White Paper

Beyond EDR: Natively Correlating and Analyzing Telemetry from Endpoint, Network, Email, and Cloud

Increasing the Efficiency and Effectiveness of Detection and Response through XDR

By Dave Gruber, ESG Senior Analyst

August 2019

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Threat Detection and Response Has Become Increasingly Challenging

With a growing threat landscape, widening attack surface, and the increasing sophistication of attacks, threat detection and response has become increasingly challenging for security teams. While multiple security solutions are deployed in most organizations, serious threats continue to avoid detection because data is collected and analyzed in silos.

Organizations have attempted to solve this issue using SIEM systems as an aggregation tool. ESG research tells us that 88% of organizations are either already running a SIEM or have plans to.[1] However, traditional SIEMs have become expensive to own and operate, often requiring significant upfront costs. Recent announcements by Google/Chronicle Backstory and Microsoft Sentinel offering cloud-native SIEM tools with unlimited data and analytics processing have reinforced the need to consolidate and analyze massive amounts of telemetry from the many security solutions, including endpoint security, network security, email security, and cloud security. While these cloud-delivered SIEM replacements eliminate the expensive SIEM storage issues, they still lack the context needed to accelerate detection and response times. SIEM systems lack ML-based correlation and analysis capabilities, leaving this effort to the already overworked SOC analysts.

To fill this gap, organizations have turned to endpoint detection and response (EDR) systems. These powerful tools aggregate and analyze endpoint activity, while comparing threat intelligence to detect attacks underway.

While security analysts use EDR tools daily to investigate threats and hunt for not-yet-identified threats already underway, EDR tools alone aren't enough for most security teams. Many companies are already leveraging APIs to export data out of EDR systems so they can combine it with other security data to gain additional insights into root cause and impact. When telemetry is correlated across the security stack, more accurate and timely detection can be automated, stopping attacks in progress and helping analysts more deeply understand adversary behaviors. Endpoint, network, cloud, and email telemetry together can paint a clear picture of attack strategies from the most sophisticated adversaries.

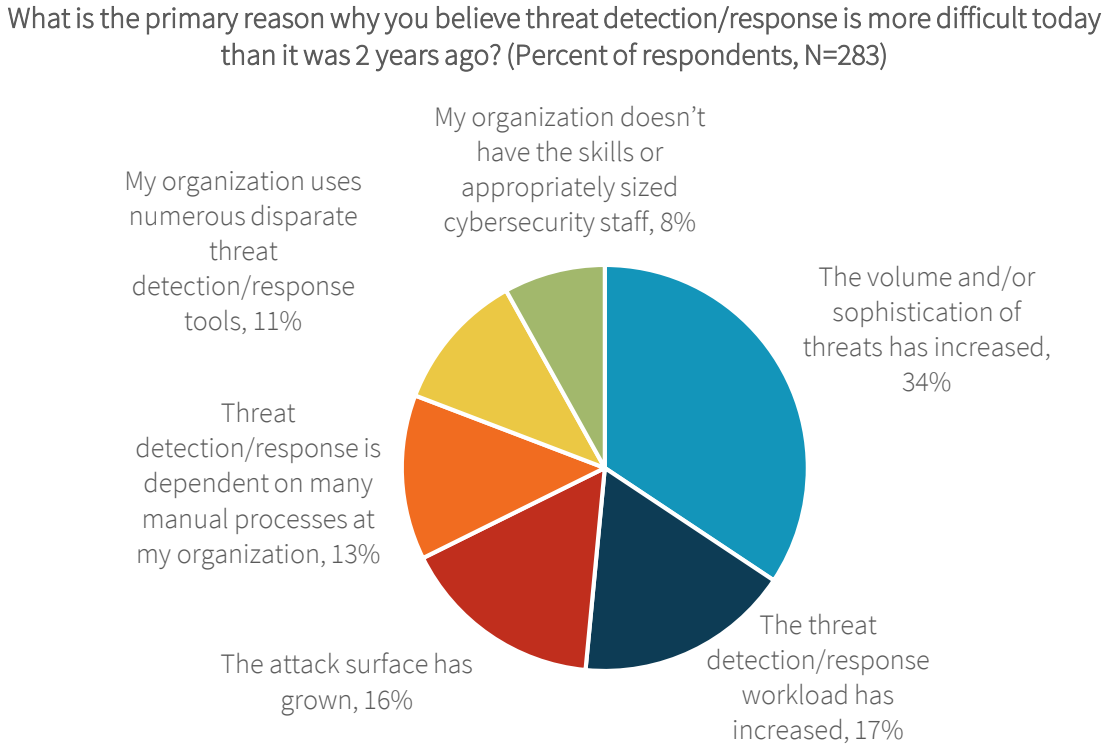
EDR alone is simply not enough to empower security pros to detect, investigate, and respond to attacks at the pace they need to keep up with modern attackers. A broader detection and response approach is needed.

