

MARCH 2022
Newsletter #28

INFOGRAPHIC

The 7 Building Blocks of
Threat Visibility

OPINION

The Evolution of Intelligent
Threat Response Tools

GUIDE

Your Journey to Evolved SIEM

BUSINESS

XDR versus evolved SIEM
– What's the Difference?

DEFENDING AGAINST THE LATEST RANSOMWARE ATTACKS WITH NETWITNESS

Powered by

 **NETWITNESS**
An RSA Business

NOT WHAT IT SEEMS

FINDING YOUR WAY
THROUGH THE THREAT LANDSCAPE



EDITOR'S NOTE

MODERN PROBLEMS REQUIRE MODERN SOLUTIONS

Leading computer and network security company RSA, in its recent paper, said that many cyberattacks don't even need malware—just compromised credentials will suffice. This statement sets alarm bells ringing in light of the ongoing digitalization and the proliferation of internet-facing devices. And with ever-evolving vectors, hackers are naturally incentivized.

Security teams, equipped with Security Information and Event Management (SIEM), are successfully fending off threats. However, SIEM and analytics tools accompany a degree of operational complexity. If anything, the status quo demands automated responses, rapid event triage and correlation, and process optimization. Also, security teams need to have built-in intelligence platforms, to unearth operational blind spots and improve learning curves.

Network security companies specializing in evolved SIEM and Extended Detection and Response (XDR) are meeting this need. As opposed to traditional SIEM, evolved SIEM optimizes from threat detection to response. It is a single, unified platform for contextualization, orchestration, investigation, and reporting—which empower security teams to stay agile and efficient.

Concurrently, XDR platforms offer a combination of network detection and response (NDR), endpoint detection and response (EDR), and SIEM. The underlying principle of XDR is the creation of a synergistic system that maximizes correlation and analysis capabilities. Although evolved SIEM and XDR are alike in so many ways, evolved SIEM facilitates recordkeeping and compliance reporting. So, depending on existing security infrastructure and future provisions, organizations can incorporate XDR or evolved SIEM and fortify their security postures.

Cyber-ready organizations are leveraging solutions to formulate a Zero Trust approach to threats. Irrespective of the adopted solution, the expected results are the same: proactive defences, efficient processes, and fool-proof postures. And between the adopters, they unequivocally agree that modern problems require modern solutions.

The writer is the Technology Editor and ROI Strategist at Dubai-based CXO Strategies. She can be contacted via twitter @CXOConnectME

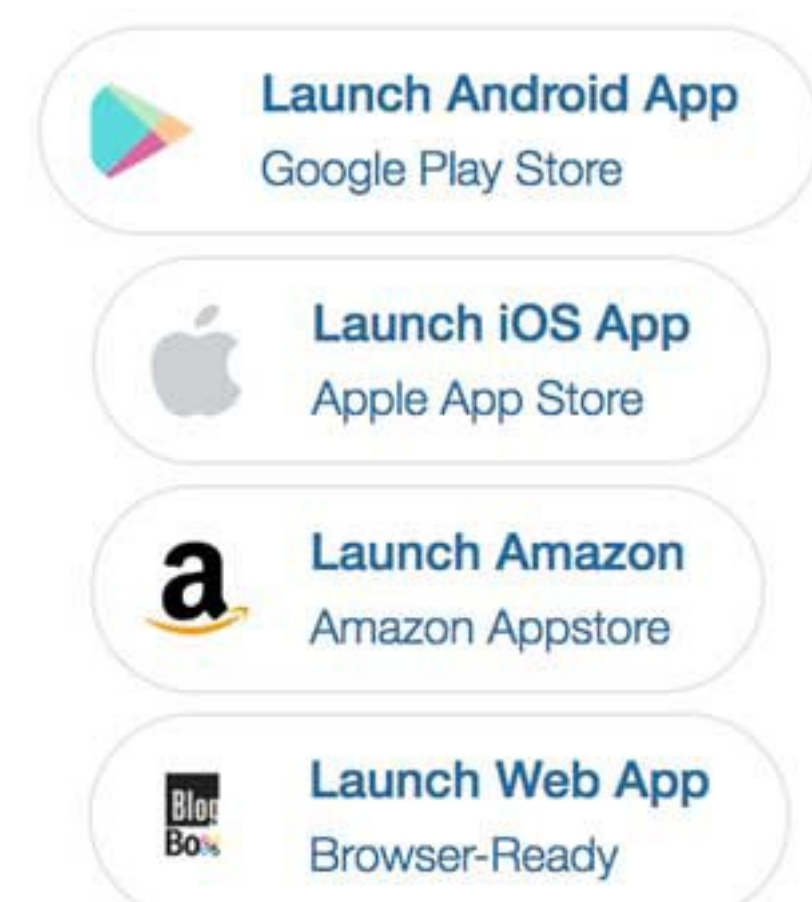


KAVITHA RAJASEKHAR

Technology Editor and ROI Strategist at Dubai-based CXO Strategies

Twitter: [@CXOConnectME](https://twitter.com/CXOConnectME)

The only thing that shapes Opinion is opinion itself. CXO Blog Box is an industry compilation of insights and opinions. Our focus is to curate the opinions shaping the tech industry



The 7 Building Blocks of Threat Visibility

HOW TO TACKLE A KEY CHALLENGE OF THREAT DETECTION AND RESPONSE

With mobile, cloud, and the Internet of Things (IoT) creating new openings for cyber threats, your organization is at greater risk than ever. So you need more visibility than ever to detect threats and respond to them effectively.

VISIBILITY:
IF YOU CAN'T SEE IT,
YOU CAN'T STOP IT.



86% of organizations collect, monitor or analyze log data and endpoint data...



50% of IT leaders worry about understanding the full scope of an attack



74% of organizations collect, monitor or analyze data from network packets...



48% of IT leaders are concerned about their ability to detect an attack in progress




10% say they're able to correlate data from different sources very well

WHAT YOU NEED:

7 BUILDING BLOCKS OF THREAT VISIBILITY


INCIDENT LOGS


ENDPOINT DATA


NETWORK PACKETS


CLOUD APPLICATIONS


DATA ANALYTICS


THREAT INTELLIGENCE


BUSINESS CONTEXT FOR THREATS

GET THE THREAT VISIBILITY YOU NEED, WITH [NETWITNESS® PLATFORM](#)

Source: "Information Security Strategies in the Age of Zero-Day Threats," Gatepoint Research PulseReport commissioned by RSA, April 2017

The Evolution of Intelligent Threat Response Tools

One of the unintended consequences of accelerated digitalization is the rapid proliferation of cybersecurity threats. Exponentially increasing attack surfaces, the constant churn of emerging technologies, and significantly more sophisticated attacks are escalating our tech-related vulnerabilities.

83%

IT professionals surveyed for a recent report⁽¹⁾ were concerned about threats posed by web applications

67%

Had either completed, or where undertaking a Zero Trust implementation. Clearly, cybersecurity pros are taking the downside of tech-adoption very seriously, to face a new generation of threats.

With the Internet of Things becoming a critical technology across virtually every industry, IoT devices and the Cloud has resulted in a massive surge in new entry and exit points, to the systems they are part of. Globally, IoT-enabled devices are projected to reach 30.9 billion units by 2025⁽²⁾, and the amount of data stored on cloud servers will have surpassed 100 Zettabytes—or 100 billion terabytes⁽³⁾ by then!

Intelligent Threat Response: Understanding the toolkit

Security Information and Event Management (SIEM) tools have been a longstanding part of cybersecurity initiatives, especially as a log management and data integration tool across event analysis, early detection, and response. Having integrated such data and system-wide visibility, a centralized Security Operations Center (SOC) allows cybersecurity analysts to continuously monitor and analyze an organization's networks, servers, and connected devices to drive the remediation process.

