SPOTLIGHT

Sponsored by: Trellix

Organizations cannot afford to adopt extended detection and response (XDR) without first assessing and then maturing their discipline in endpoint risk management.

Maturing Endpoint Risk Management Leads to XDR Success

June 2023

Written by: Michael Suby, Research Vice President, Security and Trust

Introduction

Extended detection and response (XDR) starts at end-user devices.

As an interface to network- and internet-connected applications and the engine for local programs, end-user devices have been and will continue to be the vehicles of work.

End-user devices are challenging from a cyber-risk perspective because of their large numbers, variation in configurations and software applications and, depending on the form factor, mobility. In effect, end-user devices constitute a broad and dynamic attack surface. It is no surprise that threat actors frequently target end users and their devices as an initial point of entry and compromise into organizations' systems.

This reality has a conditional bearing on the use of endpoint detection and response (EDR). Unless security teams can rein in the susceptibility of this endpoint attack surface and limit compromise, EDR investments will not reach their full potential. Rather, a high volume of endpoint-emanating alerts will continue, and the number of live threats will likely escalate, forcing EDR-using security analysts into a frequent and reactive firefighting mode.

AT A GLANCE

KEY TAKEAWAYS

- Before jumping to XDR, organizations need to ensure that they have mature endpoint risk management (prevention, protection, and endpoint detection and response) practices.
- Detection and response, whether EDR or XDR, should serve a double duty: mitigate active threats *and* provide an essential feedback loop in fortifying prevention and protection.

The remedy is to guide more of EDR's operations into threat mitigation. For this to occur, security teams need to follow a holistic and cyclical approach to endpoint risk management. In this strategy, security teams are actively engaged in the three pillars of endpoint risk management: prevention, protection, and endpoint detection and response. This approach is cyclical as detection not only supports attack-mitigating responses but also identifies gaps in prevention and protection so that these pillars can be fortified.

It's important for organizations to acknowledge that endpoints are not always the tip of the spear in cyberattacks but are part of multivector attack campaigns; in this way, organizations can recognize how the broad sense and response capabilities of XDR are the logical evolution in EDR. However, unless security teams have first matured in their use of EDR to mitigate threats, the jump to XDR is likely to also suffer from unfilled expectations in curbing cyber-risk.

In this Spotlight paper, IDC offers recommendations on how organizations can mature in endpoint risk management and establish a sturdy foundation for XDR.

Three Pillars of Endpoint Risk Management

Endpoint risk management entails continuous focus on prevention, protection, and detection and response.

Prevention

Shrinking an organization's attack surface reduces threat actors' openings to land and then expand. This is the realm of prevention: understanding and reducing the attack surface.

Shrinking an organization's attack surface reduces threat actors' openings to land and then expand.

Organizations begin prevention by continuously assessing the state of their devices. While this may seem trivial, many organizations do not have a current or complete inventory of their end-user devices and installed software. And without an up-to-date inventory, even disciplined hygiene practiced on an incomplete device inventory will leave gaps for threat actors to exploit. So, step 1 is to improve inventory management processes and procedures to ensure the inventory of devices and software is current and accurate.

Working from a current and accurate inventory, organizations can then confidently and comprehensively conduct vulnerability assessments and deploy software updates and patches in a prioritized manner. In support of prioritization, we recommend that organizations assess vulnerabilities based on severity if the vulnerability is exploited (i.e., the impact to the business) and the probability of being exploited. In addition, vulnerability assessments should encompass all layers of the device's software stack: firmware, operating system, and applications.

Another important element of prevention is tuning devices and applications for business needs only. At the device level, this means defining and enforcing device control policies such as use of USB drives and connections to peripherals. For applications, a combination of application whitelisting and blacklisting will limit exposure of unsanctioned applications installed on end-user devices. Deeper into sanctioned applications are policies that control which application processes or executables are allowable (i.e., application allowlisting).

Tuning also entails optimizing the features in endpoint security and endpoint management applications. These business-critical applications are perpetually improving with enhanced and new features. Often, vendors introduce improvements to combat evolution in threats and streamline the administrator experience. Therefore, it is in an organization's best interest to stay abreast of updates to these applications in order to assess new and updated features and fold in what is useful for the organization.