The Current State of Threat Detection and Response

In late 2018, ESG conducted research to better understand the current state of threat detection and response (TDR). Forty-five percent of respondents said that threat detection and response is much more difficult today than it was two years ago, and 31% said it is somewhat more difficult. Respondents point to the increasing volume and/or sophistication of threats (cited by 34%) and growing attack surfaces (16%) as causes for this increasing difficulty (see Figure 1). Further, 82% of respondents agreed that improving threat detection and response is a high priority for their organization.

[1] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019. All ESG research references and charts in this white paper have been taken from this master survey results set.

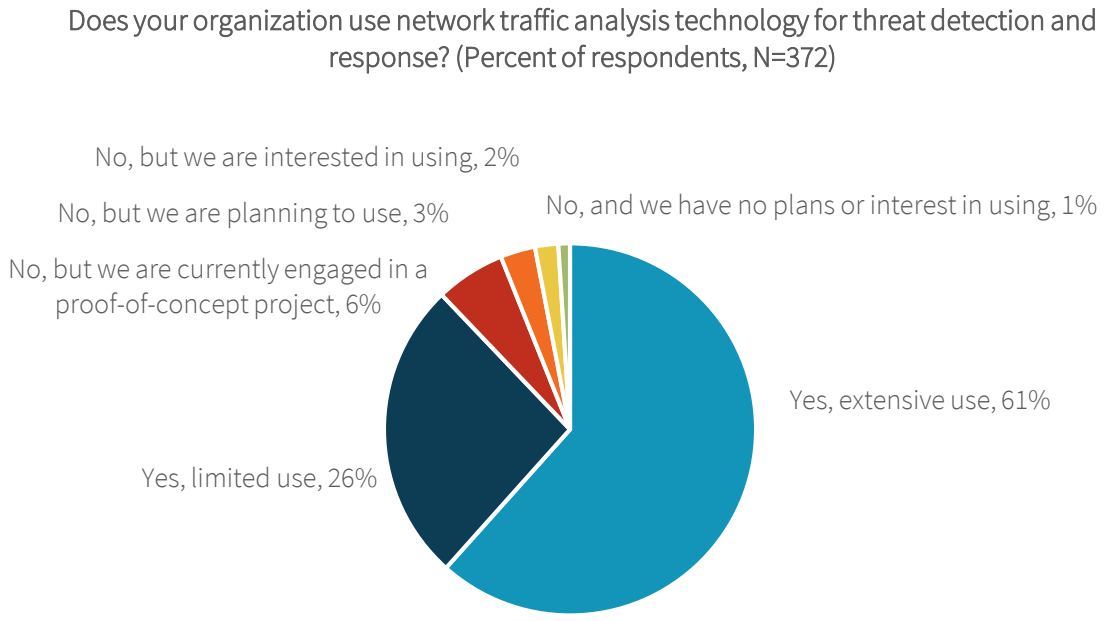
Figure 1. Primary Reason TDR Is Harder



Source: Enterprise Strategy Group

As attackers move laterally within the network in an effort to escalate privileges, the need to understand attackers' entry points, patterns of movement, discovery, and individual behaviors reinforces the requirement to aggregate telemetry from multiple threat vectors. Network traffic analysis (NTA) tools have become important in helping analysts look for lateral movement, but without correlation with endpoint activity, it can be difficult to understand the full details of an attack.

Figure 2. The Majority of Organizations Say They Depend on Network Traffic Analysis Tools for TDR



Source: Enterprise Strategy Group

Many organizations are post-processing EDR and NTA data in an attempt to stitch together attack details. Yet even with EDR solutions in place, security teams continue to struggle to keep up. While most teams are depending on multiple, independent tools, ESG research shows that 66% of respondents believe that their TDR effectiveness is limited because it is based on multiple independent point tools.

This means that despite the tools in place, teams still aren't leveraging them to their full capacity.

