White Paper

XDR
What to Know, What to Do Now

XDR: Get Past the Hype to Get it Right

Everybody's talking about XDR — and with over 30 vendors already claiming to offer XDR-compliant solutions, it's essential to separate the reality from the hype. Mimecast collaborates with many XDR providers, including best-in-class cybersecurity and IT companies that are also a part of the XDR Alliance. Our Secure Email Gateway (SEG) telemetry, alerts and overall functionality is critical to determining the initial entry point and source of many attacks, and we help organizations respond effectively to these incidents –– it's why we were chosen as one of the first member companies of the XDR Alliance.

Working with XDR providers and their customers, we've learned quite a bit about XDR technology. Our insights can help you determine if XDR is right for you, and, if so, help you evaluate and plan for deployment. In this white paper, we explore XDR's promise, help you assess how it might fit in your environment, and show you how to prepare for XDR as you strengthen security ***right now.***

Key Takeaways

- Since 94% of attacks still appear first in email, integrating a best-in-class Secure Email Gateway into XDR architecture is crucial to success.
- XDR relies on more robust and comprehensive integration across the cybersecurity technology stack and beyond: it's essential to plan for that integration, from endpoint to email to cloud, with an XDR design matched to your business.
- In evaluating XDR, focus on its ability to drive automated or semi-automated responses, not just its ability to capture and analyze relevant data.
- As XDR evolves, it's important to recognize current gaps, understand their implications, and track vendor progress in addressing them.

Why XDR? The Problem and the Promise

In an era where disastrous breaches can come from anywhere at any time, security teams must sharpen their focus on threat detection, investigation and response. Organizations need to manage growing threats more coherently and holistically, with deeper integration and far more automation.

Extended Detection and Response (XDR) promises to unify threat detection, hunting, investigation and response. It can optimize all these cybersecurity functions by leveraging tightly integrated real-time or near-real-time data from key security systems and after analysis, triage and investigation instructing those same systems to take automated actions.

In addition to accelerating threat detection and response, XDR aims to improve the productivity of security analysts at all levels, as well as the SecOps teams they work for. XDR vendors promise that lower-level (Tier 1) analysts will be able to accomplish more via automation and be free of the many false positives that bedevil them. Higher-level (Tier 2/3) analysts will receive timelier, more sophisticated analytics and recommendations for remediating advanced attacks, and insights for performing more proactive threat hunting.

Accenture has described XDR as the "central nervous system" that organizations will finally have to help protect themselves and move toward zero-trust environments.[1] XDR may be foundational to long-term cybersecurity mesh strategies that integrate security analytics, intelligence, triggers, policy management/orchestration, and distributed identity fabrics in one cooperative ecosystem.[2]

How XDR Evolved

Integrated, holistic, proactive security has been the holy grail of the cybersecurity industry for many years, yet few organizations can claim to achieve it.

Some organizations first deployed Security Information and Event Management (SIEM) systems that collected enormous amounts of log and event data — taking a "big data" approach. These systems were meant to also address adjacent capabilities such as compliance and reporting tasks. But, since they brought multiple data sources together, it made sense to also try correlating their data to identify new threats.

Unfortunately, legacy SIEM-based threat management has failed in many organizations. As Gartner points out, some haven't been able to deploy SIEMs, others have "failed or incomplete implementations," and still others have restricted SIEMs to log storage and compliance.[3] Some SIEMs have struggled to transform data into actionable insight, and high levels of analyst expertise have been required to gain value. They also often deliver too many false positives, wreaking havoc with analyst productivity and making it likelier that real attacks will escape attention. Furthermore, not all SIEMs were designed to make it easy to trace a kill chain, or to rapidly identify, triage and remediate emerging attacks. Enterprise Strategy Group (ESG) reports that roughly one-third of SIEM users complain about the cost of licensing and operation, and many worry about analyst learning curves and the effectiveness of SIEMs in detecting previously unknown threats.[4]

[1] Growing zero trust security with an XDR strategy, Accenture I [2] Cybersecurity Mesh, Decentralized Identity Lead Emerging Security Technology: Gartner, eSecurity Planet I [3] Innovation Insight for Extended Detection and Response, Gartner I [4] The Impact of XDR in the Modern SOC, Enterprise Strategy Group

Some organizations added Security Orchestration, Automation and Response (SOAR) functionality, seeking to establish automated responses to recognized threats and intrusions. However, creating SOAR playbooks often requires specialized expertise that is hard to find for many organizations. Consequently, many threat responses remain manual.

In parallel, evolution of the endpoint-based anti-virus tools led to the development of Endpoint Detection and Response (EDR). Rather than attempting to identify emerging attacks through correlating "needles in haystacks" of massive logs, EDR focuses on data generated by modern endpoints. Based on the reduced scope of data that is endpoint-centric, EDR delivers continuous detection and more automated response at endpoints, providing analytics detection rules and threat intelligence-based detection to help organizations resist modern attacks such as fileless malware or ransomware.

EDR demonstrated that focused data combined with advanced machine learning and visualization could empower security teams to identify and remediate many threats more quickly, with less complexity. Even so, it has shortcomings. Absent data from other systems, such as email or cloud applications, EDR misses many attacks. Even if one is identified, analysts might not be able to understand its extent or be prepared for a similar attack next time.

XDR: The Next Major Step Forward

For those looking for solutions that focus on threat detection and response across the organization, EDR falls short because it's limited primarily to endpoint data and response, while SIEM falls short because of its very wide functional coverage and complexity. The natural approach is to integrate more sources than current point solutions, while being more prescriptive than legacy SIEMs, and that's what XDR promises. XDR aims to capture real-time data from a wider set of enterprise security systems, ***and*** drive automated responses through them.

