Three ways to evolve your **Security Operations**

February, 2023

Introduction

Both the threat and business landscapes are always changing, but the drastic shifts of recent years have made unprecedented demands of security teams, and the security operations center (SOC) in particular. Making piecemeal or incremental changes to keep up with the latest trends is no longer sufficient. Enabling organizations to meet the needs of their digital transformation—and to face threats yet to come—requires a more comprehensive approach that can grow with them into the future.

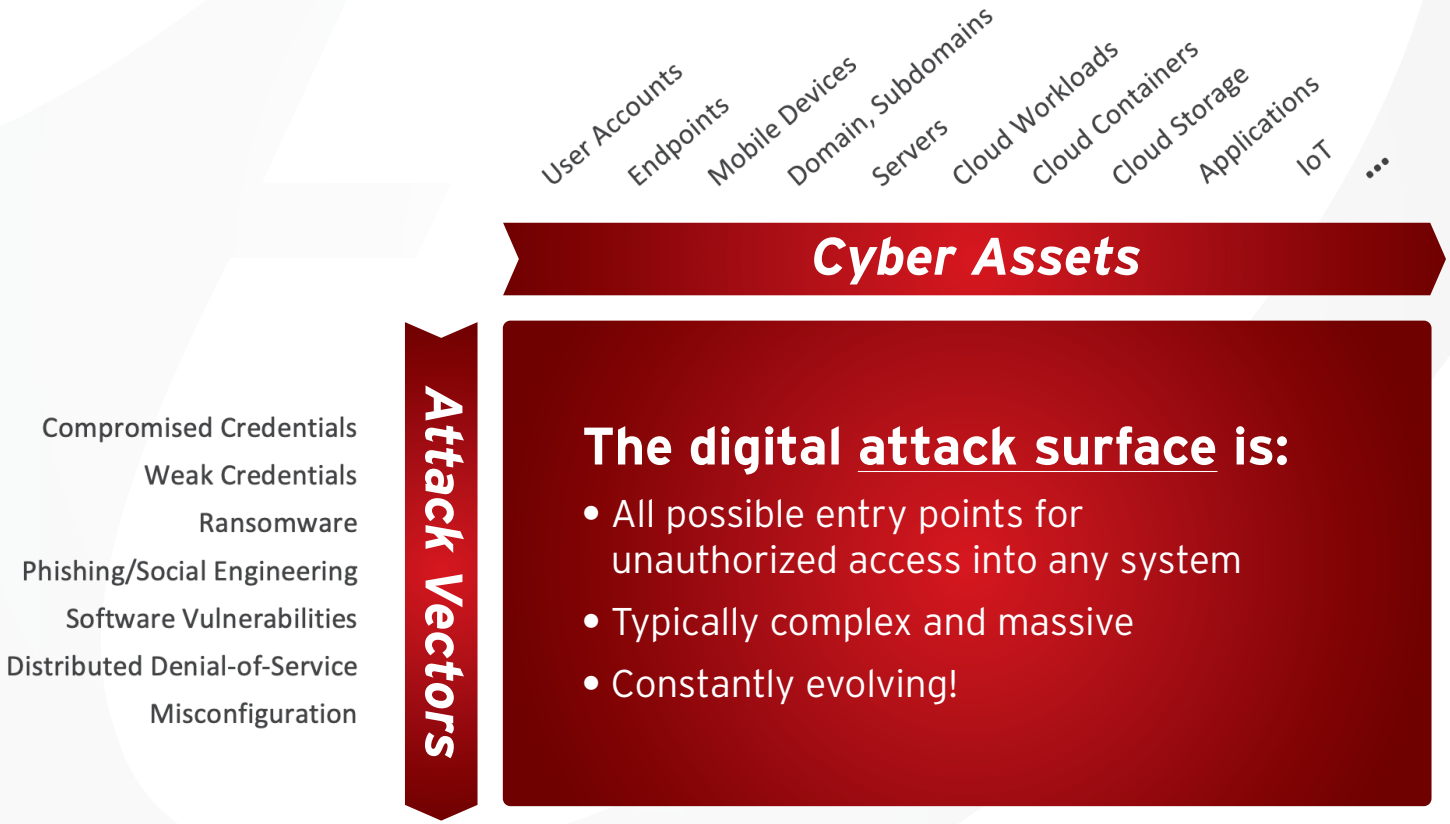
Even organizations without a formal SOC, or ones that outsource the responsibilities of the SOC to a service provider, are ultimately faced with many of the same challenges, market dynamics, and operational realities. Whether they manage without a SOC, are evolving that team's role, or taking the measure of their partner's approach to managing cybersecurity, all organizations can benefit from considering these three key areas of a modern security operations strategy:

1. **Adopting and optimizing extended detection and response (XDR)**
2. **Leveraging more proactive cyber risk management**
3. **Converging security solutions to a holistic cybersecurity platform with supporting services**

Behind the Drive - Market Dynamics and Operational Realities

Each day, the SOC team is faced with the enormous responsibility of quickly identifying and responding to critical security events to minimize the business risk and impact to their company. That is no small goal, and it requires constant effort and dedication to ensure operations are equipped and teams have the resources they need to adequately defend the enterprise. Despite the innovation and progress in SOC processes and their supporting tools, more often than not, SOC leaders will say it still takes too long to detect threats, investigations are cumbersome, response time are not quick enough, and their teams are overloaded.

The reason for this is, of course, that their battleground never stops growing and changing. Consider what has occurred in the last two years alone. Since the global rise of different work from anywhere models, organizations have been forced to accelerate their digital transformation and adopt more cloud services. Today, remote and hybrid work is the norm, cloud app usage is growing exponentially, more types of users and devices are connecting to critical systems, network boundaries are disappearing, and identity is being recognized as the new perimeter. Unsurprisingly, 46% of respondents in an ESG survey believe security operations are more difficult than they were two years ago, with the top reason cited being the growing attack surface.[1]



1 - ESG Research Insights Report: The XDR Payoff: Better Security Posture, September 2020

This very complex and diverse digital environment presents new opportunities for attack. An increased number of cyber assets means more of those assets are likely to be vulnerable, more areas of weakness arise in the infrastructure, and, overall, results in an even bigger and more profitable target that cybercriminals are only too eager to exploit.

For the security operations leader, improving the outcomes of the SOC has become more difficult to achieve yet simultaneously more important, particularly as we increasingly see security as a C-level and board discussion topic.

Alert overload	*The volume of alerts is overwhelming, making it difficult to quickly and effectively weed through the noise to find critical events.*
Missed or slow detections - MTTD	*Serious threats are evading detection because data is collected and analyzed in silos.*
Investigations take too long and are often misdirected - MTTR	*Lack of context and correlation in the incoming alerts make it difficult for the analyst to visualize the chain of events and prioritize action prolonging risk exposure.*
Too many tools, but still too many gaps	*Point solutions are focused on a particular function. Integration between solutions can provide a level of consolidated visibility, but the value is often limited by a lack of depth of telemetry and analytical capabilities. This means there continues to be gaps in what an analyst can see and do.*
Attack surface keeps growing and risks keep rising	*The growing attack surface means more assets that can be vulnerable, more areas of weakness in the infrastructure, and, overall, an even bigger and more profitable target for attack that SOC teams need to monitor and defend.*
Can't get in front of threat activity	*Overstretched teams are in constant firefighting mode, leading to burnout and further exacerbating the skills gaps.*

Why Current Approaches are Not Working

While we understand that market dynamics have intensified, the question remains why doing the same thing, but better, is no longer an option for the SOC function.

> *"One of the most difficult challenges for enterprise SOC teams historically has been the many manual tasks involved with threat detection and response processes. From observing activity, gathering telemetry, investigating an incident and ultimately remediating, resolving, and closing out a ticket, the start-to-finish process for resolving a single threat event often requires several hours of work by an SOC analyst, switching back and forth among a variety of different tools. As enterprises are aware, this is an inefficient, expensive, tedious, and often ineffective approach for finding and responding to threats."*[2]

Many organizations are leveraging a combination of security solutions, often underpinned by their heavy use of EDR and SIEM. Let's examine where these current approaches may be falling short.