A final point on prevention is cross-team collaboration. Often organizations have role separation between endpoint security and endpoint management functions. While separate, these teams should not operate in isolation. For example, the SecOps team should collaborate with the endpoint management team in defining the gold image for endpoint devices that balances risk mitigation with business and end-user productivity. Also, opinions on patch priorities and patching speed may differ. Again, the two teams should forge a collaborative relationship so that a jointly acceptable balance can be maintained.

Protection

Although prevention reduces the attack surface, threat actors will not pull back. They will continue their attempts to compromise end-user devices. Protection is the next layer of defense, and its main objective is to thwart attacks at the first signs of maliciousness.

Among IDC's recommendations that are foundational to a holistic endpoint risk management strategy is to invest in the best possible next-generation endpoint protection platform (EPP). This entails an EPP that has the following attributes:

- **Comprehensiveness.** As attacker techniques have evolved, a single detection engine such as pattern matching of known malware is insufficient. Instead, multiple engines are needed to detect a wide range of malicious code and behaviors — those that have been seen before and new variants.
- **Accuracy.** While comprehensiveness is vital, it is not the only measure of protection efficacy. The detections must also have a high degree of accuracy — that is, what is detected as malicious is truly malicious. In comparing EPPs, look for high marks on comprehensiveness and a very low frequency of false positives (i.e., classification of code or behaviors as malicious that are in reality benign).
- **Continuous improvement.** Threat actors will research EPPs to identify and then exploit weaknesses. EPP vendors must be relentless in evolving their products to maintain comprehensiveness and accuracy. Vendors' product updates, feature announcements, and engine refreshes are positive indicators.
- **End-user transparency.** Similar to prevention, protection must also balance risk mitigation with the potential impact on business operations and end-user productivity. Ultimately, EPP operates silently in the background. Detections and actions to combat threats are conducted transparently to end users. But to conduct these operations, the EPP will compete for CPU and memory resources with other software applications running on the end user's device. Consequently, EPP vendors design their products to be resource efficient without sacrificing protection efficacy. EPP peak resource utilization and duration are suitable measurements to gauge resource efficiency.
- **Resiliency.** Threat actors will seek to disable the EPP as part of their attack strategy. To combat this approach, EPPs must have immutable means to monitor their own functioning, detect corruptions, and restore. Restoration cannot be completely end-user transparent, but it should involve end users only on a minimal or very limited basis, and administrators should be allowed to conduct this operation remotely.
- **Recovery.** In light of the unrelenting plague of ransomware, organizations need options to recover files that were encrypted as part of the ransomware attack and rewind other changes the threat actor may have made (e.g., modification to local registries). Although not a feature in all EPPs, local rollback remediation is a recovery option for ransomware and other attacks that were detected after initial compromise. Similar to EPP restoration, rollback remediation may interrupt end users' routines. Nevertheless, the interruption is warranted to return devices to their previous uncompromised and fully operational state.
- **Customization.** EPP is a security workhorse that is expanding in available features. While some features justify inclusion in all device deployments, others may be justified for only a subset of end-user devices or conditional on circumstances. Additional CPU and memory requirements may also need to be considered. Thus, SecOps teams must be able to easily tailor EPP features based on their organization's unique needs.

> Protection must balance risk mitigation with the potential impact on business operations and end-user productivity.

Recognizing that cyberattacks aimed at end users and their devices are frequently perpetuated through email and web browsing, organizations should also leverage the filtering and protection features in email service subscriptions, web security gateways, and browsers. In doing so, SecOps will reduce the inflow of attacks directed at end users and their devices.

Detection and Response

Even with a disciplined approach in prevention and protection, determined threat actors can still succeed and endpoint compromises cannot be ruled out. EDR serves as the third pillar of endpoint risk management — both responding to active threats and providing a feedback loop.

EDR in Active Threat Response

In its original use case, EDR is the backstop to stop attacks that find openings in end-user devices and evade endpoint protection detections. Ultimately, the objective of EDR is to neutralize active threats before an organization suffers material harm.

While a sophisticated operation, EDR active threat response can be summarized in the following steps:

- Gather, filter, correlate, and present relevant data from which a qualified list of security incidents is assembled.
- As needed, enable security analysts to pivot into deeper incident investigations.
- Assess security, compliance, and business risk and rank the severity and immediacy of the risk.
- Assemble and present response options.
- Follow through on selected response or responses. Depending on the response and the tools and workflows used by the organization, both inter-team and tool orchestration may be required to complete the selected response.