Security Operations, Automation, and Response (SOAR) solutions help analysts at the SOC prioritize and process security events and threats, and coordinate the response, while also ensuring adherence to policies and streamlining workflows and reporting. Extended Detection and Response (XDR) tools enhance these capabilities to the next level, by normalizing and correlating security and incident data—across IoT, cloud, network, server, asset, identity, and endpoint layers—to enhance detection, analysis, and response.

Evolving to keep pace with threats

For any cybersecurity response to be effective, it has to be resilient against the volume and complexity of threats.

A 2020 survey⁽⁴⁾ found that synthesizing the results of their multiple security tools was a challenge, to an overwhelming 75% of organizations. This is inherently problematic. If a hacker or malware altering privileges, then downloading information, are seen as separate incidents, they could be confused with false positives—undermining detection, analysis, and response.

Addressing such, and other limitations of traditional cybersecurity tools, is the motivation behind solutions like NetWitness, an RSA company. Introducing the next generation SIEM and XDR solutions, such cybersecurity and digital risk management platforms go beyond traditional SIEM, by delivering comprehensive transparency from endpoint to the cloud—to identify threats, integrate organizational security tools, and generate effective responses.

Logs can help identify that an event has occurred; packets are the key to identifying the exact event, and your endpoints are where the threat's footprints can be used to unlock insights. Now multiply this across all devices in a network, and the challenge becomes obvious. Evolved SIEM and XDR platforms enable true visibility across logs, packets, and endpoints—both deep in specifics and broad in scale. And because these emerging solutions are highly effective at capturing and archiving security data, audits and reports are instantly accessible.

Evolved SIEM and XDR platforms integrate, and deliver on, the 7 building blocks of threat visibility: Incident Logs, Endpoint Data, Network Packets, Cloud Applications, Data Analytics, Threat Intelligence, and the Business Context for threats. The next-gen XDR detects known and unknown attacks, and automates the incident response, while giving security teams access to a fast and powerful user interface.

The logs generated deliver visibility across all the industry-leading devices, applications, and operating systems; and the network data is collated and analysed in real-time. Such solutions also create transparency of endpoints, continuously monitoring threats, across workstations, laptops, servers, and virtual machines. Crucially, these enhanced solutions are able to rationalize people, technology, and initiatives, ensuring coordinated efforts and quick decision-making.

AI-enabled Threat Response: Next-Gen Tools empower Next-Gen Approach

At the heart of this evolution in IT threat response solutions is the use of AI, which enables rapid detection of unknown threats, with the response and remediation process continuously evolving its Machine Learning algorithms, and empowering Cybersecurity teams. Although AI is being recruited by malicious actors, the most significant impact of these intelligent cybersecurity tools is in their ability to enable the use of powerful, collaborative, and interactive digital solutions, within organizations—without them being held back by more complex threats.

A truly effective Zero-Trust approach, which would be operating under the presumption that every interaction is a potential threat, would be impractical and counterproductive. The next generation of evolved SIEM and XDR solutions is enabling real-time analysis, system scale integration, cloud storage, and mobility, at the scale to embrace a digitalized future. The brave new digital world of tomorrow is on the horizon, and Intelligent Threat Response tools are ensuring that this evolution does not lead to increased vulnerabilities.

Sources:

1. [2022 AT&T Cybersecurity Insights Report](#)
2. [Internet of Things \(IoT\) and non-IoT active device connections worldwide from 2010 to 2025](#)
3. [The World Will Store 200 Zettabytes Of Data By 2025](#)
4. [ESG Research Note Says Stellar Cyber's Open-XDR Aligns Well with Firm's SOAPA Architecture](#)

The writer is the Technology Editor and ROI Strategist at Dubai-based CXO Strategies. She can be contacted via Twitter @CXOConnectME



Defending Against the Latest Ransomware Attacks with NetWitness

Ransomware continues to be a scourge upon the world's digital infrastructure. As noted by the Institute for Security and Technology's Ransomware Task Force in 2020, ransomware attacks on organizations resulted in, on average, 21 days of downtime, 287 days to fully recover, with over \$350 million in ransoms known to be paid, and an average ransom of over \$312,000. It's easy to feel that the bad guys have gained the upper hand.

Yet, while ransomware is a particularly noxious and damaging type of cybercrime, it's really just the latest wave in a war that's been waged continuously since NetWitness, an RSA company, was first developed 25 years ago. From a cybersecurity perspective, ransomware is reliant on the same type of tactics, techniques, and procedures (TTPs) as other types of cybercrime such as economic espionage, data exfiltration, and identity theft. It generates similar indicators of compromise (IOCs) and behavioral signatures, which can be detected and used to neutralize attacks with sophisticated tools employed by skilled threat hunters.

NetWitness customers, and our own threat hunters and researchers, understand this basic premise and battle ransomware actors continuously. Having proactive defenses in place greatly lowers the risk of the types of substantial damages cited in the Ransomware Task Force report. NetWitness stands shoulder to shoulder with the rest of the cybersecurity industry in sharing threat information and detection techniques, while constantly improving the platform's ability to successfully defend against cybercrime evolutions such as ransomware.

Supply Chain Ransomware

The latest example of this evolution is supply chain ransomware, as seen in the Kaseya attack. In this case, the infamous REvil ransomware gang combined ransomware with a supply chain attack, making it possible to attack many victims at once—a novel technique that greatly increased the impact and potential profitability of their criminal efforts. Burying the ransomware in software from Kaseya, a provider of IT/security management solutions for managed service providers (MSPs) and small to medium businesses (SMBs), REvil was able to infect many of Kaseya's customers, and Kaseya's MSP customers' customers, in a single act.

The NetWitness Platform: Defending Against Ransomware Attacks

Because ransomware, like other advanced persistent threats (APTs), must first breach a target and conduct reconnaissance to locate important assets, using well-understood tactics such as credential harvesting and network traversal, there are signals that can be targeted for detection. Finding the attack before the ransomware is detonated is critical.

NetWitness users have a range of powerful tools available, including visibility across network packets, system logs, PC and server endpoints, and Internet of Things (IoT), among data center, cloud, and virtualized systems. This makes it extremely difficult for ransomware and other exploits to hide while performing their necessary activities.

Through continuous real-world usage, NetWitness security researchers have developed a vast library of assets that help NetWitness users—and users of other systems, as intelligence sharing is a core value among cybersecurity professionals—to quickly identify new attack variants including ransomware. Some of these resources include:

🔑 **Using NetWitness to Detect Ransomware Attacks**

a step-by-step guide detailing how businesses can use the platform to identify anomalous behaviors and prevent successful attacks

🔑 **How to Begin Looking for Malware with the NetWitness Platform**

a how-to video detailing manual malware analysis and binary identification using the NetWitness Platform

🔑 **Detecting and Responding to a Ransomware Attack**

an infographic listing steps to safely detect, investigate, and respond to an attack

🔑 **Maze Ransomware Detection with NetWitness**

a technical guide to detecting Maze ransomware focused on NetWitness Network

🔑 **Strategies for Managing Ransomware Risk in Healthcare**

a white paper discussing ransomware in highly-targeted industries

The latest guide, appropriately, is **Detecting and Responding to Kaseya Ransomware** with the NetWitness Platform, which provides specific technical content on how to detect the Kaseya attack using the NetWitness Platform, and the specific steps to take to respond.