Discrete detection solutions, like EDR, can't see everything

Endpoint detection and response (EDR) has proven enormously valuable. However, despite the depth of its capability, EDR is restricted because it focuses only on managed endpoints. As managed endpoints represent only a portion of the attack surface, this limits the scope of threats that can be detected, as well as visibility regarding who and what else is affected. These restrictions ultimately limit response effectiveness within the SOC.

The same is true for any single vector, point solution detection capability. In these cases, each solution offers a specific perspective, collecting and providing data as relevant and useful for that function. Detection employed on individual security layers can provide alerts of suspicious activity for that vector but cannot account for how it may relate to other suspicious activity happening elsewhere in the network. This missing context is often what allows threats to avoid quick detection.

Consider network traffic analysis (NTA) or network detection and response (NDR) tools, which provide a deep view into the monitored network segments. These solutions offer incredibly valuable information but tend to drive a massive number of logs. Understanding network alerts in the context of other activity data is critical for the SOC to make sense of, and to fully capitalize on, the abundance of rich network alerts received.

2 - Fundamentals of XDR versus SIEM and SOAR: Understanding the Evolution of SecOps Architectures, 26 March 2021

SIEM can centralize logs/alerts for consolidated visibility, but often offers little correlation

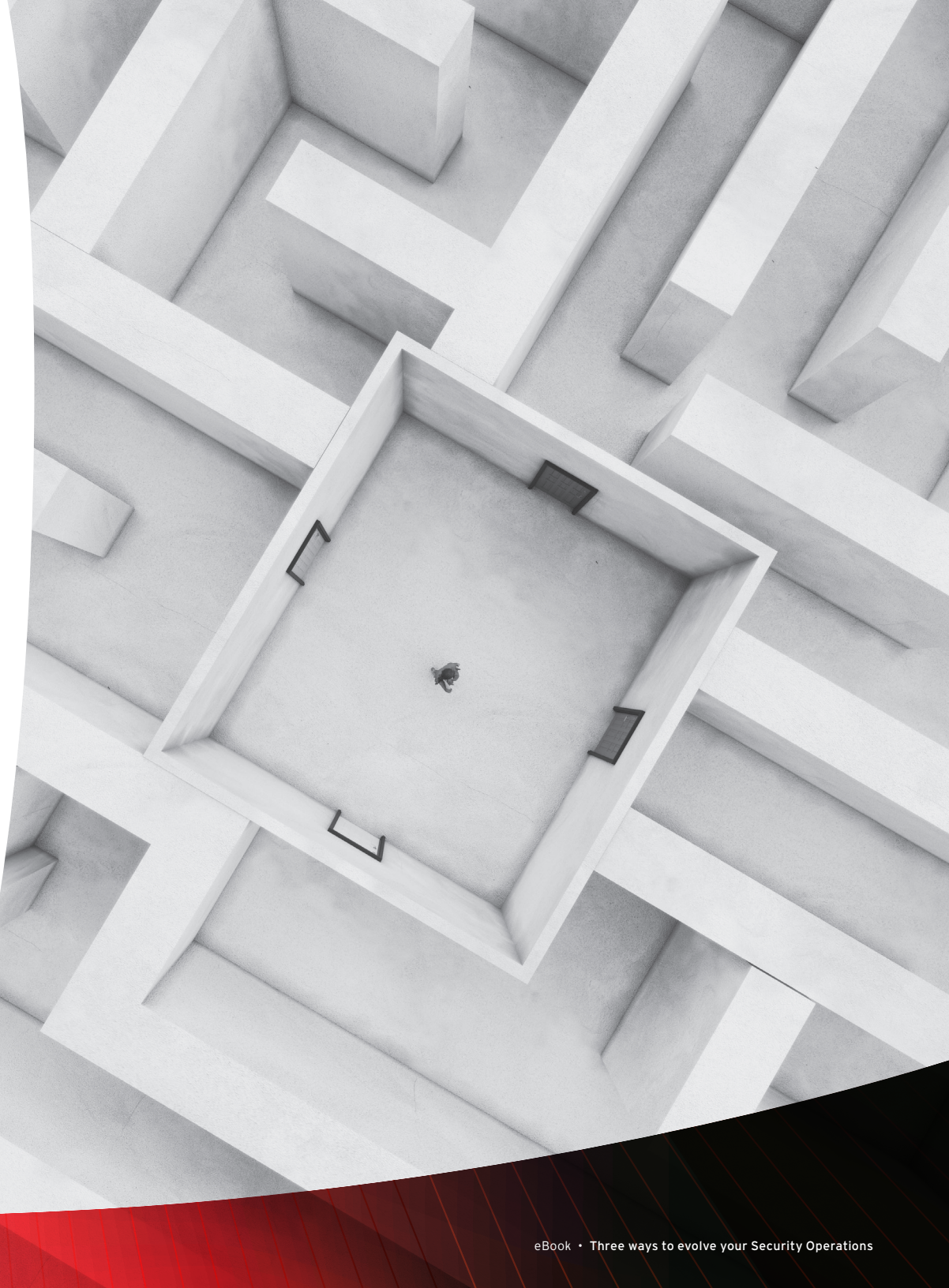
While security information and event management (SIEM) is widely considered a go-to tool for threat detection and response, almost 58% of respondents in an ESG survey[3] said there was room for improvement with upfront correlation activities.

SIEM is effective at aggregating logs and alerts, but it has not proven to be as adept at connecting multiple alerts related to the same incident. This leaves organizations with plenty of data but also visibility gaps. Piecemeal alert data collected across disparate point products, even if centralized in a SIEM, still leads to alert overload compounded by an unproductive number of false positives. According to Trend Micro Research, 27% of security analysts' time is wasted on investigating low-fidelity alerts that turn out to be false positives.[4]

Correlating data to produce high-confidence detections is the urgent need, and this requires analysis at the root telemetry level across security layers.

> As Gartner noted, ***"Attack signals and indicators of compromise (IOCs)are often buried in the noise. Getting a deterministic alert from your favorite point security product is becoming increasingly rare. More commonly, security controls are producing general indicators, elements or telemetry related to an attack. They do this from their unique point of view of the attack, which is often lacking context (as seen from other points of view). A modern SOC can consume all these indicators and make an assertion based upon analysis using data science methods"***[5]

Security operations teams need to establish new goals around bolstering their threat detection and response maturity, in addition to evolving broader security competencies, infrastructure, and services that can support the transformation.



3 - ESG Research Insights Report: The XDR Payoff: Better Security Posture, September 2020

4 - Security Operations on the backfoot: How poor tooling is taking its toll on security analysts, 2021

5 - Gartner: 2022 Planning Guide for Security and Risk Management, 11 October 2021

1. Adopting and Optimizing XDR Capabilities

As previously mentioned, while detection employed on individual security layers can alert to suspicious activity for that vector, the ability to automatically correlate events and related activities has been lacking. That is the power of XDR.

Multiple data sources feed XDR analytics and detection models to identify events that EDR or point products can't see alone. This expanded approach to detection and response is gaining rapid market acknowledgement as SOC leaders look to determine the approach and supporting technology that will work best within their organizations. As they do so, there are multiple factors to consider.

Taking the right XDR Approach

Understanding where SIEM fits:

Larger enterprises with existing investments in SIEM are looking to XDR to complement or augment their use of SIEM. In this scenario, XDR is implemented as part of the broader ecosystem and improves workflows. SIEM acts as a log aggregator but is fed correlated detections from the XDR platform, which can improve critical incident identification to reduce triage time and efforts. Conversely, data from the SIEM can be fed into the XDR platform to provide enrichment for XDR detection and investigation. The XDR platform primarily serves the threat detection and investigation use cases, while SIEM provides visibility and reporting of log data for compliance and regulatory use cases, or for broader security data analysis.

The benefits of SIEM and XDR integration are made more valuable by the ease with which even small organizations can combine them. API integrations can ensure both XDR and SIEM provide their maximum value for the SOC's investment in each.

