Achieving High-Fidelity Security

Combining Network and Endpoint Monitoring With RSA NetWitness and RSA NetWitness Endpoints

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for RSA

July 2016

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Achieving High-Fidelity Security

The term "hi-fidelity" was first coined in the entertainment industry in the 1950s to indicate advances in audio technology that provided the listener with a richer "just like being there" experience. In the security context, "high fidelity" communicates the ability to provide a richer experience to the security analyst to deliver better security outcomes.

High-fidelity security systems provide more comprehensive and timelier information *from multiple sources,* both internal and external, in the appropriate volume and with the appropriate types of data to provide the best context and priority for decision making and to drive appropriate detection and incident response activities.

This paper discusses the benefits of using both network and endpoint data with a strong analysis toolset to create high-fidelity security.

Visibility Provided by Endpoint Monitoring

Quite simply the endpoint is where the bad action takes place. Each device connected to an organization's network where information resides or is processed, especially if it's a device people work on directly, is a potential point for security threats to enter and exploit an enterprise. In today's environments, endpoints are no longer just desktop or laptop computers. The definition of an endpoint has expanded to include everything from servers to smartphones and tablets to special function and embedded Internet of Things (IoT) devices.

However, IT professionals have been somewhat slow to acknowledge these newer endpoints. While over 90% of IT professionals use smartphones themselves, only 64% of respondents identified smartphones as endpoints in EMA's 2016 "Achieving High-Fidelity Security" research. Servers scored even lower, with only 57% considering those as endpoints. While the shift to a more mobile workforce has been taking place, the shift in understanding of what a potentially vulnerable endpoint is has lagged behind.

To make matters worse security threats targeting these endpoints are many and varied and go well beyond malware. Threats also include attack modes that include misusing user credentials, running rogue services, using unapproved applications and sharing company data, running apps that leak confidential data, and many others. Whatever the mode, the detailed data about the execution of the attack that is contained within the endpoint is far richer than anything that can be gained at the network level alone or by merely looking at activity logs. Given that threats at some point in their lifecycle operate directly on endpoints, it is only common sense that monitoring systems should have a strong capability for monitoring the endpoints directly.

Visibility Gaps in Endpoint Monitoring

Security data from the endpoint is extremely important when it comes to an overall security monitoring program. But it only goes so far. Endpoint data by definition covers the last mile of an attack, but on its own does not provide a 360-degree view of the security posture of an organization.

Endpoint data can be compartmentalized since the endpoint monitoring system only knows about the activities happening within the monitored and impacted endpoints. Attacks that hit unmonitored endpoints obviously will not be picked up unless additional security monitoring is being used. This brings us to the importance of network-level visibility.

Visibility Provided by Network Data

The two most popular network security monitoring data sources used by organizations today are network flows and deep packet inspection (DPI). Network flows are used by 42% of respondents, and DPI (which is sometimes referred to as "full packet capture") is used by 36%. Of course, when trying to get a full picture of security threats, DPI provides a much more complete view than network flows, but for practical purposes using network flows also has its place.

Network flow (netflow) tools, such as NetFlow, J-Flow, sFlow, etc., are great at identifying the usage of odd protocols and abnormal traffic patterns at an overview level. But they can't provide information on the details of a network conversation, such as details on the data and files that were passed. DPI-based monitoring systems can provide those details. A best practice is to use DPI to monitor Internet egress points and very sensitive network segments and to use netflow to cover other internal network segments, in particular to monitor for attackers' lateral movement.

Organizations need visibility to prevent and detect breaches. Most attacks traverse the perimeter of the network, meaning network-based tools have the opportunity to identify an attack at an early stage and to alert on and address it before a significant incursion occurs. Maximally effective network tools can identify many types of activity, from reconnaissance and initial malware payload drops to the use of malformed protocols, protocol tunneling, abnormal encrypted traffic, and unusual/abnormal communication between hosts. Any of these can be indicative of not only compromise but also lateral movement, data collection, and data exfiltration.

Visibility Gaps in Network Data

Unfortunately, there are also gaps in network data. First, network monitoring systems for practical purposes are generally only deployed at the perimeters and at select internal network segments. When this is the case, data gaps can occur within or between local segments where the network is not being as closely monitored. This can lead to a false sense of security via false negatives in those missing areas of network coverage. Second, network solutions can't detect, at least initially, attacks that occur off network (for example, attacks that come in the form of removable media or come across home, hotel, or coffee shop networks). Not only are these attack vectors common, but compromising mobile devices that are connected to other endpoint systems for charging can also be an attack technique. This threat combined with the potential gaps in network data means an organization could be compromised on multiple internal hosts before the enterprise even sees the first network communication to or from those hosts. Third, there is a problem with false positives. In cases where the inbound communication and/or data payload is detected but no outbound response is observed, there is no way for the network detection tool to be certain that the incursion was successful or is simply lying dormant

Confirmation of the scope of an attack is also difficult to discern if the communications are encrypted. While there are ways to peer into encrypted network traffic, this requires the deployment of specialized decryption devices. In each of these cases, a false positive (or false negative) response may occur. The obvious point of this paper is that many of these gaps can be filled with the complementary use of endpoint *and* network monitoring tools.