Summing Up

The continued use of ransomware is dominating headlines, due to its high impact and continuing innovation in things like Supply Chain Attacks and Ransomware as a Service (RaaS). And while a

lot of appropriate attention is focused on geopolitical efforts to deny ransomware practitioners the safe harbor they require, it's safe to say that ransomware – like other types of cyber-attacks – will always be with us in some form. Organizations seeking to defend themselves and reduce the risk of catastrophic outcomes can act today with a leading cyber defense platform like NetWitness.

**Finding
the attack
before the
ransomware
is detonated
is critical.**

Sources:
<https://www.netwitness.com/en-us/blog/fight-ransomware-with-netwitness/>

Can your SIEM do this?

Security Information and Event Management



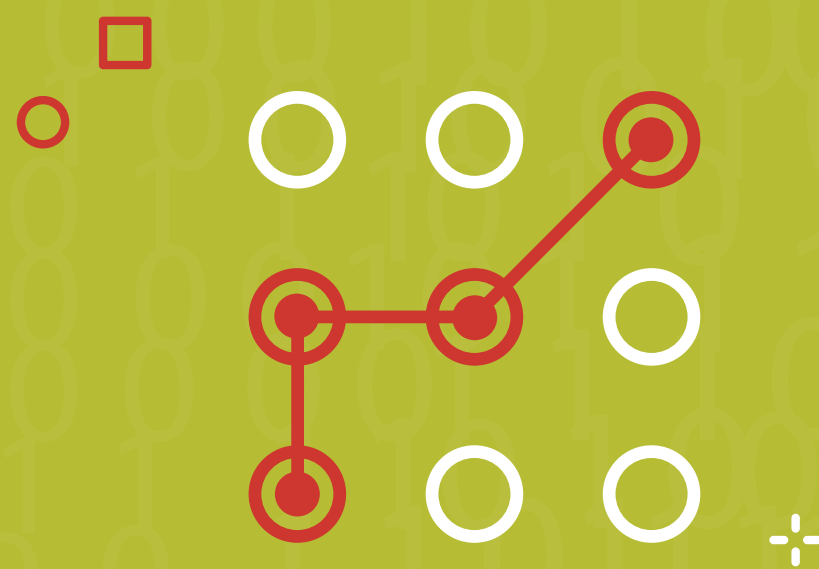
See the threats that matter

The NetWitness Platform is the only solution that allows you to see everything with point in time identification, real-time analytics, and full historic data from across your entire network. When your team spends less time digging they have more time to look ahead and operate strategically.



Incident response done right

NetWitness has your back. When an incident happens, you can count on our IR team to respond immediately and comprehensively to close the breach and reestablish security. In fact, organizations around the world use NetWitness for their own internal IR needs. Our IR team is one of the few in the industry certified by the NSA.



More visibility means better detection and response

The NetWitness Platform provides the deepest and broadest visibility through Logs, Packets, and Endpoint to help you define "how bad is it." Logs identify something has gone wrong. Packets actually tell you what occurred. Endpoint gives you deep insight into each and every machine on and off your network.



Find the full scope of the threat

It's about connecting the dots in real time so you don't miss something. And, you can't do that without end-to-end visibility and behavior analytics to find the threats that would normally fly under the radar. Once you understand the full scope of what you are dealing with, you need to take prioritized action to stop an attacker before damage is done.



The NetWitness Platform provides the deepest and broadest visibility through Logs, Packets, and Endpoint to help you define “how bad is it.”

The NetWitness Platform is more than a SIEM, it is a holistic view of your infrastructure – from the endpoint to the cloud – that allows you to quickly identify and respond to the threats that matter. The NetWitness Platform was designed to be the foundation of your security strategy, the hub that easily connects with your suite of security tools. It reduces dwell time and provides a prioritized view that encompasses the full scope of the threat.

The power of full visibility

If you can't see it, you can't detect it. Other SIEMs are heavily reliant on logs and are blind to the cloud. The NetWitness Platform consumes disparate data from across your entire network and makes it intelligent in real time. Network packet data sees everything. Deep endpoint data, at the kernel level, identifies if a file is behaving differently on disc vs. in memory. Indexing and correlation capabilities extend across metadata from all these sources, so analysts can detect known and unknown threats, see the complete scope of an attack, and reduce business impact.

Why good enough isn't good enough

Not all packet capture technology is created equal. Solutions that only start capturing data when an alert triggers only give you partial ability to investigate an attack and have no ability to detect the threats that may be flying under the radar. The NetWitness Platform captures and enriches full network packet data, along with other data sources, and creates a uniform metadata model across all data types, allowing you to find the attacks that logs miss.

Compliance is the by-product of security done right

Because the NetWitness Platform captures, retains, and archives data to support your security needs, you are already prepared for an audit and enabled to share your out-of-the-box compliance reports with regulatory bodies.

Visit [NetWitness.com](https://www.netwitness.com) to learn more.

*Sources:
Evolved SIEM – Security Information and Event Management – NetWitness*

Your Journey to Evolved SIEM

THE MISSION

Even with increasing focus on security, breaches still occur at record rates. Whether it's outsiders stealing and misusing personal data, phishing or malware attacks through company emails, or nation-states trying to disrupt critical services, cybercriminals are constantly evolving their craft in attempts to stay undetected as long as possible.

These serious threats to your finances and reputation make it critical that your organization embrace an equally important mission: to continuously evolve security information and event management (SIEM) as the centerpiece of your security operations.

Evolved SIEM gives you deeper visibility into endpoints and network traffic, accelerates threat detection and response, and incorporates business context to prioritize threats and security incidents.