The value of XDR platforms is felt immediately in organizations that lack the right mix of financial, staffing, or technical resources to deploy SIEM/SOAR but still require enterprise-grade threat hunting, detection, and response capabilities. And organizations prioritizing an XDR capability are considering XDR platforms in place of implementing or maintaining a SIEM with custom integrations and analytics, given that the operational efficiency, security effectiveness, and data storage/processing costs can offer advantages over a SIEM-led architecture.

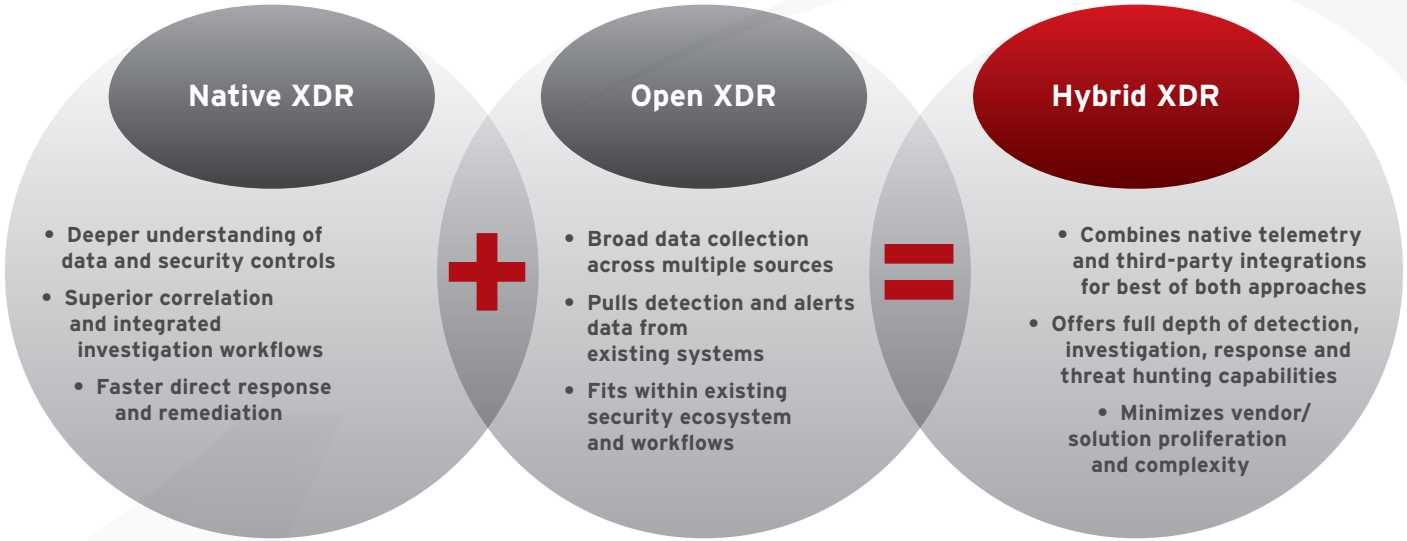
Native, open or hybrid XDR:

There is no one way to achieve an XDR capability, and not all XDR solutions or approaches are created equal. Solution providers tend to be categorized into three types:

1) Native XDR (also called Comprehensive XDR) leverages a vendor's own native security stack as the foundation for many of its data sources and uses its platform for organizations to manage the full XDR process – across detection, investigation, response and threat hunting.

2) Open XDR delivers certain XDR capabilities via a collection of third-party integrations.

3) Hybrid XDR is a combination of native and open approaches that attempts to offer the best of both worlds, capitalizing on the advantages and minimizing the constraints of each



Native XDR offers significant advantages in data analysis:

Using a single vendor for XDR data sources offers the advantage of providing a deeper understanding of the data. This enables the platform to collect precisely what is needed to optimize analytical models for correlated detection, in-depth investigation, and threat hunting.

An analytics engine fed by native sensors offers more effective security analytics than can otherwise be achieved on top of third-party products and telemetry, because an XDR platform provider will know the best analytical technique or combination of techniques to make a detection—whether that is AI/machine learning, data stacking, or other big data analysis.

Because data shares a common format regardless of its point of origin (domain), the XDR system's analysis engines can quickly and accurately find common data points that are indicative of a threat event. XDR analytics examines activity data and looks for different behavioral patterns across security layers to identify complex, multi-step attacks, as well as to provide early warning of a potential incident based on predictive analytics.

Open XDR offers broader data collection, but thinner detection and response capabilities:

While open XDR has the advantage of broader data collection across sources, in many cases it is only collecting and assessing alert data. This isn't the type and depth of telemetry needed to understand the full context of a given threat and, importantly, feed deep analytical models.

This challenges the very goal of XDR in terms of being able to correlate activity data across sources for quicker, more confident detections. In many cases, open XDR equates to being able to share basic threat data and query across collected data (such as file hashes, URLs, and IOCs).

> *"Detecting threats, as opposed to just writing rules, is a function of data analytics. For any analytics to perform, you need data—lots of data, not just alert data. You need to change the way you aggregate data depending on whether you use it for detection or investigation. Without this sort of modernization, analytics won't help increase SOC performance."*

– Gartner 2022 Planning Guide for Security and Risk Management[6]

Hybrid takes native XDR and supplements with additional integrations for the best return:

It comes as no surprise that the recommended goal is to take a hybrid approach—leveraging native telemetry where possible—from endpoint, network, and cloud sources at minimum, and using third-party integrations to supplement and enrich wherever needed. The imperative here is to gain not only comprehensive XDR data sources but also to integrate detection and response functions across those layers to gain the advantages that come with native XDR.

Some vendors may claim to offer hybrid XDR, but their XDR offering is often only focused on the endpoint. Legacy EDR vendors are building upon EDR by ingesting more data, but many of the deep analytical capabilities and the investigation and response components remain limited to a single layer—the endpoint. Enriching existing endpoint telemetry with third-party data sources is just one component of XDR, but the ability to serve the customer's need is dependent on being able to offer the full depth of detection, investigation, response and threat hunting capabilities for other layers.

Importantly, this approach minimizes vendor/solution proliferation, while still recognizing and capitalizing on the other systems being used within the organization.

6 - Gartner: 2022 Planning Guide for Security and Risk Management, 11 October 2021

Correlating data across more security layers for greater detection effectiveness

A growing adage of XDR is "the more integrated data sources, the better." In principle, yes, but in practice this can be a trap. Integration for the sake of integration is not a strategy. Integrating data sources should be considered in the context of where and how it will be used and what added value it can offer. More logs may technically mean more visibility, but it doesn't, by default, mean more insight or better detection. What differentiates an XDR platform is what is done with the data collected.

As a general rule, the more security vectors brought into a single, integrated XDR solution, the greater the correlation opportunities, which will result in more comprehensive detection. One caveat is that you must be careful to prioritize the security layers that can drive the most impact.