Issues with Current Programs

Overconfidence

When asked about the maturity of their endpoint and network security program in terms of prevention, detection, and response, over 60% of the respondents identified all three aspects of network and endpoint as having "strong" or "very strong" maturity. (See Table 1 below.)

Function/Maturity	Network Maturity: Strong or Very Strong	Endpoint Maturity: Strong or Very Strong
Prevention	66%	63%
Detection	71%	67%
Incident Response	65%	62%

Table 1. Endpoint and Network Program Self-Reported Maturity

However, based upon other information collected in the survey, these results seem to be a sign of overconfidence. It is very likely organizations don't yet understand the level and type of network and endpoint monitoring needed to protect against today's threats. Surprisingly, the answers given leaned more towards strong or very strong maturity in both areas, whereas the results of other parts of our research indicated these security programs were actually very underdeveloped. For example, EMA asked about confidence in and use of network and endpoint tools. Only 15% of respondents were confident in the accuracy of their network and endpoint tools. Figures 1 through 3, shown in the following section, depict other inconsistencies.

High-Fidelity Challenges

Clearly a high-fidelity security approach that combines network and endpoint level monitoring would solve many of these security monitoring challenges. So what's preventing companies from going down this path? Largely, it's because the security systems they have in place lack key capabilities.

When respondents were asked to indicate the top challenges inhibiting the combined use of network and endpoint security data, the top response was lack of analysis capabilities in their existing solutions (59%), as shown in Figure 1.

Figure 2 illustrates perhaps the most glaring challenge organizations have in achieving high-fidelity security: Over 60% of organizations do not have any network analysis tools (packet capture, netflow, etc.) deployed.

Figure 3 shows another major challenge: lack of historical data for analysis. Forty-two percent (42%) of respondents do not store the data they do collect for any length of time, which means it is not available for historical detective analysis or post-event investigation and forensics.

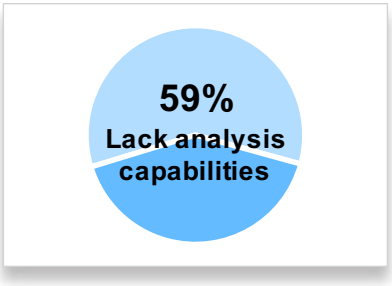

Figure 1. Lack of Analysis Capabilities

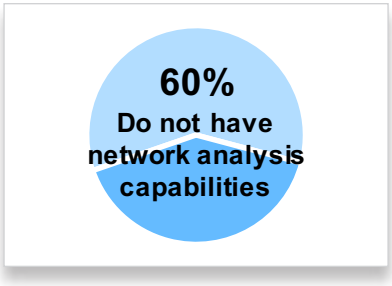

Figure 2. Lack of Network Analysis Tools

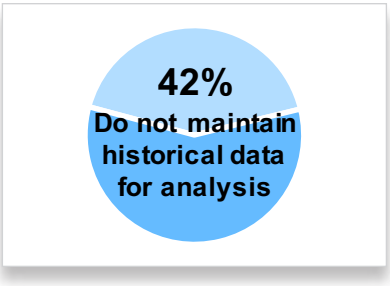

Figure 3. Lack of Historical Data

Combining Network and Endpoint Data Creates High-Fidelity Security

The Right Data for the Right Job

Due in part to these fundamental issues, organizations often rely on the wrong data when it comes to their security monitoring programs. Figure 4 shows responses concerning the types of data respondents used most often for providing an early warning of a breach. Though each of the data types listed has its place in detection and investigations, some are better than others.