PERVASIVE
VISIBILITY

ADVANCED
ATTACK
DETECTION

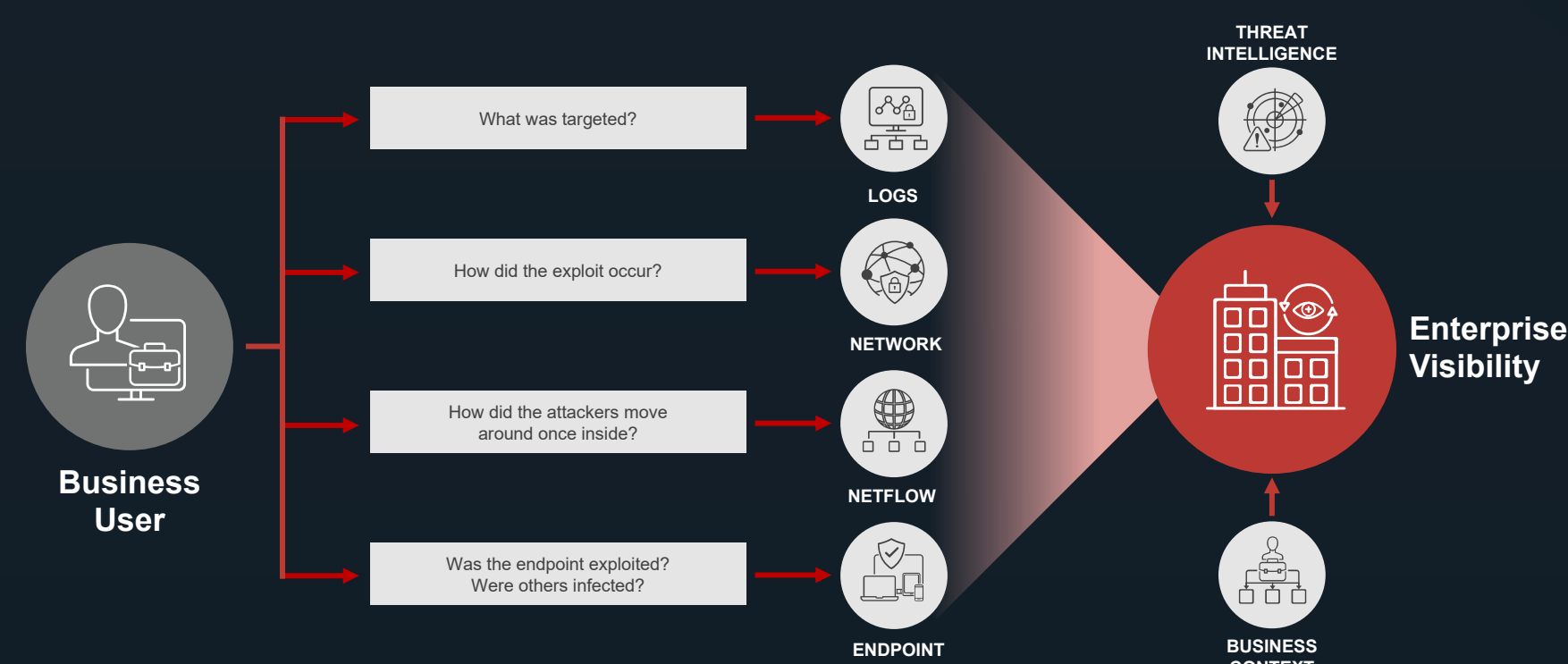
INVESTIGATION
AND RESPONSE

CONNECTION
TO THE
BUSINESS



PERVASIVE VISIBILITY

To get a complete picture of your enterprise security and answer all of the important questions, you need visibility—and context—across logs, packets, NetFlow and endpoints. That includes the ability to collect and normalize data from on-premise, virtual and cloud infrastructures.



WHAT TOOLS AND PROCESSES DO I NEED?

Log monitoring

Network traffic
analysis and forensics

Endpoint detection
and response (EDR)

Cloud and virtualized
environment support

WHERE ARE YOU ON THE PATH OF PERVASIVE VISIBILITY?

Examine the breadth and depth of your current visibility across:

- Logs, network, endpoints and NetFlow
- On-premises, virtualized and cloud environments
- Integrations and parsers

Evaluate your collection strategy:

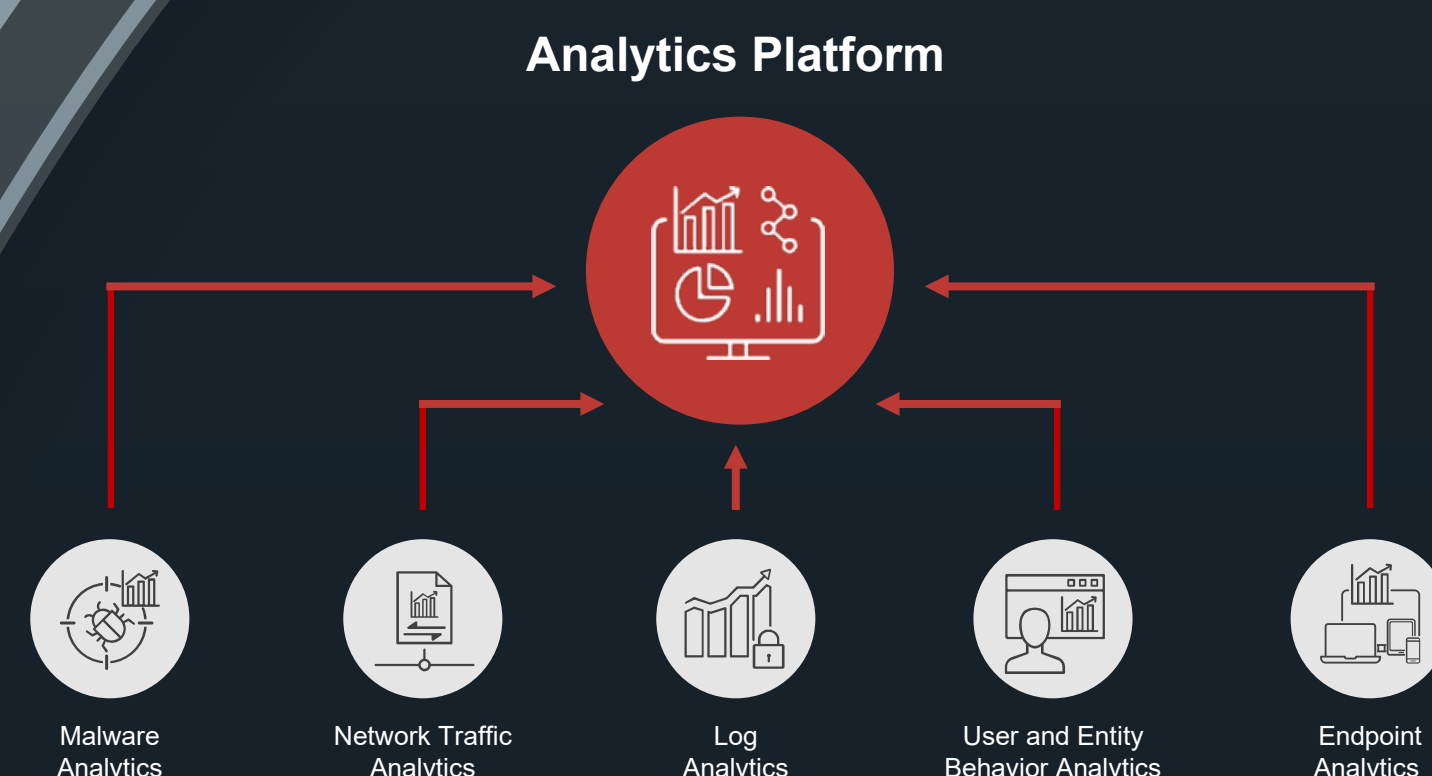
- Do you have multiple repositories?
- Is the data normalized for analysis?
- Do you apply metadata at collection time?
- How do you store and manage data over time?



ADVANCED ATTACK DETECTION

To detect attacks, you need a multifaceted analytics approach that:

- Detects anomalous user behavior—even across a large number of events—to find unknown threats
- Uses unsupervised statistical anomaly detection to identify unknown threats
- Applies advanced correlation rules across all data to identify known threats
- Keeps a library of known threat indicators
- Interacts with third-party and community threat intelligence



WHAT TOOLS AND PROCESSES DO I NEED?

Security analytics applied to logs, network and endpoint data

Threat intelligence

User and entity behavior analytics (UEBA)

HOW WELL CAN YOU DETECT ADVANCED ATTACKS?

Examine your ability to identify attacks and compromises using:

- People, processes and technology framework
- Computer science and AI (big data and machine learning)
- User and entity behavior analytics (UEBA)