Since security analysts are up against the clock to intercede before harm occurs, enabling speed, precision, and confidence in decision making is a core tenet of an EDR solution. Consequently, automation interwoven into all steps is vital in the effective use of EDR.

EDR as a Feedback Loop

In this use case, EDR is a fortifying feedback loop for prevention and protection. With visibility, EDR brings to the forefront how, through real-world incidents, attackers identify and seize upon exploitable opportunities in an organization's endpoint estate, gaps in prevention and protection, and pathways to higher-valued assets.

For SecOps teams, their opportunity is to apply what was learned from EDR-handled security incidents and improve the effectiveness of prevention and protection. In doing so, the SecOps teams shift more of their focus to preventing security incidents that require EDR reaction.

With highly evasive and targeted attacks, the full scope of EDR-handled incidents is only partially uncovered. While neutralization of an active threat appears successful, the threat actor may make tweaks to the endpoint that are not gathered by the EDR system. Incident-handling success is, in reality, only partial. In these circumstances, SecOps teams need the option to go further back in history, prior to the triggering of EDR involvement, to ascertain the full root cause. This is the discipline of forensics, a post-incident, deep-dive assessment. Because forensics analysis is dependent on historical data, endpoint data recording for forensics purposes must be continuous and immutable. Armed with post-incident forensics material, the SecOps team is equipped to develop fortifications that span prevention and protection and can also include refinements to EDR incident triggers.

Benefits of Disciplined Endpoint Risk Management

IDC believes there are three streams of benefits — strategic, operational, and XDR on-ramp — in being disciplined in endpoint risk management.

Strategic

Foremost, a disciplined and holistic approach to endpoint risk management contributes to a positive behavioral effect. It directs behaviors and decisions on evolving SecOps practice from reacting to threats to the overall objective of continuously improving risk management.

Second, there is an equally positive and correlated effect of shifting measurements of SecOps success. Rather than concentrating on measurements of post-compromise incident handling, such as mean time to detect (MTTD) and mean time to respond (MTTR), organizations should place greater emphasis on reducing the number and severity of security incidents. While both are important, overemphasis could result in diminished focus on and fewer investments in keeping bad actors out.

Operational

Operationally, a focus on endpoint risk management contributes to a higher degree of standardization across the device estate and, conversely, less complexity because there are few instances of one-off device configurations. And with less complexity, there are fewer gaps in prevention and protection that threat actors can exploit. In addition, fewer one-offs and less complexity lead to higher SecOps productivity because scalability is a byproduct of standardization.

We anticipate that from an alert fatigue perspective, alert processing will change. With more attacks being automatically neutralized via prevention and protection, the mix of alerts will shift from alerts pertaining to active threats to alerts that confirm attempted attacks were effectively thwarted. In addition, we also anticipate a decline in the number and severity of urgent and critical security incidents to be investigated and resolved.

Security is a team sport, but the team is not only personnel with security titles. IT personnel are integral to endpoint risk migration because their responsibilities entail more direct engagements with end users and their devices. IT is on the front line of affecting endpoint risk management. Consequently, a top-down focus on endpoint risk management will encourage SecOps and IT to collaborate. In addition, as SecOps teams have found themselves with technology sprawl in their security stacks, a similar scenario of overlapping capabilities and redundant and possibly conflicting estate inventories among SecOps-funded and IT-funded tools is also likely. We believe that this represents another opportunity for cross-team collaboration and collaboration that will contribute to tool and vendor consolidation resulting in cost savings.

XDR On-Ramp

IDC contends that XDR is a logical evolution from EDR. Functionally similar but broader in scope, XDR expands the aperture of signals in detecting active threats and broadens the response options. Similar to EDR in endpoint threat mitigation, the expanded real-world view of security incidents that XDR affords also contributes to more options to tighten prevention and protection controls over more IT assets and security control points. Furthermore, we believe the previously mentioned strategic and operational benefits can be expounded with XDR. The broad scope of XDR contributes to more beneficial opportunities.

However, an immediate jump to XDR is not suitable for all organizations. Instead, gaining mastery of EDR (technology and process) equips SecOps to better articulate and realize the incremental benefits of XDR. So, rather than jumping into XDR, organizations should step into XDR from a strong foundation of EDR with proven success in holistic endpoint risk management.