Endpoints

- Most attacks involve user devices
- Detect and determine what happened on the endpoint
- Understand how it propagated

Email

- #1 attack vector/entry point
- Identify all impacted parties
- Get details on the scope of compromised accounts

Network

- Sees EDR blind spots (unmanaged devices, legacy systems, IIoT/IoT)
- See lateral movement across the organization
- Identify command and control communications

Cloud Workloads /Containers

- Detect and determine what happened within the workload
- Gain automatic visibility of new cloud infrastructure and specific applications/ workloads added

Identity

- Identity is the new security perimeter: credentials are a priority target for attackers
- Identify exploitation, misuse, or stolen enterprise credentials

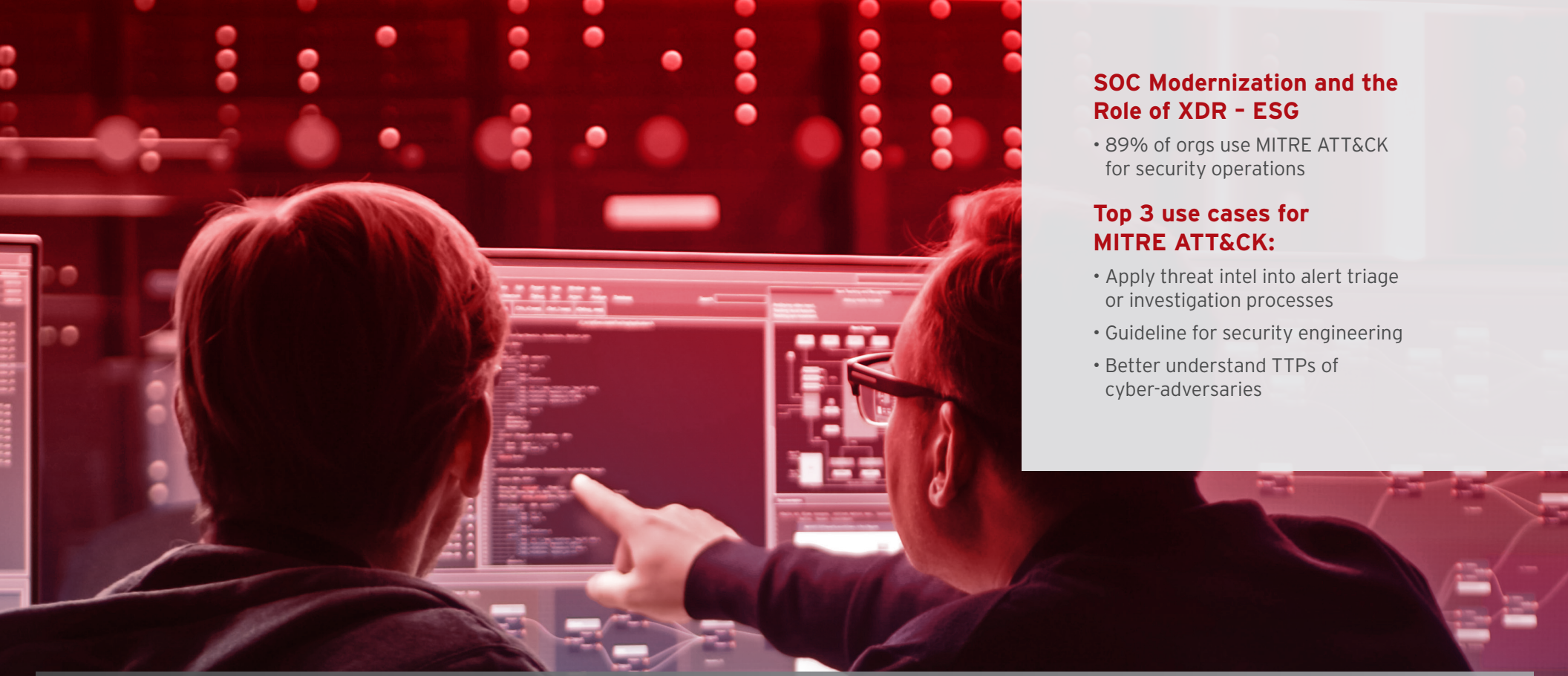
Data Detection and Response

- Gain a better understanding of all data assets
- Keep track of all asset history (renaming files, zip transfers, file encryption)
- Incorporate data context to understand the full scope and impact of a cyber event

Prioritizing critical events to reduce alert overload and ease the triage process

Effectiveness for the SOC team means always knowing where to focus, and what actions to take. A part of any XDR competencies is the ability to easily zero in on what needs attention first. Security analysts are overwhelmed by alerts and detections, so the ability to identify critical incidents as prioritized by the severity of the detection and scope of impact is the fastest route to better outcomes.

This information needs to be automatically served up to the analyst, presented visually and with the ability to dive deeper to investigate and respond across each part of an attack. Only when you have the necessary depth and breadth of data collection and product integration will you also have the full context to make important determinations of incident prioritization, along with the insight and controls to take subsequent action.



SOC Modernization and the Role of XDR – ESG

- 89% of orgs use MITRE ATT&CK for security operations

Top 3 use cases for MITRE ATT&CK:

- Apply threat intel into alert triage or investigation processes
- Guideline for security engineering
- Better understand TTPs of cyber-adversaries

Simplify incident investigation and response for faster analysis and action

XDR should enable more insightful investigations by showing the connections of events and activities within a single view. Having a graphical, attack-centric timeline view can provide answers in one place, including:

- How the user or hosts were compromised - What was the first point of entry - What or who else is part of the same attack
- Where the threat originated - How the threat spread
- How many other users are potentially vulnerable to the same threat

XDR augments security analysts' capabilities and streamlines workflows. It optimizes a team's efforts by speeding up or removing manual steps and enables views and analyses that are difficult or impossible to achieve otherwise.

Automated playbooks and integration with SIEM and SOAR solutions further empower the analysts to orchestrate XDR insight with automated tasks across the broader security ecosystem, whether that is supporting a triage workflow, collecting additional threat intel during an investigation, automating a response action, or more.

7 - SOC Modernization and the Role of XDR | ESG eBook - Cisco

Operationalize threat intel for greater insight and resiliency

As attackers become increasingly sophisticated and successful, the requirement to incorporate threat intel as an integral part of the daily security operations function has never been more acute. The more you can understand the attacker, their maneuvers and objectives, the more resilient and responsive an organization can be.

According to ESG's research SOC Modernization and the Role of XDR, the top SOC improvement initiative for 2022 was to "Improve operationalization of threat intelligence."[7]

The MITRE ATT&CK framework has been particularly valuable in being able to map to specific attack campaigns, threat groups, and individual attack activities. While much attention has been given to this framework, many organizations are still figuring out how best to leverage it in daily operations. Moving beyond using it as a third-party reference source, the next step in the journey is making it an integral part of the SOC function.

From a detection and response solution perspective, this is about using TTPs to develop detection rules and models, while also ensuring that threat intel is directly inserted into investigation of events to identify a particular attack campaign and give visibility into the full campaign lifecycle.

From a threat hunting perspective, this involves the ability to use TTPs to develop threat hunting criteria or provide proactive views of identified TTPs in the environment that can be leveraged as a starting point for targeted hunting and investigation.

Lastly, from a proactive perspective, the MITRE ATT&CK framework can be used to assess cyber risk in the environment and an organization's current security posture, with the goal to identify security gaps and prioritize activities to lower risk and improve resiliency.

Learn more about XDR:

How XDR Security Aids in Cyber Risk Management

ESG Economic Value Validation of XDR

How XDR Can Enable Your Enterprise

XDR by the numbers*

- 79% reduction in security spend
- 99% reduction in distilling activity logs down to correlated actionable alerts
- 70% faster identification and response to security events
- Replaces eight full-time employees

* According to the ESG Economic Validation: Analyzing the Economic Benefit of Trend Micro Vision One

The XDR checklist:

- Are the integrated security layers and data sources leading to faster and more accurate detections?
- Can I easily prioritize the most critical incidents, so I know what to act on first?
- Can I clearly understand the bigger picture of what has happened and immediately dive deeper to investigate and respond across each part of an attack?
- Can I hunt for threats easily and without sophisticated search queries?
- Am I getting threat intel that provides the context I need where and when I need it?

As attackers become increasingly sophisticated and successful, the requirement to incorporate threat intel as an integral part of the daily security operations function has never been more acute. The more you can understand the attacker, their maneuvers and objectives, the more resilient and responsive an organization can be.

2. Leveraging More Proactive Cyber Risk Management

While threat detection and response is the strategic imperative of the SOC, it does, by default, place the function squarely in a reactive state.

The goal of defending the enterprise against security incidents means SOC teams are tasked to respond only when a risk has been realized; they react once an event has been detected. With current market dynamics, there is a growing requirement to not only optimize threat defense, but to look at the opportunity for more proactive cyber risk assessment and mitigation as a means to reduce the likelihood of an attack or breach and, in turn, help temper the frenzy of the SOC's constant firefighting mode.

Championing a security organization that equally focuses on cyber risk assessment and response is emerging as a key priority, and this can mean significant benefits for multiple functions across the security organization from the CISO, to the SOC, to IT Ops.