Challenges: Data Aggregation and Analysis Are Expensive and Time Consuming

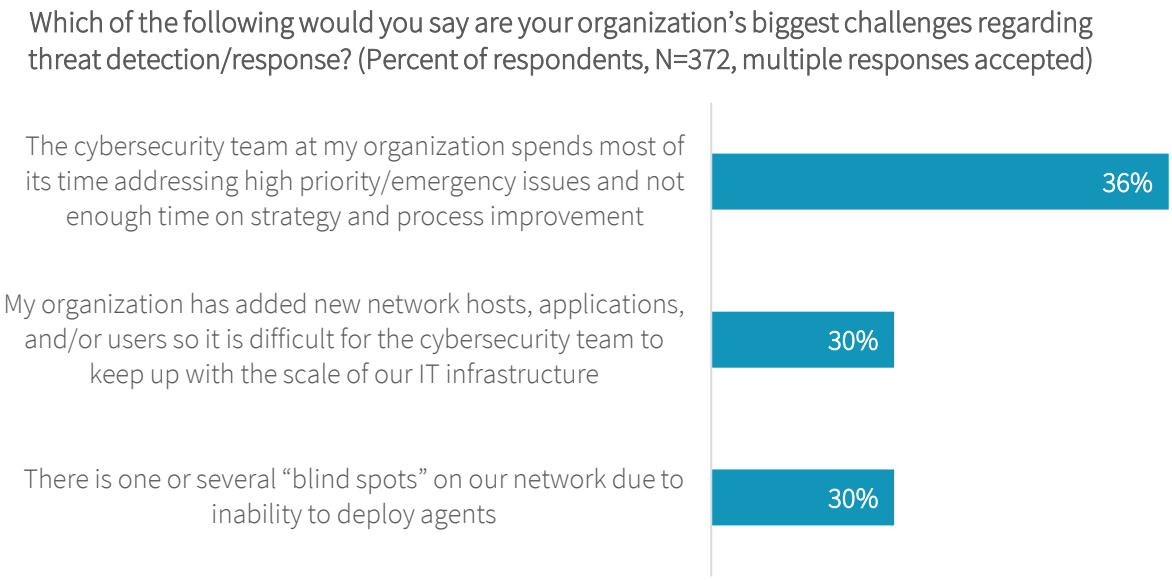
Aggregating telemetry from the many tools in the security stack is not only challenging, but also impossible in many cases. Individual tools store and index data differently, forcing local teams to go-it-alone in their effort to integrate. Building and maintaining security data lakes is also expensive and time consuming. Most organizations aren't equipped to employ AI/ML techniques on these custom-built security data repositories, lacking skills and the budget required to build them.

Even when data is aggregated, it is seldom integrated with the daily workflow of the security analyst. As insights are derived, most solutions lack the ability to apply these learnings to future detection. Insights are often captured in other siloed systems, requiring analysts to again manually correlate the data. These tools also often lack sophisticated attack visualization, forcing analysts to query and parse data manually.

Challenges: Security Teams Can't Keep Up

When security analysts were asked what their biggest TDR challenges are, ESG survey data showed that analysts are so busy triaging current issues, that they aren't spending any time getting more proactive with strategy, processes, and improved infrastructure (see Figure 3). This research further shows that organizations are struggling with the rapid addition of new hosts, applications, and users, together with the inability to deploy agents on a percentage of their devices.

Figure 3. Top Three TDR Challenges Include Firefighting, Growing Attack Surface, and Lack of Real-time Visibility



Source: Enterprise Strategy Group

With limited ability to impact the skills shortage, focusing on the volume of alerts and the time it takes to investigate and remediate needs to become the key focus to overcome the current situation.

Challenges: EDR Solutions Lack the Full Range of Telemetry

EDR solutions have opened the eyes of many, but at the same time lack the broader visibility that is needed to operate at the speed required. While EDR solutions can sometimes detect lateral movement, the absence of network, cloud, and email telemetry makes it difficult to rapidly detect and paint a clear picture of true attacker behavior.

EDR solutions have set the stage by delivering powerful threat detection and response capabilities, including the abilities to continuously compare activity with threat intelligence, visualize an attack, respond by killing or banning processes, restrict access to specific domains and IP addresses, and request additional forensics data. But while the functions available in modern EDR solutions are valuable, they often require correlation with other security data to construct a complete view of the attack.

For organizations that have already deployed endpoint detection and response solutions, endpoint-only telemetry lacks completeness and therefore potentially hides attacker behaviors.

What's Needed

> The ability to rapidly and continuously analyze events, behaviors, and alerts from all aspects of the security stack is paramount to optimizing TDR.

Threat detection and response is a core process for every security analyst. The ability to rapidly and continuously analyze events, behaviors, and alerts from all aspects of the security stack is paramount to optimizing TDR. When analysts can validate incidents across multiple security vectors and are equipped with the complete picture of endpoint, network, email, and cloud, they can shut down threats faster, respond faster, and ultimately head off attackers before they do damage.

More telemetry is needed from network, email, and cloud devices. Further, AI/ML-driven analytics need to be applied across this broad data set to detect and prioritize the most important threats. Combining network traffic analysis with endpoint telemetry signals early signs of attackers attempting to move laterally throughout the infrastructure. This integrated data set also helps analysts determine root cause faster.