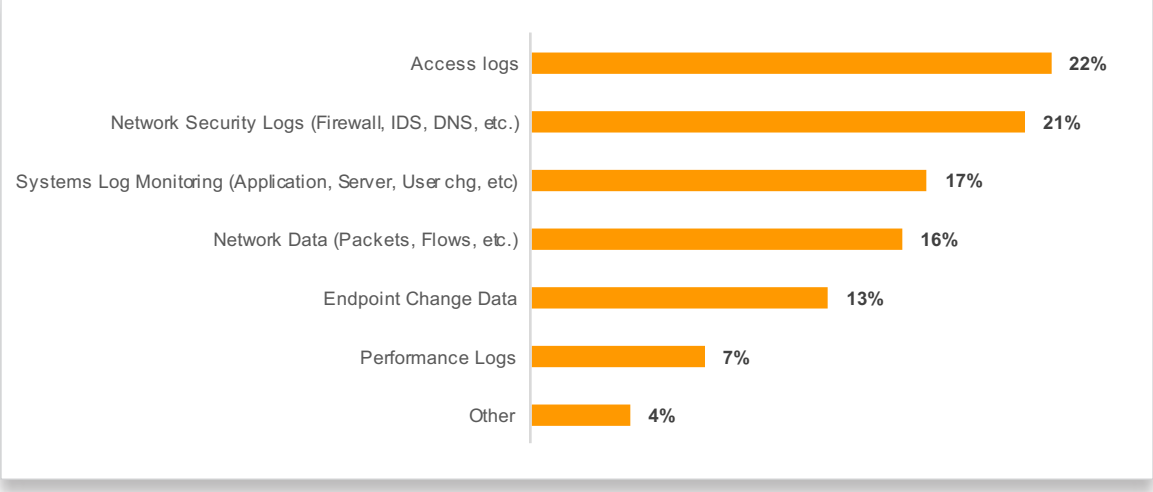

Figure 4. Data Used for Early Breach Detection

This data is highly indicative that many of the respondents either did not understand the value of the data or did not have the tools to leverage the data, regardless of their understanding. Access logs can indicate access attempts, but in most environments successful logins either are not logged or are not investigated unless they are preceded by a significant number of failed logins. This approach will not show an exploited vulnerability, a malware-based attack, or even a previously phished, legitimate credential. Network security logs and systems logs are similar in nature as they will both identify attempts to access resources that violate policy, but unless a successful attempt has been preceded by numerous failed attempts, it doesn't tend to be investigated in a timely manner. In the opinion of EMA, network packet data flows and DPI provide the best data for early threat warning, and, when combined with endpoint monitoring data are generally superior for threat detection and response.

When asked how important it was to integrate their endpoint security system with network security, less than 20% of organizations thought this was "very important," "extremely important," or "critical." Clearly organizations have a long way to go to understand the critical and complementary value of network and endpoint monitoring data.

The role of metadata in this area is also crucial. Metadata, or data about data, can provide valuable information about the characteristics of an attempted attack, such as the creator, the time and date of creation, and even the geographical location it came from. It is encouraging that over 80% of organizations that use network data in security investigations employ systems that create metadata. And, of these organizations, almost 85% found metadata to be extremely valuable to their investigations. However, 60% of organizations only keep this metadata for two weeks or less, which is a short time window given that incidents often persist for over six months before being detected.

Obtaining High-Fidelity Security with RSA NetWitness and RSA NetWitness Endpoints

RSA NetWitness

RSA NetWitness enables organizations to collect, manage, and analyze their security activity, leveraging logs, events, netflow, DPI, endpoint data (provided by RSA NetWitness Endpoints), and other data. It does this through two core elements: its capture infrastructure and its analysis and retention infrastructure.

The capture infrastructure features a highly configurable Decoder that works with packet capture data (as well as a version that works with netflow, logs, and events). The Concentrator portion, which sits behind the Decoder, aggregates the metadata and enables query scalability, letting organizations deploy the solution across diverse network topologies and geographies. Finally, the Broker and RSA NetWitness server allows for queries to be distributed across enterprise-level deployments.

The analysis and retention infrastructure is made up of an Archiver, which manages long-term data storage as well as an Event Stream Analysis (ESA) service which processes high volumes of disparate event data, including correlating logs, packets, netflow, and endpoint-sourced information as well as executing real-time machine learning and data science models. The metadata can also be fed into Hadoop infrastructures for more historical analysis.

RSA NetWitness' interface presents incident data, investigations, and reports in multiple formats that can be customized by role/function to match incident management and investigative workflow needs. Dashboards are also customizable by the user.

RSA NetWitness Endpoints

RSA® NetWitness Endpoints is designed to enable active endpoint defense against advanced threats by rapidly detecting and blocking or quarantining suspicious files and processes without the need for signatures.

Through its behavior-based detection, RSA NetWitness Endpoints lets organizations discover attacks that might otherwise be hidden. It accomplishes this with kernel- and user-level system monitoring, enabling real-time alerting, using unique scan techniques, full device inventorying, profiling, risk scoring, and automatically scanning the system when unknown files or processes are loaded.

If a possible threat is detected, NetWitness Endpoints quickly analyzes the endpoint to confirm an infection. The system then scores and flags suspicious endpoints and the associated activity for further investigation. NetWitness Endpoints also maintains a global repository of all existing files and IP addresses connected to the network to help reduce investigation time. It also performs a wide range of file checks to determine if a file is malicious and to provide more context—incorporating YARA rules, STIX-delivered threat intelligence, and the results of multiple AV engines to complement its behavior-based analytics.