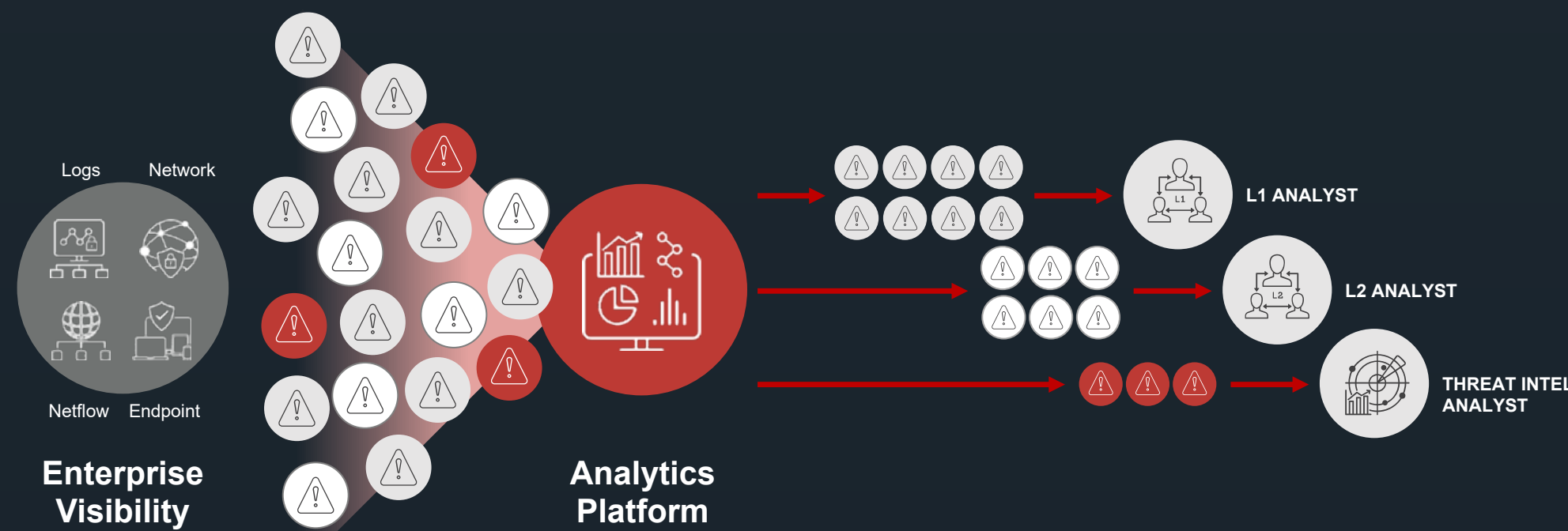
Evaluate your readiness:

- What systems and tools are in place for threat detection?
- Have you deployed UEBA capabilities?
- How advanced are your current analytics? How well can they detect anomalies?
- Are you capturing all the data you need for effective detection?
- Are you fully leveraging threat intelligence?



INVESTIGATION AND RESPONSE

To eradicate attacks and mitigate business risks, you can't rely on technology alone. People and processes are just as important as tools. How well can you understand the full scope of an attack—and how quick and comprehensive is your response?



WHAT TOOLS AND PROCESSES DO I NEED?

Orchestration and automation

Playbooks and machine learning

Collaborative incident response

HOW RAPID AND ROBUST IS YOUR INVESTIGATION AND RESPONSE?

Examine your ability to identify and react to attacks using:

- Incident management
- Automation and orchestration
- Dashboards and reporting
- Security, Orchestration, Automation and Response (SOAR) framework

Evaluate your SOAR requirements:

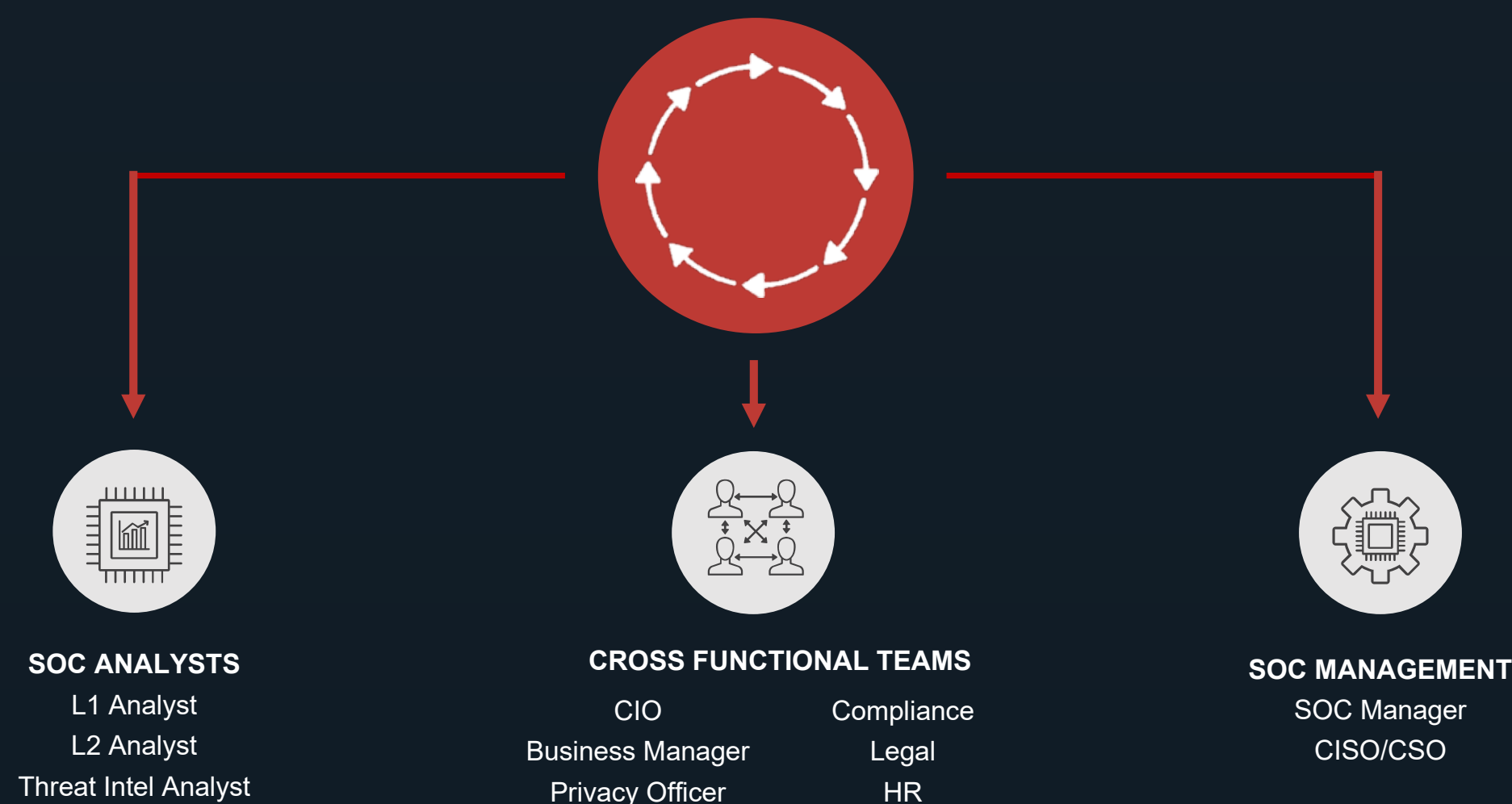
- Can you manage incidents collaboratively?
- Can you automate common tasks effectively?
- Do you have an orchestration solution (leveraging security and nonsecurity tech)?



CONNECTION TO THE BUSINESS

Are your priorities for IT security aligned with business risk?

Prioritize and Orchestrate



WHAT TOOLS AND PROCESSES DO I NEED?

Asset criticality assessment

Connections between risk and IT security teams

Cyber risk quantification

HOW RAPID AND ROBUST IS YOUR INVESTIGATION AND RESPONSE?

Examine collaboration between your IT security and business risk teams:

- Does your organization regard security breaches as a business risk, not just an IT risk?
- How's the working relationship between the two groups?
- Do business risk personnel feel responsible for IT risks (and vice versa)?
- Have you quantified the impact of various digital risks?

Evaluate your IT risk strategy against business risk imperatives:

- Do you have systems and processes that inform IT security about business risk strategy?
- Do your tools automatically integrate IT risk and business risk?
- Does executive management (CISO/CRO) prioritize collaboration at all levels?
- Do both IT and business risk manage your incident response plans?

Rapid investigations

Single, unified platform for all your data

Automated behavior analytics

Benefits of an Evolved SIEM

Flexible, scalable architecture

Integrated threat and business context

End-to-end security orchestration and automation

NETWITNESS EVOLVED SIEM

The NetWitness Platform uses an evolved SIEM approach that empowers security teams to quickly detect and respond to threats. It proactively watches for activities signaling the presence of active exploits across logs, network, endpoints and NetFlow. And it leverages deep analytics, with machine learning, advanced threat intelligence, and user and entity behavior analytics (UEBA), to improve analyst productivity.