Gartner's 2022 Planning Guide for Security and Risk Management observes, "A sustainable security program that provides data-driven risk decision making and measurable treatments as an outcome is essential to manage the new normal. Up-to-date risk assessments and risk communication practices are the driving forces for improving the current state, as indicated by our recent interactions with clients."[8]

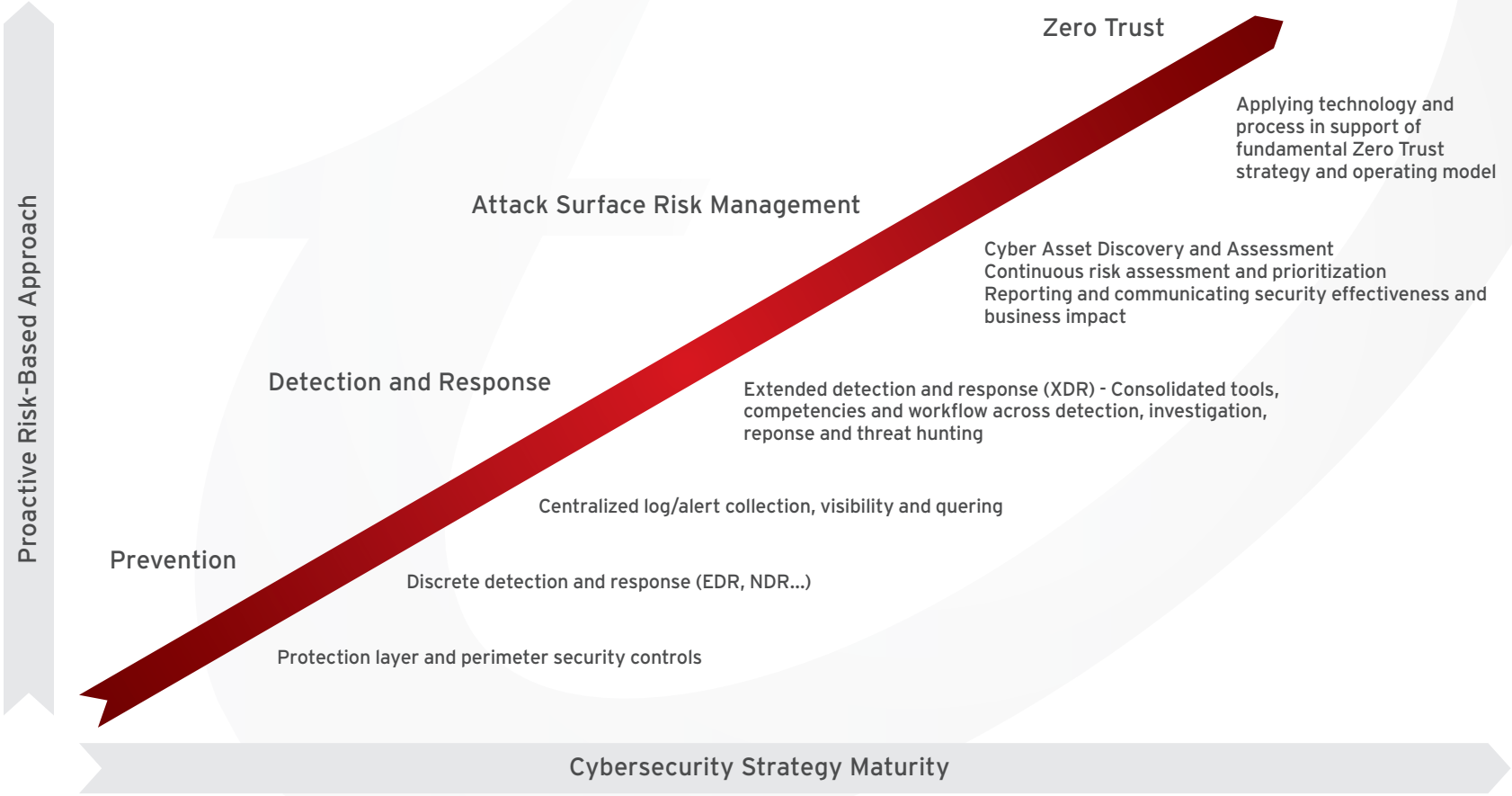
To improve security outcomes, you need to empower functional collaboration across IT and Security Ops by breaking down visibility silos and closing the gap between proactive risk management and reactive threat detection and response. This calls for reorienting the role of risk assessment from a high-level, point-in-time function to adopting a continuous risk management approach that permeates across security's functional lines.

Learn more about cyber risk:

Managing Cyber Risk:
The People Element

Cyber Risk Index (2H'2021):
An Assessment for Security Leaders

Cyber Threat Intelligence:
Risk Management Strategies



8 - Gartner: 2022 Planning Guide for Security and Risk Management, 11 October 2021

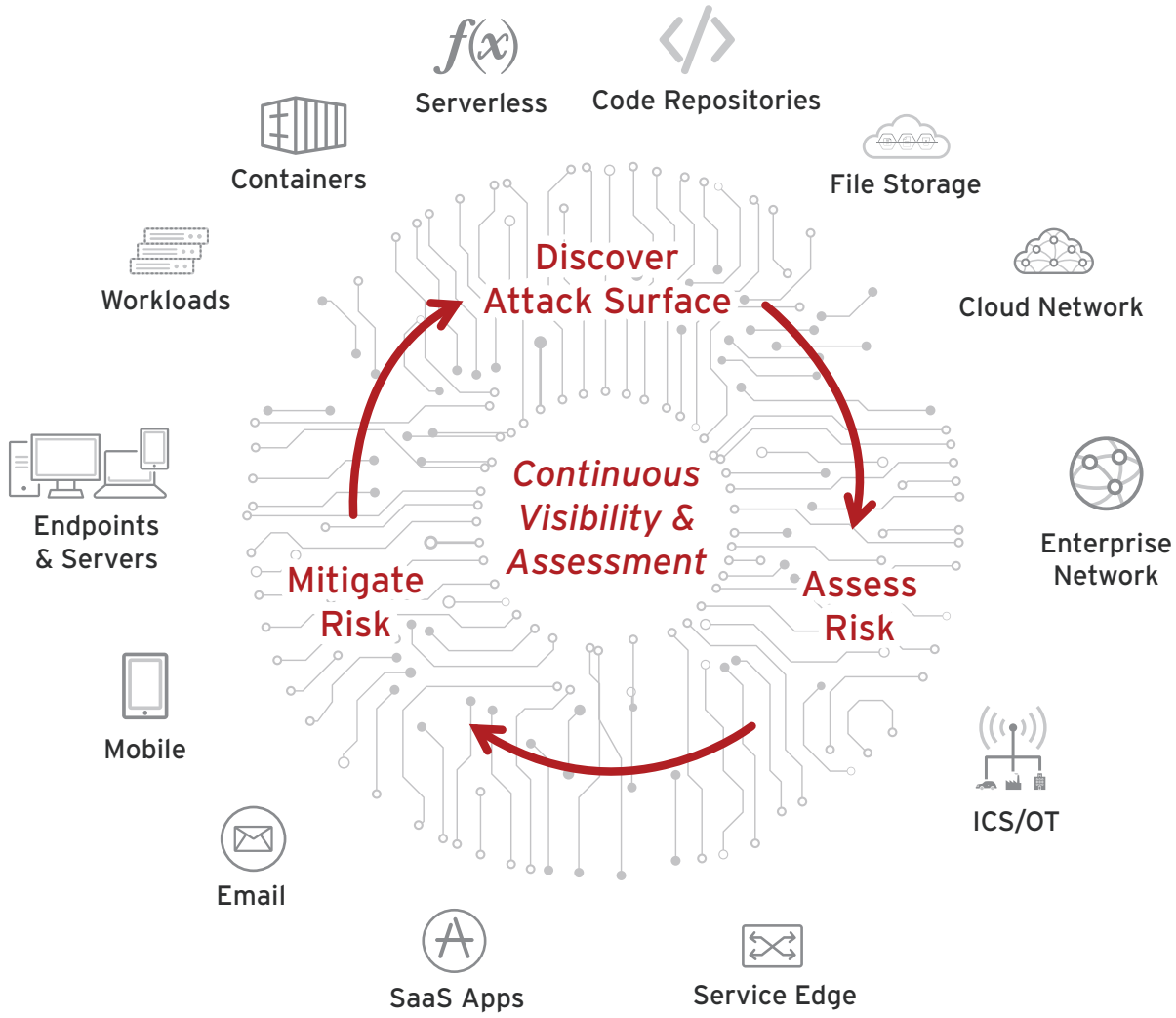
Attack surface risk management- Cyber asset discovery, risk assessment, and risk mitigation

