It's About Time: Accelerating Threat Detection and Response

Minutes. That's all you and your team have before a cyber threat can compromise your organization. According to the Verizon 2017 Data Breach Investigations Report, in 98% of the breaches,[1] it took just minutes to compromise the endpoint. It looks like the halcyon days of simple viruses and worms deflected by basic antivirus and firewall protections are long gone. Today's cyber attacks are unparalleled in sophistication and frequency and, with the broader digital transformation being undertaken by many organizations, the potential attack surface for organizations is growing exponentially. With the advent of the cloud and an increasingly more mobile workforce, an organization's servers and endpoints can't be protected by four secure fortress walls anymore. Employee laptops are used off premises on untrusted networks and then brought back—warts and all—into the trusted environment. Encrypted traffic is expanding—both internally and externally—as organizations comply with increasingly stringent privacy requirements and seek to better protect customer and corporate data. In addition, cloud services and deployments arguably increase productivity and convenience, but security monitoring and pervasive visibility into threats in these environments continue to be challenging.

With the advent of the cloud and an increasingly more mobile workforce, an organization's servers and endpoints can't be protected by four secure fortress walls anymore.

Is it any surprise that 75% of organizations are unsatisfied with their current ability to detect and investigate threats? Or that only 11% of organizations say that they can investigate attacks very quickly?[2] Time is just as much of an adversary as are our attackers.

So, what's missing?

Naturally, organizations of all sizes will have many challenges—both business related and security-related—that pertain to their ability to respond more efficiently and effectively to threats. It's no secret that there is a real "skills gap" in the cybersecurity industry. In the 2017 Global Information Security Workforce Study, Frost & Sullivan forecasted a 1.8 million security professional shortage by 2022.[3] Clearly, this distinct lack of available human resources will affect every organization. In addition and often in response, organizations begin stacking disparate security products that then bombard their security teams with an ever-growing number of alerts, which creates both too much noise and an inordinate amount of extra work with no real value in combating threats.

Ultimately, to be successful, an organization must address three core challenges:

- **Difficulty in assessing which are the real threats that matter t he most**—More threats mean more alerts. More alerts mean more valuable time wasted on potential false positives.
- **Incomplete visibility that prevents them from seeing the scope of the (larger) problem**—With multiple sources of threat data from the endpoint to the cloud, security teams are challenged to pull the data together in meaningful ways to better understand the full scope. This challenge is only exacerbated when you have a shortage of skilled security analysts who actually know how to do the often time-consuming investigation work.
- **Lacking context that is vital to prioritize investigation and response**—Who is the target of the threat? Is it your CEO or is it the marketing intern? Is it an asset with intellectual property and financial records or an asset with a college résumé? For security analysts, knowing which one is which could be the difference between stopping the threat or letting data be exfiltrated.

Evolved requirements for threat detection and response

So what can organizations do to combat fewer resources or manage the unprecedented amounts of threat data bombarding them every day? Organizational visibility must be made more useful and actionable. This means obtaining deep, pervasive visibility into the right assets and resources.

Organizational visibility must be made more useful and actionable. This means obtaining deep, pervasive visibility into the right assets and resources.

But visibility isn't enough. Security teams can rise up to face their challenges more effectively when their visibility is paired with three things:

1. **Deeper insights and more complete information for faster detection and response**—By pairing visibility with analytics, your team can gain deeper insights into user behavior, device type and other variables. As "best practices" to maximize depth and quality of insight, security operations should apply an assortment of techniques such as behavioral analytics, data science modeling and machine learning.
2. **Broader understanding from a more complete view of the full scope of an attack campaign**—Threat data is only as valuable as how actionable it is. Disparate sources will require more manual labor to "connect the dots." Arguably, security operations should look for integrated data sources as well as threat intelligence from community and expert sources to better correlate isolated incidents and respond before the business is breached.
3. **Increased context that is invaluable to your team for prioritizing which threats are the most important**—A greater awareness of context—particularly business context—is absolutely essential for your team to better prioritize investigation and response. When multiple threats are detected, security teams can rely on business context to understand which asset poses the greatest business risk.

These capabilities are vital for security operations to better recognize the true nature of a threat, confidently decide how to prioritize re sponse and then quickly take action based on that decision.

Accelerating threat detection and response with NetWitness® Platform

Here at NetWitness, we've developed an integrated suite of technologies designed to directly address these challenges. We call it the NetWitness Platform. The platform delivers end-to-end visibility across the organization. It does all this from one central console that pulls in data from logs, packet capture, endpoint telemetry and NetFlow—from on-premises deployments up to the cloud. With the integration of business context to better determine risk, the NetWitness Platform immediately exposes the most important and high-risk threats across the organization, optimizes security processes to drastically reduce attacker dwell time and prioritizes response to target the threats that matter most to the business.

In addition to the platform's own modular monitoring capabilities, it also can consolidate alerts from your existing security point products, so it can truly serve as a centerpiece of your security operations. Uniquely, NetWitness Platform enriches the data it takes in—whether from its own modules or from other products—with rich, contextual metadata about business context, identity and threat intelligence through a patented process. This means that instead of "dumping" more alerts in your overstuffed analyst work queues, NetWitness Platform leverages machine learning, advanced analytics and behavior modeling to automatically correlate indicators, behaviors and enablers of compromise that would be absolutely impossible to match on a manual basis with human skills. This provides your team with valuable prioritization of the threats that matter the most, casting them in plain view for your analysts to see and investigate.

In addition to the platform's own modular monitoring capabilities, it also can consolidate alerts from your existing security point products, so it can truly serve as a centerpiece of your security operations.

NetWitness Platform offers a highly intuitive and blazing fast user interface that was designed and tested through thousands of hours of observations and interviews with security teams. Respond and Investigate workflows make it easy for security analysts to triage information rapidly by presenting all vital, correlated threat information across all data sources on one screen. The Suite is also a favorite for threat hunters, who can be even more impactful in their incident response roles. From novice to hunter, these workflows will make any security analyst better at defending their networks.

Ultimately, the NetWitness Platform interweaves business context and risk with the most advanced cybersecurity capabilities to help the entire organization—from the CEO and CISO to the security operations center—make stronger decisions to protect themselves from known and unknown threats, minimize attacker dwell time and mitigate negative business consequences.

Threats move fast. Move faster.

Get the insight and context your security team needs to respond to the most advanced cyber threats fast, with the NetWitness Platform. Implementing it is a straightforward process. Professional Services or Partners can deploy and configure the NetWitness Platform and help your team accelerate their detection of threats already lurking on your network and shore up their response to future attacks.

For more information or to get started with the NetWitness Platform, visit rsa.com/domore or visit the RSA Link Community.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to netwitness.com.

1. Verizon 2017 Data Breach Investigation Report (DBIR)
2. RSA Threat Detection Effectiveness Survey 2016
3. Source: 2017 Global Information Security Workforce Study.

NETWITNESS
An RSA Business