Source: Extract from RSA EBOOK: YOUR JOURNEY TO EVOLVED SIEM

XDR and Zero Trust: Partners in Threat Detection

By Spencer Lichtenstein, Brian Robertson, Karim Abillama

Are **Extended Detection and Response (XDR)** and **Zero Trust** simply two new security buzz words?

There is a lot of talk about both, but the deeper question is, “Are they related, and if so, how?” To level set the conversation, let’s look at why implementing Zero Trust as part of XDR strengthens an organization’s threat detection.

The premise of XDR is that XDR collects and automatically correlates data across multiple security layers (identity, asset, user, endpoint, email, server, cloud workloads, network, and IoT) so threats are detected faster and security analysts improve investigation and response times.

The premise of Zero Trust is that enterprises should not inherently trust any attempt to connect to a business system or application—and must be verified before any level of user access is granted.

There’s a vital relationship here—but why is it so critically important to cybersecurity?

How We Got Here

Before we examine how XDR and Zero Trust are related, we need to understand why they are building blocks to threat detection and response.

The way in which organizations operate securely is transforming due to **seismic shifts in how employees access information** and other macro-pressures, especially during this new working world of remote access during a global pandemic.

These new realities are forcing companies to **accelerate their digital transformation** by expediting large transformational projects. This results in a massive expansion of the threat landscape at a faster pace than most would have expected, created in part by:

- ⊞ Acknowledging remote workers accessing sensitive information from many devices globally
- ⊞ Changing approaches to data storage, causing many organizations to migrate their traditional physical data centers to dynamic cloud infrastructure
- ⊞ New applications being developed, adopted, and moved to production at a rapid pace, often using publicly available code structures

As these adjustments are embraced, here’s the rub: they carry increasing security challenges.

Security Challenge 1

The expansion of connected users and devices from remote workers that extend beyond the physical boundaries of the company

Security Challenge 2

Third-party infrastructure that diminishes an organization’s ability to administrator granular controls

Security Challenge 3

Rapid adoption of new software with wide-ranging codebases and versions, often outside an organization’s control

Companies need to rethink security in the present. And future. Any device attaching to the network, any application being moved into production, and all users must be scrutinized.

Zero Trust Required, Not Optional

The erosion of the security parameter paved the way for Zero Trust requiring organizations to find new ways to establish trustworthiness.

Traditional security has always said, “Trust, but verify.” But Zero Trust says, “Never trust, always verify.” Zero Trust security never really clears anything. Instead, Zero Trust considers all resources to be external to an organization’s network—continuously verifying users, resources, devices, and applications before granting only the minimum level of access required.

Zero Trust is proving to be a **strong solution to addressing security holistically** with the ability to keep up with the shift and expansion of the threat landscape.

If an organization implements tenets of Zero Trust, they have a significant risk reduction when they accelerate digital transformation initiatives. For example, rapid adoption of new software applications, or a new IaaS provider for a critical project all become a natural part of your “security glue” because Zero Trust assumes nothing is trusted until it actually proves to be trusted.

Keeping this in mind, security organizations need a mechanism that constantly surveys the environment and identifies known risks and emerging or unforeseen new threats across every attack surface anywhere in this modern, expanded infrastructure. That’s where XDR comes into play.

XDR: A Key Component to a Zero Trust Approach

Look at how the **National Institute of Standards and Technology (NIST)** interprets Zero Trust. Here are some compelling assessments of the need for deep visibility and speed of detection:

1 Architecture

Zero Trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.

2 Devices

Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently (including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personal devices) that may be allowed to access some, not all, resources.

3 Data

An enterprise should collect data about asset security posture, network traffic, and access requests; process that data; and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

4 Traffic

All traffic is inspected and logged on the network and analyzed to identify and react to potential attacks against the enterprise. However, some (possibly the majority) of the traffic on the enterprise network may be opaque to layer 3 network analysis tools. This traffic may originate from non-enterprise owned assets (e.g., contracted services that use the enterprise infrastructure to access the internet) or applications/services that are resistant to passive monitoring. The enterprise that cannot perform deep packet inspection or examine the encrypted traffic must use other methods to assess a possible attacker on the network. That does not mean that the enterprise is unable to analyze encrypted traffic that it sees on the network; the enterprise can collect metadata (e.g., source and destination addresses, etc.) and the encrypted traffic and use that to detect an active attacker or possible malware communicating on the network. Machine learning techniques can be used to analyze traffic that cannot be decrypted and examined. Employing this type of machine learning would allow the enterprise to categorize traffic as valid or possibly malicious and subject to remediation.

5 Network

For network requirements to support Zero Trust architecture, the enterprise can observe all network traffic. The enterprise records packets seen on the data plane, even if it is not able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE as it evaluates access requests.

XDR: Delivering Vast Visibility

The NIST paper referenced above specifically calls out the need for deep visibility in the network. If Zero Trust requires organizations “...to collect data about security posture, network traffic, and access requests, process that data, and use any insight gained to improve policy creation and enforcement” then having the ability to abstract data from every data source across the endpoint and network becomes more vital.

Layer on top of this is the ability to use machine learning analytics to identify anomalies such as new endpoints or users, or anomalous changes in behavior, and XDR becomes a powerful way to trust, but always verify, those end devices.

Leveraging automation actions through orchestration and automation when endpoints or users are deemed risky takes this approach a step further to ensure assets are swiftly removed when their trustworthiness is questioned.

For organizations adopting a Zero Trust model, the visibility of XDR is a key requirement to this cybersecurity strategy.

Traditional security has always said, “Trust, but verify.” But Zero Trust says, “Never trust, always verify.”

Speed Detection and Reducing Dwell Time

Zero Trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different or no more trustworthy than any non-enterprise owned environment.

A real-world analogy for Zero Trust: imagine a stranger going unnoticed, hiding in your residence in an area lacking surveillance. The consequences threaten both the assets you own and your own safety. Being able to instantly react and respond are critical; our human brain (one of the most sophisticated neural networks) is trained to react quickly to those emergencies.

XDR is a Zero Trust enabler when it comes to elevating the speed of detection. This is a very important concept if we consider an attacker is already present. To thwart attackers and reduce dwell time, it is imperative to act fast and be able to quickly analyze Indicators of Compromise and behavioral anomalies in a central location with all contextual information related to the business asset. The result? Efficient identity and comprehensive threat intelligence across the endpoint and network infrastructure.

An **XDR platform becomes more efficient** in invoking authentication mechanisms (suspected breach or threat) when access to end-user entitlements—a.k.a. Zero Trust—is engaged. For example, invoking a step-up authentication mechanism leveraging biometrics as a response to an XDR-identified anomaly. This is a powerful enabler for the SOC grounded in Zero Trust principles.

So how does an organization mitigate risk effectively—that makes the most sense for a company’s unique security needs? **Zero Trust is the fundamental answer.** It’s a critical enterprise-wide mindset that’s part of an XDR strategy to keep your house safe.

To learn more, check out **NetWitness for XDR** here.

*NIST Special Publication 800-207, Zero Trust Architecture:
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

2022 Cybersecurity Predictions by NetWitness

Ben Smith, Field CTO at NetWitness, an RSA business, discusses the predictions for the cybersecurity and risk management world of 2022

Nation-state actors will continue to prepare the battlefield for future action: they are canny and deliberate and are thinking about long-term gain, not short-term disruption. Social media platforms will represent the biggest, cheapest, and fastest method for an adversary to effect change in the physical world – not by destroying equipment as part of a cyberattack, but in mobilizing humans towards the adversary's goals. These are just some of the cybersecurity predictions for 2022 that Ben Smith, Field CTO at NetWitness, predicts for this year.