Considering Trellix

Trellix, a result of the 2021 merger of McAfee Enterprise and FireEye, has a broad portfolio of products in endpoint security, email security, network security, data protection, and cloud security. Unifying administration, management, and cross-product integration in support of XDR is the Trellix X-Console.

Underpinning Trellix's XDR strategy and also applicable to any products in the Trellix portfolio, the company's intentions are to advance the X-Console's user experience (UX) to be second to none. Objectives of the UX redesign include elevating workflow automation, enhancing observability, accelerating time to action, eliminating tedious tasks, minimizing pivots, and expanding push-button playbooks.

In endpoint security, Trellix is bringing together the best of both companies and building a unified solution. The solution consists of McAfee's multiple endpoint protection engines, a superset of EDR capabilities from McAfee and FireEye, and threat hunting and forensics capabilities from FireEye. A layer deeper, the agent is being built on the modular architecture championed by FireEye. This modularity allows customers to tailor capabilities over and above those included in the default package to better meet their cyberneeds and changing circumstances. In addition, coming from the McAfee side are capabilities in host data loss prevention, desktop encryption, application and change control, and mobile security.

Trellix is also assisting customers in closing gaps in security posture. Two features to highlight are adaptive defense (a continuous process of assessment and guided strengthening of security posture) and live response (a mechanism to remediate hosts and refine security settings at scale with ease and certainty).

Challenges

The foremost challenge facing Trellix is how quickly and effectively it can accomplish the mash-up of McAfee Enterprise and FireEye products and technologies. It is, in essence, attempting to upgrade the car while driving through rush-hour traffic. In addition, with other security vendors in the past having attempted similar mash-ups with uninspiring results, Trellix is at risk of being greeted with market skepticism. Openness by Trellix in sharing tangible evidence of its upgrade progress can offset this skepticism.

Concurrent with the in-motion upgrade challenge, Trellix has the additional challenge of modifying its product and channel strategy to align with the profile of customers it intends to serve long term. Inheriting companies with lengthy histories in the security field, Trellix is weighed down by a very broad customer base spanning very small businesses to global multinationals and an expansive product lineup in need of pruning. Consequently, Trellix must balance its attention, resources, and investments over building for its future while selectively downplaying its past. In contrast, other vendors competing against Trellix with shorter histories do not have this balancing challenge.

Conclusion

Organizations cannot afford to embark on XDR without first assessing and then maturing their discipline in endpoint risk management. Lacking maturity in endpoint risk management, SecOps teams are in danger of entering a perpetual and reactionary cycle of tamping down security incidents that, in reality, could be reduced in number and severity by paying greater attention to strengthening the security posture of their endpoint estates and elevating endpoint protections. Moreover, organizations should embrace detection and response solutions, first EDR and then XDR, for the two essential functions they can and should deliver: active threat response and feedback mechanism to heighten prevention and protection efficacy.

> Being serious about reducing cyber-risk requires vigilance in holistic endpoint risk management.

About the Analyst

***Michael Suby,** Research Vice President, Security and Trust*

Michael Suby is a Research Vice President in IDC's Security and Trust research discipline. In this role, Mr. Suby concentrates on endpoint security and, in collaboration with IDC team members, engages in research spanning a wide and evolving spectrum of security and trust topics.

MESSAGE FROM THE SPONSOR

More About Trellix

Endpoint security is foundational for any security program and the baseline for securing enterprises of all sizes, as each endpoint serves as an entry point into the business. Organizations must be equipped to act ***before, during, and after*** an attack to protect their digital assets and reduce business impact.

Trellix Endpoint Security is a foundational Endpoint solution focused on delivering a complete endpoint security lifecycle and improving visibility & control. Trellix optimizes Endpoint Protection to reduce the risk of incidents and minimize SOC workloads. It offers pro-active attack surface management, a rich and fully featured threat prevention stack that includes next-gen anti-malware. The platform simplifies and increases response efficiency with guided investigations, forensics, and root cause analysis, all integrated with threat intelligence for prioritized threat response. Trellix strengthens security operations with this solid endpoint foundation through native integration with XDR that delivers advanced correlation for better prioritization of threat alerts.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.