If an endpoint compromise has occurred, NetWitness Endpoints enables security teams to take quick action. NetWitness Endpoints helps the analyst to determine the scope of an attack instantly—for example, by simply right-clicking on a malicious file, the system will show all other endpoints with that same file. NetWitness Endpoints automatically gathers critical forensic information that allows teams to see all modified and deleted files at a glance. Finally, NetWitness Endpoints allows teams to conduct precise blocking. By providing the exact location of malicious files, NetWitness Endpoints lets teams quarantine and block malicious files quickly.

In addition, RSA has integrated RSA NetWitness and the RSA NetWitness Endpoints tools together to provide a unified data source, analytics, reporting, and a single console for security detection and investigations.

Customer Perspective

Perhaps the easiest way to understand the benefits of high-fidelity security and how it can be achieved using RSA NetWitness and NetWitness Endpoints is to discuss how a real customer is using these solutions. This customer perspective was drawn from an interview with cyber security personnel at a large healthcare services provider.

Any healthcare services company is responsible for safeguarding a tremendous amount of extremely confidential data—security cannot be an afterthought. The systems processing, storing, and transmitting this data represent a wide variety of device platforms that combine to deliver the data in diverse forms.

Before introducing RSA NetWitness and NetWitness Endpoints into its environment, the company had several issues. Though the security team relied heavily on packet capture and endpoint information, this data was maintained by separate teams with separate systems. These teams had little operational integration and no mid-level management in common, so coordination between them was cumbersome at best. The security team in charge of investigations did not have direct access to certain types of data, and making formal requests for delivery of copies was required to pursue investigations. To top it off, the security team would receive the data raw and unparsed, with no metadata. Reporting was a manual process that required cobbling data together from several different tools.

After implementing RSA NetWitness and NetWitness Endpoints, the situation improved significantly.

Now, the security group has much greater visibility into its security data because it is piped directly into RSA NetWitness from the respective network points and systems. Using the now-unified data, NetWitness creates confidence ratings for alerts, which has led to both higher accuracy when determining security threats and vastly improved work prioritization, thus reducing risk to the environment.

When responding to incidents, the security team values the network and endpoint visibility they get from RSA NetWitness and RSA NetWitness Endpoints. For example, once an alert against an internal host is presented in RSA NetWitness, the security team can pivot on the IP address to determine what other alerts have been presented against that host, or they can pivot on the alert to determine what other hosts in the environment have been exposed to the same threat. Using the IP address (or DNS information), the analyst can pivot into NetWitness Endpoints to get more details about the host in question and perform further investigation or remediation activities remotely.

Before the deployment, the healthcare provider had also been plagued by false-positive alerts that wasted the time of its limited staff. The RSA NetWitness–NetWitness Endpoints combination has also dramatically reduced the false positives by providing better context with its metadata.

Not only has the metadata improved accuracy, the RSA NetWitness alert filtering has also significantly improved the security team's ability

> The benefits the company has gained by being able to combine deep packet inspection and endpoint data and augment them with unified metadata has been tremendous for accelerating investigations and closing incidents. Investigations have been reduced from hours or days to just minutes or hours, leading to a 10X reduction in resolution time!

to retrieve data and focus only on information that is relevant to the current situation. They were using a top five antivirus provider that was creating a huge number of false infection alerts, but by using RSA NetWitness and NetWitness Endpoints together they were able to isolate and remove these false positives from the investigation queue.

The benefits the company has gained by being able to combine deep packet inspection and endpoint data and augment them with unified metadata has been tremendous for accelerating investigations and closing incidents. Investigations have been reduced from hours or days to just minutes or hours, leading to a 10X reduction in resolution time!

EMA Perspective

Organizations today face a high level of complexity when trying to secure their systems and data and must address a stunning number of issues, such as the ever-expanding number and types of endpoints, the sophistication of threats being used against them, and the sheer amount of security data being produced and captured, to name a few.

To deal with these issues, organizations need better information, analysis, and prioritization to identify and act on the most important security threats.

Generally, organizations have relied on either endpoint or network-sourced security data to make decisions. But in order to have optimal situational awareness they really need the combination of network and endpoint security and the ability to enrich that data with metadata and use it for both detection and response. Only through this combination can organizations have *all* the information they need to effectively identify and respond to security threats.

RSA NetWitness and NetWitness Endpoints provide an opportunity for security organizations to propel their security operations and analysts forward. Using a single interface with all the relevant data for both detection and investigation, combined with the drill-down and pivoting capability between the two products, allows a high degree of flexibility for the investigation of events and incidents.

When used together, RSA NetWitness Endpoints and RSA NetWitness provide visibility and agility at levels unparalleled by other tools that use more limited data feeds. Together they provide a comprehensive security monitoring solution, accelerating incident detection and investigation and significantly reducing the time to resolve. This provides a high return on investment for both security and IT operations teams.

About RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3334.063016