You and I are living in the middle of an arms race in cybersecurity – can you feel it? Adversaries are leading the way through constant evolution of attacks via new tactics or techniques, or simply new combinations of old techniques. The good guys reconfigure and retool their threat detection and response capabilities to recognize this new threat vector, which frustrates but typically does not deter the adversaries, who inevitably come back via some other path. And the cycle continues.

Especially troubling is when this week's or this month's big breach grabs the headlines, and when the details emerge, it becomes clear that the path into the victim's house wasn't a battering ram created specifically for that purpose, but rather a previously unknown weakness in how that front door was constructed years or even decades ago – a now-vulnerable front door which secures not only your home, but thousands or even millions of "homes" (connected systems, in this analogy) around the globe. This is our cybersecurity reality.

Looking forward to 2022, what should we expect in the world of cybersecurity and risk management?

Ransomware tactics will continue to evolve.

The "double-extortion" model, where your data is encrypted and the adversary simultaneously threatens to release the data, will persist. Much as there has been every year, there will be new combinations of existing tactics, as attackers continue to innovate in how they run their own revenue-generating business operations for greatest efficiency. Attacks launched from locations not addressed by the US legal system will further complicate response efforts.

Privacy legislation globally will accelerate.

Data residency will continue to be an important component at the national level worldwide. Regardless of your corporate size, if you are charged with securing your global organization, be thinking about your own architecture and where the data is collected, where it lives, and where it is handled – these may be three different jurisdictions. The flexibility of your current architecture will become even more important as new privacy regulations are passed and enforced.

The cybersecurity skills gap will only widen.

Despite the large number of educational programs and certifications designed to demonstrate proficiency as a cybersecurity professional, those numbers will be outstripped by the quantity of new jobs which must be filled. Smart organizations will relax their “perfect candidate” standards and widen the net to find good people. Do you really think that attackers have “the right security certifications” that you demand of your new hires?

The cybersecurity skills gap will only widen.

Many organizations scrambled to keep moving forward in the chaos that was early 2020, and there were shortcuts and other compromises in that compressed timeframe. Some companies found that their pre-pandemic architecture was built with assumptions about where data is typically handled — and with the remote workforce wave, these legacy data handling practices didn't keep up with new geographies. What was previously not a compliance issue may be one today. Regulators will start to notice this and take action.

Nation-state actors will continue to prepare the battlefield for future action.

Sometimes an attack against critical infrastructure is deployed to cause an immediate effect, but sometimes the attack is carried out simply to leave behind code which may prove useful to the adversary in the future. Nation-states are not petty thieves rattling door handles as they walk around. They are canny and deliberate and are thinking about long-term gain, not short-term disruption.

Social media platforms will become the fastest-growing attack surface.

Most stories about cyberattacks leading to kinetic (or physical) outcomes tend to focus on things like car hacking, medical device compromises, and other stunt-hacking proofs-of-concept. But it is today's social media platforms which represent the biggest, cheapest, and fastest method for an adversary to effect change in the physical world — not by destroying equipment as part of a cyberattack, but in mobilizing humans towards the adversary's goals. Disinformation, and its skillful development and deployment, will produce real-world physical effects.

These are some of the key areas to keep an eye on for next year. But it's poor form to offer up a slew of predictions and not to conclude without any actionable ideas of how to recognize and remediate some or all of these challenges. Here are two closing thoughts.

Plan for uncertainty, plan for resiliency.

Just because the world we live in seems to be whirling around faster and faster with adversarial attacks and fresh regulatory challenges alike doesn't give us an option to plant our flag in the ground and defend it at all costs. One of Aesop's Fables, “The Oak and the Reed,” guides us on this point: in a storm, it is the unbendable tree that is more at risk of failing, whereas the smaller, more nimble reed bends and bounces back. You and your business must remain flexible and adaptable — this is one of the many drivers leading companies to the cloud and its ease of scaling up and scaling out in very short timelines.

You cannot protect what you cannot see.

Too many organizations, driven by a check-the-regulatory-box model, decide that “visibility” means being able to collect and aggregate logs from key devices found in their operating environment. That might have been the right answer twenty years ago — but it's absolutely the wrong answer today. Log-based information — typically, text files which are produced by applications, servers and infrastructure — is operationally useful, but if you are charged with securing your environment and responding to threats both external and internal, you can't achieve true visibility unless you can peer into your network traffic and the endpoints to and from which that data is moving. Seeing those logs, network and endpoint data together is even harder when your environment is a mix of on-premise, virtualized, and cloud-based tools.



Ben Smith

Field CTO at NetWitness

Ben Smith is Field CTO with NetWitness, an RSA business. He brings more than 25 years' experience in the information security, risk management, networking and telecommunications industries. Smith holds industry certifications in information security (CCISO, CISSP), risk management (CRISC), and privacy (CIPT); he is an acknowledged contributor to NIST SP 1800-1, -3, and -7; and he is a member of the Cybersecurity Canon Committee.

INTERVIEW with Halim Abouzeid Advisory Systems Engineer, NetWitness (RSA Security)

13 January 2022

You've worked with a lot of enterprise clients in the META region, so let's start with the cybersecurity landscape. What are the top threat detection and response priorities organisations should keep top of mind?

The first priority to think about is the world of work. Whether it's a fully-remote workforce or a hybrid model, this type of new work environment is here to stay. In the META region specifically, this is the norm in most industries. So security teams have to be focused on these remote environments because these networks can be much less secure than an enterprise network. Which means, unfortunately, that breaches from a remote workforce can be more common.

Another priority is effective resources. Organisations are accelerating implementation of many new applications/tools/solutions/technologies to fulfill the requirements of a hybrid workforce. And in light of the damaging [Log4j vulnerability](#), identifying which applications are impacted by these zero-day exploits becomes even more difficult and time consuming to repair. These exploits are open for longer periods of time which means bad actors have more time to exploit—which leads to another layer of problems for security teams.

So the bottom-line priority is really to take a step back.

A proactive approach to threat hunting, instead of being reactive and waiting for an alert to be triggered. Visibility is the foundation. Analytics are only as good as the quality of the data that you analyze—and without good visibility—you can't do proper and holistic threat hunting. Hence the need to first build the foundation by gaining detailed visibility over logs, network endpoint, on-prem, and in the cloud. And then build on top of that.

Are there any issues you are seeing consistently with customers and prospects? Perhaps many of these companies have "blind spots" that they need to address?

Organisations tend to invest in the "best in breed" technology (AI/machine learning for example). But if it's not properly and fully integrated, if it's not adapting as quickly as the attacks of the bad actors, you still have a visibility gap. And as you move to the cloud, if you don't integrate quickly with your SOC, you will still have more visibility gaps from other perspectives. Threat actors can bypass some of your preventative measures, some of your visibility and protection.

If an organisation is re-evaluating their cybersecurity posture—from the SOC to the one-person team—what are some best practices for intelligent threat management and security ops?

I think regular assessments are key.

Assessments can come in many forms: they can be a SOC assessment when you review processes, tools, or gap analyses, or proactive incident response engagements by third-parties (because sometimes we get tunnel vision and need another pair of eyes looking at what we're doing and how we're doing it). Understand where you are today and how to build on that—and expand on that—to optimize your SOC operations.

Also, conducting regular incident discovery engagements or other IR services.

These can help identify potential threats that are currently in your environment that have been undetected by the SOC. Utilizing these services can help you enhance the SOC's performance. And even if there is no breach, these [IR services](#) can identify and mitigate gaps and weaknesses early, increasing your security posture and preventing a potential future breach.