Businesses continue to expand their digital footprints at an exponential rate, so it's easy for legacy systems, applications, devices, and more to get left behind in the process. Remote and hybrid work has led to a dramatic increase in connected devices—IDC predicts this number will rise to 55.9 billion by 2025. The sheer number of users, devices, and cloud apps has made attack surface management complex.[9]

ESG reported that only 9% of organizations believe they actively monitor their entire attack surface, so it's unsurprising that 69% of organizations experienced some type of cyberattack that started through an exploit.[10]

Overstretched security teams are challenged with finding the opportunity and resources to take stock of their cyber assets, and too often it involves a static audit which can be outdated as soon as the effort is completed. Auditing the attack surface is also only a first step. Understanding the risk and exposure of what that attack surface represents and translating that into mitigation actions is necessary to produce actual business value and performance outcomes.

The goal is to operationalize cyber risk management, which requires continuous command of the attack surface risk lifecycle across the phases of discovery, assessment, and mitigation.



9 - IDC: Security and the Global DataSphere: A Data-Driven World Needs its Data Protected, 2022

10 - Look for attack surface management to go mainstream in 2022 | CSO Online, 11 Feb 2022

Cyber Asset Discovery:

This should cover discovery and continuous monitoring of known, unknown, internal, and internet-facing (external) assets. Automated identification and profiling of the organization's dynamic digital attack surface provides an always-current inventory of cyber assets that the security team is responsible for defending. The goal is to gain the necessary visibility to answer questions such as:

- What is my attack surface?
- How well can I see what assets are in my environment?
- How many, what types, and what attributes are associated with these assets?
  Which are my high-value assets?
- How is my attack surface changing?

Attack surface management (ASM) vendors tend to focus only on this first stage of asset discovery. While this type of visibility is valuable, it alone doesn't solve the ultimate need to take that attack surface insight and be able to understand and assess the associated risk and exposure.

Learn more about attack surface management:

Mapping the Digital Attack Surface: Why Organizations are Struggling to Manage Cyber Risk

Why It's Time to Map the Digital Attack Surface

How to Better Manage Your Digital Attack Surface Risk

Attack surface concerns*

- 43% argue it's spiralling out of control
- 37% said it is "constantly evolving and messy"
- 62% admit they have blind spots when trying to secure their attack surface

* According to data from Mapping the Digital Attack Surface: Why Organizations are Struggling to Manage Cyber Risk

Risk Assessment:

Historically, efforts have been focused on point-in-time risk assessments for stakeholder reporting and big picture planning. What is emerging is a means for continuous, real-time risk assessment that can enable not only the strategic insight to determine security priorities and impact, but it can and should provide tactical insight that dives deep into specific risk and threat factors, including consideration for individual asset risk and criticality, vulnerabilities, security misconfigurations, risk exposure, attack activity, and more. Ideally, this risk information will be contextualized for greater understanding, presenting answers to questions such as:

- Can I quantify my risk? What is my overall risk score?
- Is it increasing or decreasing over time?
- How does it compare to peers in the industry?
- Where do I see the most significant security risks?
- What risk factors need immediate attention?

Risk Mitigation

The attack surface insight provided should drive prioritized mitigation recommendations that can lower risk exposure - patch for a high-risk vulnerability, change configuration options on a prevention control, and control user access parameters as just a few examples. There should be options to automate and orchestrate risk response across the enterprise for greater efficiency. This type of actionable insight can focus and help coordinate teams - across the SOC/SecOps through to IT Ops - on the activities that will make the most difference in reducing the chance of successful attacks or breaches.

The opportunity is to create a common framework and a single pane of glass from which teams can work across their borders to contribute and benefit from greater risk management. Depending on the capabilities, the SOC's XDR platform could present an opportunity to realize this broader goal.

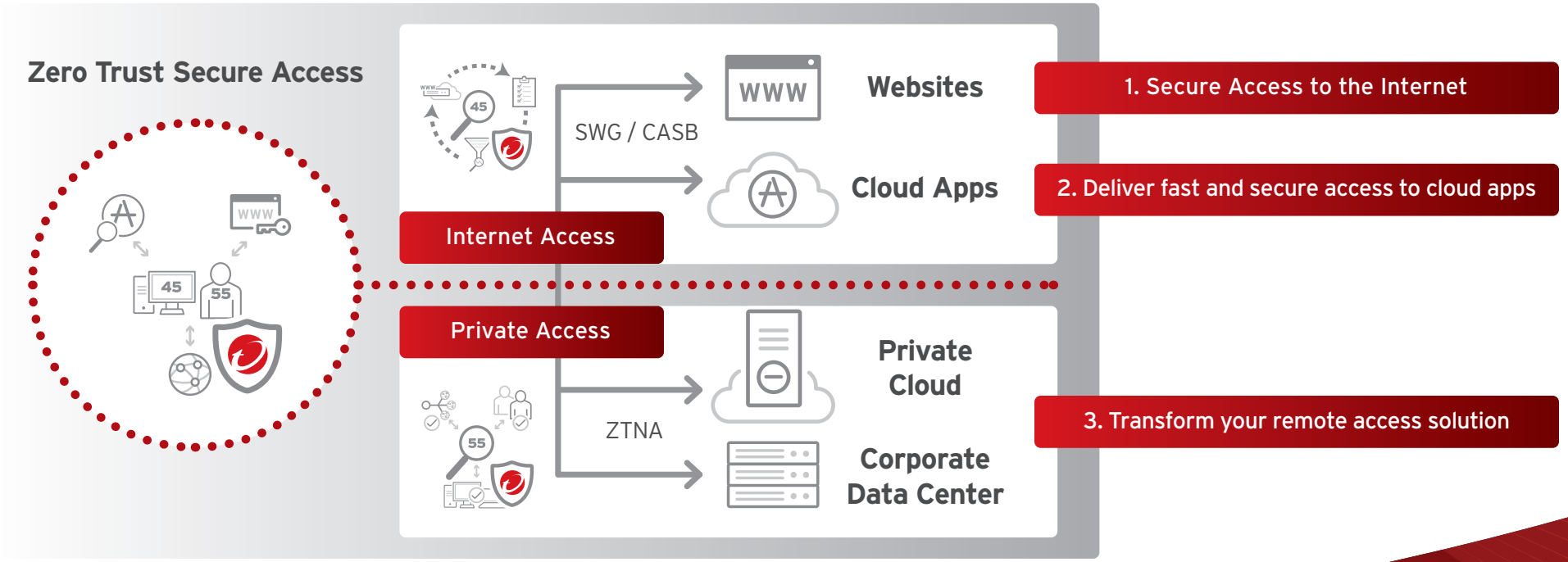
Investments in XDR mean there is data, analytics, integrations, and a technology architecture in place that could act as a foundation to serving other use cases and providing insight and operational value beyond the realm of detection and response. It can be a natural point of solution extension since there are mutual influence points between attack surface risk management and XDR. More proactive risk prioritization and mitigation benefits the SOC by reducing overall exposure and the potential of a security incident. Conversely, detection data collected by XDR provides valuable insight into attack surface threat activity and how current defenses are coping. This in turn can inform risk assessments and response recommendations.

