetWitness Platform.

See the full scope of what happened

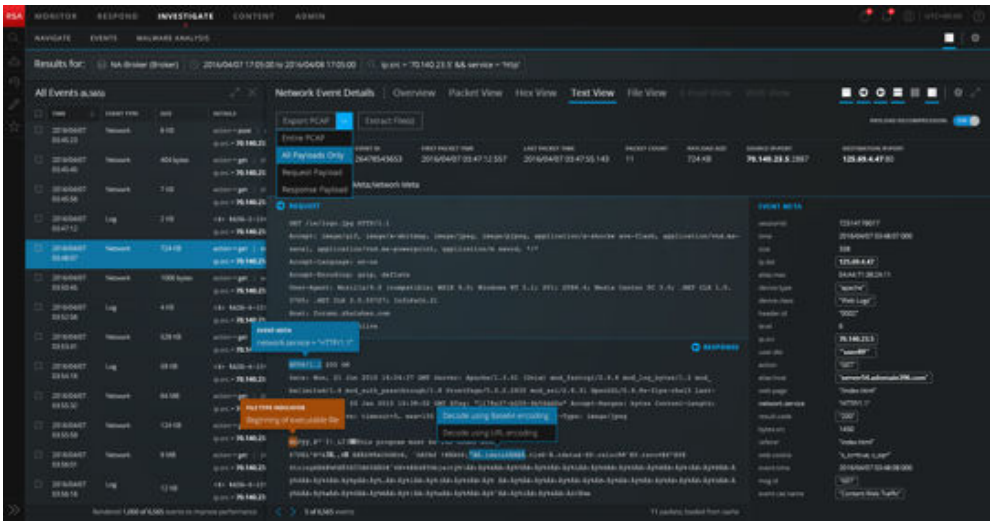

Figure 2 –The NetWitness Platform INVESTIGATE Interface

The Investigate interface is where deep analysis is enabled. The NetWitness Platform offers various methods of displaying the data, filtering the data, querying the data, acting on a drill point, and inspecting specific events. The Investigation workflow is designed for the more experienced analysts who typically would dive immediately into the colder deeper waters.

The Investigate workflow encapsulates all the relevant elements to enable investigations by consolidating information for analysts into a single screen. Querying of metadata delivers not only related metadata and related sequential events but also a reconstruction of event analysis to speed investigations. Designed for the more advanced analyst (the Hunter, Event Analysis within Investigation workflow, provides several options for the advanced analyst to dig deeper, reconstruct events, see patterns, find clues in the data, and export artifacts including PCAPs and other information for future reference.

Seeing is believing, but understanding builds knowledge. NetWitness Event Analysis encompasses event reconstruction with interactive instruction. Bolstering analysts' knowledge and capabilities through investigation provides ways for analysts to learn and perfect their talents as they start to easily sift through mountains of data. Empowering analysts to see the structures and interconnections within the data during triage of an incident or breach or while hunting for threats as they unfold.

Power of packets

Within Investigate workflow, analysts can reconstruct spearfishing emails and fake web sites to aid investigations. This can help identify insider threats or understand the criminality behind threats. The "devil is in the detail" and powered with NetWitness Network, the relevant details are organized and presented so that security analysts can discern valuable information and neutralize threats faster. Event Reconstruction is enabled by the power of the details captured by packets and delivers the ultimate visibility to what really happened. Events which can then be reconstructed include Email messages, Web transactions, and IM conversations, just to name a few. 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. Event Reconstruction delivers a level of depth for analysis that differentiates NetWitness Packets capabilities for forensic activities.

Additional visibility capabilities include the highlighting and revealing of Common File Patterns and shading of HEX Bytes in packet analysis. Even for experts this helps make certain indicators stand out and increases overall efficiency. The shading helps reveal hidden patterns. Reconstruction capabilities, auto detection of common file patterns and the shading HEX Bytes all deliver additional depth of visibility.

See no evil, hear no evil. Stop pretending that ignorance is bliss. The critical part in any investigation is being able to see what actually happened. NetWitness Packets empowers analysts to harness the evidence to determine what transpired in the environment.

Dive in

The NetWitness Platform delivers pervasive visibility and actionable workflows for responding to and investigating incidents that illuminate the full scope of an incident. Since the Platform prioritizes incidents based on business and security context, analysts, regardless of their skill level can dive deeper with greater confidence, knowing they will not drown in alerts.

Support

NetWitness' 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. NetWitness provides the resources you need to quickly and proactively resolve product-related issues and questions to ensure business continuity. For more information, visit the **NetWitness Services page**.

Next steps

For more information about the NetWitness Platform, visit **NetWitness.com** or contact your RSA Channel Account Manager or Authorized Distributor.

NETWITNESS