How do you see the customer journey (roadmap) for building an end-to-end, extended detection and response (XDR) platform? What do organisations need to consider?

I would ask: what problem are you trying to solve? What challenges do your security teams have? What are you trying to achieve? You need to answer these questions first. And then look for the features that can actually solve the security problems in your specific environment. Because each environment is unique. Each customer has different requirements.

What security solution works best in one organisation may not work that well in another. And the requirements might be different; the maturity of the customer might be different.

Another example: a customer says, "I want a SOAR solution." But if you don't have proper SOC processes, if you don't have playbooks, if you don't have things to automate—you won't get the value from an orchestration tool. So it's important to build security tools from the ground up, and not be seduced by a trend in the market.

You have to build in a phased approach. You should not skip steps. Because then you're creating problems on top of the tool. It's not giving you the output you want, or you may not have the right teams or skills to operate the tools.

There are a lot of threat detection and response platforms available to enterprises. But why is the NetWitness Platform different in your opinion—what "weapons" does NetWitness deliver to help win the cybersecurity war?

The first differentiator is NetWitness technology.

[NetWitness](#) is one of the only solutions in the market that has it all—logs, packets, EDR, orchestration, automation—in a single platform, from the same vendor, fully integrated.

We've seen customers who buy the "best-in-breed" of each technology, and when they do that and it comes to practice, and they want full integration, it doesn't work as well as they hoped for. So having everything natively integrated and working together, being able to navigate all the data from a single pane of glass, offers tremendous value. And being able to expand the solution as your organisation matures in security operations and your requirements evolve. Adding automation. Adding orchestration. Adding machine learning.

Whether NetWitness does it for you on-prem, or in the cloud, having a modular solution that can expand with your requirements and provide all the needed capabilities under one roof is a huge plus.


The second differentiator is the NetWitness knowledge base.

We're not just building a technology based on market trends. There's a lot of influence from our own field response teams: we get recommendations and input from actual security practitioners, analysts, and security responders. So the people who use the NetWitness Platform are the ones who are providing essential, valuable feedback into the direction of the product and the solutions that are needed to make NetWitness better—and organisations safer.

The fact that we use our own product for our own threat detection and response can benefit customers as well. We get to test innovations in the field and get feedback from actual investigations and detections of advanced threats and attacks. We build NetWitness with all this intelligence; it's not just a "good to have" set of features of what's popular in the market.


Looking to this new year, what do you think are some of the threat and attack tactics that nation states or bad actors may pursue in 2022?

1. Ransomware




It's still going to be a big problem because it's extremely lucrative. Bad actors are investing more in zero-days and even giving a share of the ransomware profits to accomplices to encourage bypassing preventative measures completely. [RaaS](#) (Ransomware as a Service) is already a big thing. These attackers are shifting the way they've been operating; they understand companies are taking more proactive measures. So they are investing in more advanced tools, techniques, and time to infect more machines and commit more dwell time (often 2-3 weeks before starting an encryption!) within a customer's environment. This means that the traditional types of preventative measures that security teams used to do (for example, single point solutions) are not as effective anymore.

2. Exploits



In the case of vulnerabilities like [Log4Shell](#), there's zero intervention needed from an end user. The moment your application is published on the internet and vulnerable, it's game over. We can expect to see more of these types of exploits. Bad actors are becoming more flexible, more agile, and more adaptive to current trends.

3. Cloud



Governments and organisations here in the META market (unlike North America) aren't as driven or ready to migrate their critical infrastructures into the cloud. While some applications are still being used via the cloud, and cloud migration is part of customers' future roadmaps, many security ops in the META region prefer on prem. Even so, as cloud migration develops, security teams must remain vigilant. This new year will be an evolution of what we've been seeing in 2021. Be ready.

Can you share any client success (case study) stories?

There are many success stories in the META region, some of which the journey started as early as the proof-of-concept stage and turned into a full partnership.

In one of the cases, our relationship with a high-profile customer started during a proof-of-concept for NetWitness Network and Endpoint. During this time, malicious activity which was previously undetected for more than a year and linked to a state-sponsored threat actor active in the region was identified. To augment the capabilities of the customer's team, they called in NetWitness' Incident Response services who brought exhaustive experience and knowledge from engagements both global and regional in the META region. This allowed the organisation to significantly ramp up their SOC capabilities and prevent further breaching attempts by state-sponsored threat actors.

Another success story includes an organisation that kept getting infected and re-infected by ransomware. After deploying [NetWitness XDR](#), it was then possible to gain full visibility across network and endpoint data that allowed the client to conduct a comprehensive analysis. This resulted in 1) effectively responding and remediating the incident; 2) cleaning all impacted systems; 3) providing recommendations to close the weakness gaps (that were being exploited by threat actors to breach the environment); and 4) stopping further re-infections.



Halim Abouzeid

Advisory Threat Hunter Systems Engineer

Halim Abouzeid is an Advisory Threat Hunter Systems Engineer at NetWitness, covering Europe, the Middle East and Africa. He has 15 years of work experience in cyber security with a background in ethical hacking, penetration testing and threat hunting.

XDR versus evolved SIEM – What’s the Difference?

By Brian Robertson

XDR focuses on identifying, investigating, and taking action to resolve incidents as quickly and efficiently as possible. While evolved SIEM fundamentally does the same, it also serves as the system of record for compliance monitoring, retention, and reporting.

Extended Detection and Response (XDR) and evolved security information and event management (SIEM) solutions offer similar capabilities and benefits. For example, they both tend to incorporate advanced analytics, machine learning, and security orchestration and automation to improve threat visibility and dramatically accelerate threat detection and response. So how do you decide between the two?

To answer that question, let’s recap some of the fundamental differences between evolved SIEM and XDR:

XDR focuses on identifying, investigating, and taking action to resolve incidents as quickly and efficiently as possible. While evolved SIEM fundamentally does the same, it also serves as the system of record for compliance monitoring, retention, and reporting. To support threat detection and response and compliance requirements, evolved SIEM platforms leverage as much of an organization’s data as possible, including logs, network data, and endpoint data.

In contrast, because XDR isn’t intended to satisfy compliance mandates in the way that evolved SIEM is, XDR platforms generally do not need to collect logs to assist with threat detection and investigation; instead, network and endpoint data typically suffice. Even if an organization occasionally needs user logs to resolve security issues, XDR platforms require far fewer of them than evolved SIEM platforms. Because evolved SIEM platforms need to collect logs to support compliance, they incur throughput costs that XDR platforms don’t.

Bottom line: If your organization already has a log management and retention tool in place to support compliance, you may not need an evolved SIEM solution for threat detection and response. XDR may be a better (and more cost-effective) fit for your organization. But if you don’t have a log management and retention tool or a threat detection and response platform in place, then an evolved SIEM can serve both purposes. Either way, RSA NetWitness Platform has you covered.

DATA SOURCES	XDR	EVOLVED SIEM
<ul style="list-style-type: none"> • Network • Endpoint • Multi-source Threat Intelligence 		<ul style="list-style-type: none"> • Logs • Network • Endpoint • Multi-source Threat Intelligence
ANALYTICS <ul style="list-style-type: none"> • Advanced Analytics • Behavior Anomaly Detection • Guided Threat Hunting 		<ul style="list-style-type: none"> • Advanced Analytics • Behavior Anomaly Detection • Guided Threat Hunting
AUTOMATION <ul style="list-style-type: none"> • Orchestration and Automation 		<ul style="list-style-type: none"> • Orchestration and Automation

Source: <https://www.netwitness.com/en-us/blog/xdr-versus-evolved-siem-whats-the-difference/>