Supporting zero trust strategies

Taking an integrated approach to risk management and threat detection and response can help organizations operationalize elements of a zero trust strategy. Zero trust fundamentally operates from the principle of least privilege. Any connection—whether it is from inside the network or not—should be considered untrustworthy. Considering that there are so many different entry points or connections into an enterprise now—BYOD devices, remote work, cloud elements, and as-a-service solutions—this is no easy feat.

Enterprises are forced to look at new ways of how to assess risk and posture, which requires assessing risk in a very detailed way: looking at multiple factors of identity, user and device activity, application, vulnerability, and device configuration. This assessment cannot be binary, nor static (for example, you are an employee and therefore you are always trusted). This is a continuous process so that if risk status changes, so can trust parameters.

Applying the attack surface risk insight and analysis discussed above can support zero trust strategies and result in implementing mitigation controls, as we are seeing with the shift toward Secure Access Service Edge (SASE) for example.



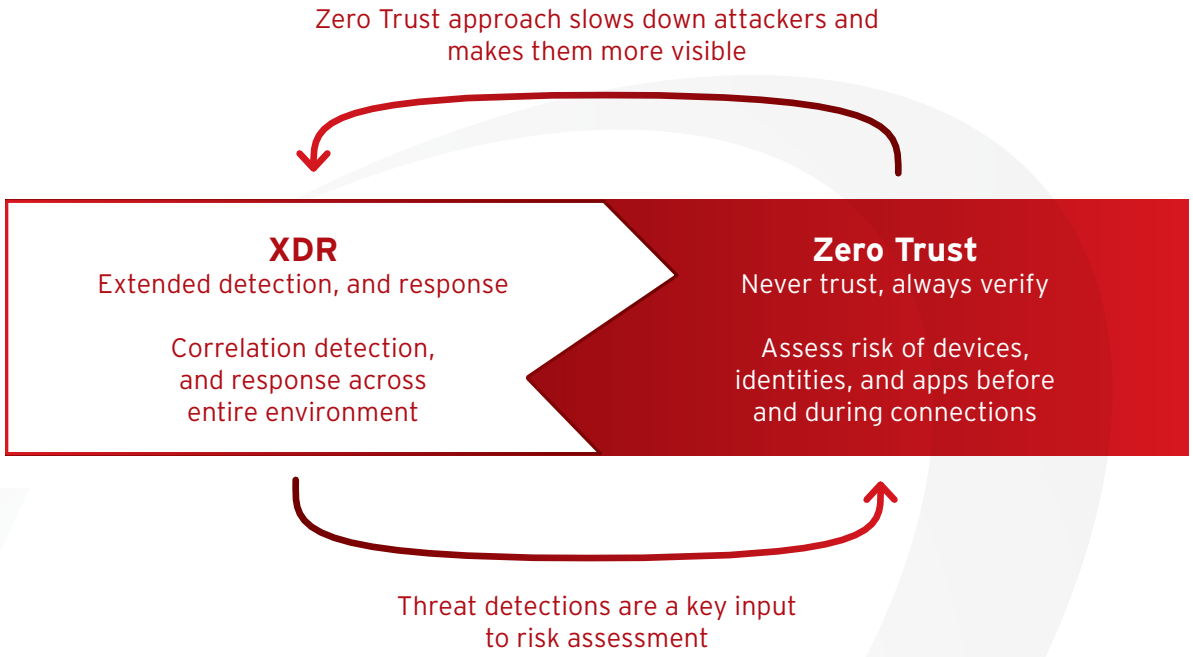
Supporting zero trust strategies (continued)

Modern SOCs should leverage tools aligned with the SASE model, which would help them efficiently process and analyze incoming and outgoing data to detect and address suspicious or unauthorized activity as soon as it occurs.

XDR alongside risk insight and mitigation that is aligned with zero trust can further enhance security. Strong endpoint controls provide a solid foundation for verifying and establishing trust by providing SOC teams with comprehensive endpoint visibility into potential threats. Without said visibility, it's an uphill battle to establish trust in good faith.

Additionally, since XDR continuously collects and correlates data, it establishes the continuous assessment pillar of the zero trust strategy. This means the asset will be continually reviewed and reassessed to ensure it remains uncompromised. And in the event of suspicious behavior, such as simultaneous logins from various geolocations, XDR will send a notification for the SOC to withdraw access and terminate a potential attack vector.

SOC organizations that can harness and capitalize on the continuous interplay between discover, assess, and mitigate will see the path to new and better SOC outcomes.



The Cyber Risk checklist:

- Do I have a complete and always up to date view of my growing attack surface across known, unknown, internal, and internet-facing (external) assets?
- Can I examine specific risk and threat factors to identify where I am most exposed?
- Do I know what mitigation actions I should take, and what kind of impact they will have?
- Am I confident in my ability to be proactive in reducing the likelihood of an attack or breach?
- Do I have the information I need to understand and communicate the business impact of risks?

Learn more about ZTNA:

How Zero Trust and XDR Work Together

How to Use Zero Trust Security for the Hybrid Cloud

A Secure Access Service Edge (SASE) Guide for Leaders

How to Apply a Zero Trust Security Model to ICS

3. Converging Security Solutions to a Cybersecurity Platform with Supporting Services

Security infrastructure for enterprises has become as complex as the threats it's trying to defend against. This can present hurdles and roadblocks instead of being the enabler the security organization needs. Achieving a more holistic approach to managing security operations is difficult with siloed architectures, views, analytical capabilities, and workflows. And silos also cause security gaps that can be exploited, especially in our increasingly distributed world.

In the 2022 Planning Guide for Security and Risk Management Gartner notes, "With the increase in remote work and the migration of applications and data to cloud services, the perimeter is gone. Digital assets—and individuals—are increasingly located outside of the enterprise, forcing organizations to rethink their approach to security controls. Traditional security controls are hard to adapt to this new reality, so a new architectural model for security is needed."[11]

11, 12 - Security Operations on the backfoot: How poor tooling is taking its toll on security analysts, 2021

Leveraging a platform approach

With the level of technological innovation seen this past decade, many enterprises pursued a best-of-breed solution strategy as a means to keep ahead of the threat landscape with the most compelling technology available. While each investment may have driven initial value, that value diminished as the next new thing came along. And unfortunately, for too many organizations, this has left them with dozens of distinct solutions that don't connect with each other and, hence, don't come together to solve their challenges. In fact, the disconnect has created new problems to solve.

Trend Micro Research found that 55% of SOCs have security infrastructure that is not in use, with the most common reason being lack of integration.[12]

Security and IT Ops must support a variety of environments, systems, and applications. As such, monitoring and managing each—and moreover, the connections between each—can get complicated and distract from their very purpose of defending the enterprise.

The solution? Shifting from point products to a comprehensive cybersecurity platform to:

- Gain comprehensive visibility and control for greater security effectiveness
- Improve operational efficiency by minimizing constraints and maximizing contributions of analysts

Security-minded organizations are converging on a single platform to consolidate tools and activities for a more seamless operation. This gives enterprises a means to integrate security visibility, analysis, and controls across an array of security layers and data sources while enhancing protection, scalability, and performance.

Previously, the in-depth coverage and capabilities of a cybersecurity platform were only available to large, established organizations that could afford to architect their own security ecosystem. Now, in partnership with a platform vendor, a much broader range of organizations can leverage the protection of an integrated platform without the heavy lifting once required.

Even organizations that have invested in specific point products can benefit from adopting a platform-based approach. The opportunity to resolve longstanding pain points while laying the groundwork for consolidation, knowing that each addition will mesh seamlessly with the others and unlock new benefits through synergy, makes it a worthwhile endeavor.

While the main goal is to reduce and consolidate the number of disparate tools, no platform can or should provide all security and security-related functions for a company. A cybersecurity platform's effectiveness is only as great as its ability to integrate within the enterprise's IT ecosystem. An open API strategy is required for the integration with other systems to provide critical information for added insight, perform additional security functions, automate tasks and response actions, and complete other key activities.

A platform is about consolidating where you can, tying it together with your other sources and systems to provide all the security and connectivity that your company needs to rely on in its daily operations.