With the prolific use of phishing to steal credentials, and 94% of all malware coming from email,[2] correlating email-borne threats to attempted malware execution on individual endpoints and lateral movement through network traffic data provides the context required to understand attack strategies.

Once broad telemetry is aggregated, correlated, and analyzed, this continuous analysis process needs to be tightly integrated into the workflow of every security analyst.

Introducing Trend Micro XDR

Trend Micro XDR, offered as a solution platform or delivered as a managed service, aggregates and analyzes telemetry from endpoint, network, email, and cloud, using machine learning and security analytics to correlate events. This new level of automation not only saves security analysts hours of upfront time triaging and researching issues, but also automates detection and response, improving mean time to detect and mean time to response. Detailed telemetry from each vector provides insights and intelligence into ongoing attacks, enabling the XDR analytics engine to detect attacks faster and with more clarity, leading to faster response.

[2] Source: 2019 Verizon Data Breach Report.

Table 1. Rich Telemetry Drives More, Deeper Insights and Faster Outcomes

Endpoint	Network	Email	Cloud
Processes	Lateral connections	Processes invoked through attachments	Configuration changes
Network connections	Traffic flow	External links	New/changed instances
Files accessed		User activity	Serverless telemetry
Registry modifications			Privileged access

Source: Enterprise Strategy Group

Stored in the Trend Micro data lake located in both the US and Europe for data residency compliance, telemetry from individual organizations is carefully protected from any cross-contamination with data collected from other organizations.

Through the use of machine learning, expert security analytics (enriched via global threat intelligence from the Trend Micro Smart Protection Network (SPN)), and detection rules (maintained by Trend Micro security experts), XDR aims to reduce noise levels by correlating and prioritizing alerts. Analysts can instead shift focus to more critical issues with less distraction from false positives.

When ML-based data analytics leverage native sensors, they can typically achieve a deeper understanding of activity and detection data. This approach is expected to be more effective than what can be achieved via APIs to other third-party products.

While other vendors attempt to supplement their EDR solutions using integrations with third-party network and email providers, they often fall short without a fully integrated, ML-driven approach to analyzing telemetry from endpoint, network, email, and cloud.

For example, the type of data being pulled is different. Often, only alert data is used, and not full activity data (such as telemetry, metadata, and netflow). This means there is less to feed into the analytical models for correlation and prioritization. In addition, definitions of detections and severity indicators can vary, as each vendor defines its data differently. Misalignment of indicators can make it difficult to reconcile/understand the data and assess overall risk.

As an example, early warning signs from network traffic analysis can be paired with endpoint and cloud activity to zero in on specific attacker behaviors, helping analysts not only stop attacks in progress, but also stop future attacks.

Trend Micro XDR offers guided investigation and coordinated response capabilities across multiple security layers, enabling analysts to take action and remediate attacks across the many devices affected within the infrastructure.

With the underlying solutions being native to Trend, organizations can automatically enable real-time security updates to all protection points.

Available APIs enable Trend Micro XDR solutions to be integrated with SIEM and SOAR solutions.

For organizations that lack enough detection and response resources or want to add 24x7 coverage to their team, Trend Micro offers managed detection and response services for endpoint, network, email, and cloud workloads. As customers use more than one service, they see the benefits of cross-layer analytics, incident prioritization, and response.

XDR and the SIEM

Modern security information and event managers play a key role in most security architectures, providing an aggregation point for logs, events, and alerts. XDR solutions won't replace the SIEM, but instead will provide a new level of automation and analytics that will augment the SIEM, reducing the amount of effort required by security analysts. The SIEM will continue to act as a historical collection point when organizations want to look back in time for digital forensics or compliance. While many organizations depend on their SIEM as an aggregation mechanism today, the SIEM lacks sophisticated ML-based analytics and context of related events and alerts. XDR solutions aim to get in front of the SIEM, correlating events in a way that leads to faster detection and response. As XDR solutions evolve, it is possible that they will replace many of the use cases satisfied today by the SIEM.

The Bigger Truth

With 76% of companies claiming that threat detection and response is more difficult today than it was two years ago, current detection and response tools aren't keeping up. While endpoint detection and response solutions have helped many organizations identify and respond to attacks they believe would have otherwise been missed, many organizations say that they are still falling further behind, lacking the ability to keep up with the volume of modern attacks. A new approach is needed.

The vast majority of organizations expect to increase spending on TDR over the next 18 months (46% significantly, 42% somewhat), highlighting the critical state of the problem. With new TDR solutions and managed services emerging through the introduction of XDR, users should expect to achieve new levels of visibility and automation, reducing mean time to detection and response. This will free up security analysts to spend more time on the most sophisticated attacks, in addition to maturing strategies and processes.

XDR solutions from vendors like Trend Micro provide new promise in helping security teams keep up the ever-changing threat landscape.