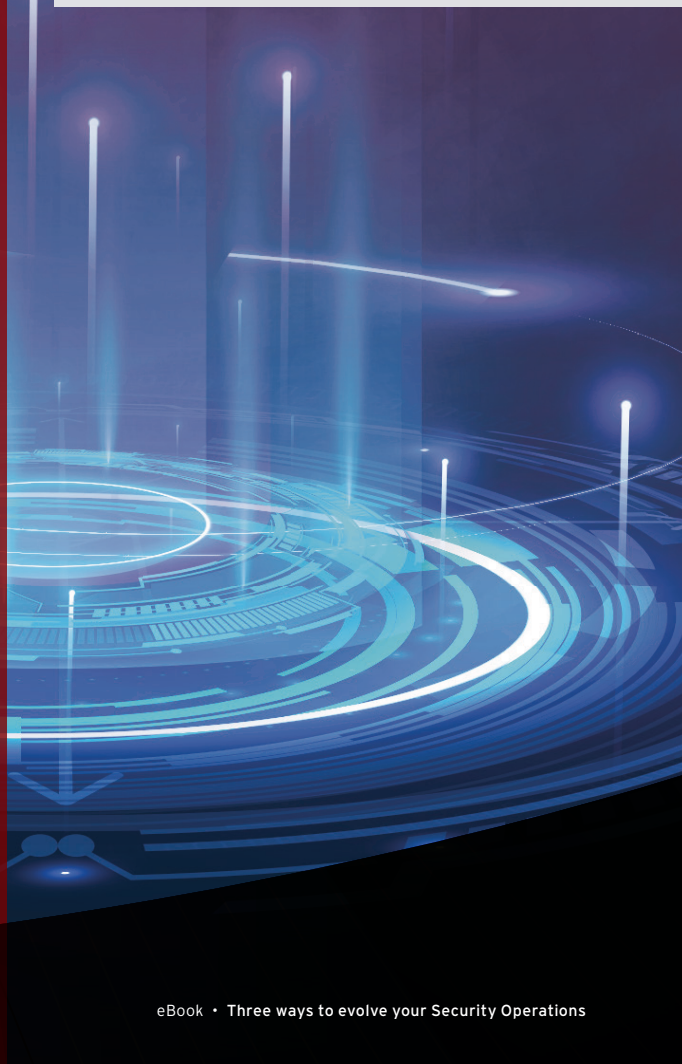
11, 12 - Security Operations on the backfoot: How poor tooling is taking its toll on security analysts, 2021

66% of organizations are actively consolidating the number of security operations tools in use, according to ESG

Learn more about a platform approach to cybersecurity:

Addressing Cyber Risk with a Platform Approach

What is a Cybersecurity Platform?



Supporting both cloud and on-premises environments

A cybersecurity platform must be based on a cloud-native architecture as it can offer analytical and computing advantages over on-premises architectures. The ability to leverage the power of the cloud to collect, synthesize, and analyze the high volume of data and activities feeding into the platform provides a level of function, performance, and scalability that would be impossible to achieve with on-premises solutions.

Having said that, any platform should support hybrid environments and be able to capitalize on data from any existing or required on-premises components. Despite a dizzying pace of cloud adoption, hybrid environments are a reality for most, and any platform needs to accommodate and operate with those requirements in mind. On-premises solutions, whether implemented by choice or by mandate, are part of the ecosystem and need to be equally considered as part of the security strategy.

Automating security processes

A part of any security architecture discussion should be the level of automation that can be acquired. Automation is a force multiplier for security teams, especially those leveraging a platform. Under-resourced security teams combined with the chaotic threat landscape have created massive demand for streamlined workflows and automated processes for alert monitoring, triage and response, threat intel, and compliance—to name only a few applications.

When making plans to implement automation, SOC/SecOps must remember that automation should focus on enhancing human work, not replacing it altogether. It needs to augment security analysts' efforts by speeding up standard operation procedures, removing manual steps, and enabling quick analyses and action that may not be able to be executed otherwise. Automation should focus on facilitating tasks without removing human input that can offer the reasoning and creativity that is often needed when dealing with complex situations.

According to Gartner, automation needs to aid processes that are well established and often repeated. SOCs should ask themselves these questions before making moves to automate:

- What processes could specifically benefit from automation?
- How many times have these processes occurred?
- Are their needs consistent across the board?

A platform's automation options should enable an organization to:

- Reduce the time required to build automation themselves. (With already stretched resources, the SOC can leverage a library of ready-made automation workflows/playbooks.)
- Reduce the skill set required to develop custom automation. (Most enterprises don't have the in-house skills to code and operate automation, so they need automation built by experts.)
- Address the process immaturity. (Many organizations haven't built good processes in the first place, so they can leverage recommended/best-practice workflows as established by the platform provider.)

51% or organizations have improved threat detection as a result of automating security processes via playbooks. - ESG

Strategic use of managed services

Many organizations are strategically using managed services to reduce internal resource requirements, gain complementary competencies and obtain much-needed security expertise.

In particular, they are opting to supplement any internal resources with managed detection and response (MDR) and/or incident response (IR) services that can offer dedicated resources to ensure threat monitoring around the clock, and critical response in the event of an attack. This approach to services enables security staff to focus on improving their security program and expanding their strategic focus.

All types of organizations across all levels of maturity can have a use case for MDR services. Organizations who have constrained resources and skill sets that cannot execute detection and response effectively in-house look to MDR services as a full outsourced partner to manage activities on their behalf. On the other end of the spectrum, you may have large, mature organizations who have already built a SOC but see an MDR service as supplementary to in-house activities. (For example, having a" second set of eyes" and monitoring coverage for nights and weekend. Access to added expertise and threat intelligence can help in both investigations and threat hunting.)

In either of these cases, or a use case in between, MDR is adopted in recognition that an expert service can perform certain activities more effectively or efficiently than the enterprise is able to do. The goal is to clearly understand that gap and support it appropriately with the right level of service.

Incident Response (IR) is another useful place for SOCs to leverage the help of specialized services. IR services often combines cyber crisis management, threat hunting expertise, digital forensics, and expert guidance that is often difficult to maintain in-house. It helps supplement teams in cases of a breach where there is an urgent need for added resources to help contain, minimize, and remediate an attack.

A platform with built-in managed services can provide the best return for SOCs as it can ensure integration across the platform, and the service is seamlessly supported from deployment.

59% of organizations are using managed services as an extension of their internal resources

SOC Modernization and the Role of XDR – ESG[13]

"By 2024, more than 90% of buyers looking to outsource to security services providers will focus on threat detection and response services."

The Managed Security Services Landscape Is Changing – Gartner[14]

State of managed services

- 96% of organizations are using managed services to some extent with high satisfaction
- 52% of security professionals believe service providers can do a better job with security operations than their organization can
- 88% said they will increase their use of managed services for security operations

13 - ESG Research Study, SOC Modernization and the Role of XDR, June 2022

14 - Gartner: The Managed Security Services Landscape Is Changing, 14 April 2020 Gartner Blog Network

The SOC Platform checklist:

- Are siloes in my security infrastructure creating security gaps that could be exploited?
- Am I lacking visibility and are my workflows fragmented because of a lack of integration with systems, environments, or other solutions?
- Am I doing everything possible to leverage the power of the cloud? In addition, am I making the most of data from my on-premises components?
- Is my team employing automation to enhance their work and streamline time-intensive processes?
- Would outsourcing certain services improve my strategic focus and free up internal resources that could be better spent elsewhere?

The Bottom Line

Security leaders are tasked with leading the charge by implementing a modernization strategy that includes XDR, attack surface risk management, and a new architectural model that can support emerging priorities.

Although the demands of the ever-growing attack surface and evolving threat landscape can seem overwhelming, leaders who take proactive steps today will benefit from a strong foundation to build upon as needs shift and change in the coming years. With the expansive, in-depth protection of a platform and new methods to bolster their defenses including automation, mapping the attack surface, and applying zero trust strategies, security leaders can be confident they're prepared for whatever comes next.

For more information visit **trendmicro.com**