Which systems? Potentially, many: email gateways, web gateways, cloud workloads and cloud access security brokers (CASBs), SaaS applications, IoT devices, network analysis and visibility tools, firewalls, identity/access management platforms, endpoints detection and response, and more. Of course, as Forrester observes, XDR should integrate only those inputs that actually improve detection, investigation and response — no more, and no less.[5] Cluttering a new XDR deployment with irrelevant data can make it harder to deploy and use, as occurred with many SIEMs.

Consider this hypothetical example of how XDR can improve on existing point solutions in the real world. An EDR system might recognize an unusual attempt to change a registry key on a given endpoint, but not understand the sources or implications of the attempt. In contrast, XDR could link this attempt with network telemetry from multiple systems to recognize a connection with traffic to a specific IP address, seeing how information traversed internal switches to reach a high-risk Internet site that delivered a keylogger-infected file to the endpoint. The XDR system, capturing email gateway telemetry an EDR wouldn't possess, could then link the same attack to an attempt to send emails containing high-risk links from the infected endpoint to accounts throughout the organization.

[5] Adapt or Die: XDR is on a Collision Course with SIEM and SOAR, Forrester Research

These machine learning analyses, based on multiple data sources, could recognize this attempt at widespread data exfiltration almost immediately. But that's only half the story. The XDR could also recommend a set of remediations and immediately execute them through the same linked systems. For example, it could isolate all endpoints impacted by the attack and instruct an email gateway to delete any dangerous emails delivered within the organization before the attack was discovered. Since this occurs in near-real-time, such an automated response could prevent most of those emails from being opened by recipients. Meanwhile, the XDR system has developed knowledge it can use to recognize attacks with similar characteristics going forward, enabling it to respond even more quickly and accurately in the future.

Unsurprisingly, many XDR solution providers are moving into delivering more detection and response use cases. And as traditional SIEM providers add more machine learning, visualization and analytics, they too are claiming XDR-style functionality. Therefore, over time, SIEM and XDR appear to be converging towards a broader threat detection, investigation and response (TDIR) set of capabilities — but this will take time.

Characteristics of a Full XDR Solution

XDR solutions are still rapidly evolving, but you should expect them to include the following attributes:

Cloud native.

XDR systems should leverage cloud scalability and flexibility. They should be able to collect data from remote systems and endpoints outside traditional enterprise perimeters and without VPNs. Some XDR solutions will be available in managed services versions called Managed Detection & Response, or MDR. With MDR, a service provider should include human analysts to handle some or all the manual response tasks that would otherwise be the responsibility of your security operations center, using a 24x7 coverage model.

Strong integration.

XDR systems should have much stronger integration support than SIEMs. While XDR connectivity will evolve and grow over time, XDR systems should offer robust core integration with endpoints, email and web gateways, network security systems and cloud workload protection platforms, among others.

Centralized, normalized data.

As Gartner writes, XDR systems should centralize, preprocess and normalize all the data streams they ingest, storing them in common data formats in a unified repository for analysis and query — ideally in a data store that can power the connection of new events (or series of events) that haven't been defined in advance. Unlike many SIEM systems, XDR should surface and uncover complex, low-and-slow attacks that manifest over time. Whether via new or overhauled architectures, XDR should overcome the data challenges associated with legacy compliance-centric SIEMs that have struggled to identify threats by layering analytics atop enormous data sets that are costly and impractical to maintain, especially where organizations are charged based on volume.

Automated, easy-to-customize responses.

As suggested above, XDR should go beyond SOAR, making it much easier to create, customize, select, prioritize and execute automated responses to both common and emerging threats.

Focus on analyst productivity.

As Forrester recommends, XDR systems should empower less experienced Tier 1 analysts to prioritize responses and execute automated responses. XDR should also empower more experienced analysts with all the tools, insights and automated workflows they need to investigate and address even highly complex attacks. Drawing on more sources of data and more advanced machine learning, XDR should accurately identify more threats and present fewer false positives. Visualization should make everything more intuitive. Finally, for both entry-level and experienced analysts, XDR systems should eliminate the need to switch among platforms for threat analysis, triage, remediation or hunting — making all these tasks more accessible and efficient

[6] Adapt or Die: XDR is on a Collision Course with SIEM and SOAR, Forrester Research

Approaches to XDR: Proprietary vs. Open

Analysts often distinguish between proprietary or “native” XDR solutions and open XDR solutions. With proprietary XDR, an organization buys into most or all of a single supplier’s security stack, assuming that the vendor will ensure integration of the security systems that feed the XDR solution, and execute its instructions, by providing most or all of those systems itself. Customers get a single point of contact, but they take on the risks of a single-vendor security monoculture — from vendor lock-in to suboptimal subsystems, to concerns that attackers can steal the keys to the kingdom by evading just one defender. Moreover, adopting monoculture solutions may require organizations to discard security systems that are working well (i.e., the dreaded rip-and-replace approach).

In contrast, open XDR systems (sometimes called “hybrid XDR”) assume that customers want to keep relying on best-in-class solutions such as email gateways, network traffic analysis tools and cloud workload protection platforms. These systems integrate primarily through open APIs. They work best when the connected technologies have APIs that are robust, mature, well-documented and modern — for example, streaming rather than traditional REST APIs. What’s even better is when a vendor provides direct integrations based on open APIs for all the security systems a business needs to deploy its chosen XDR implementation.

Because open XDR requires deep integration across multiple vendors’ systems, XDR providers and other participants in XDR ecosystems are now coming together in alliances to define and evolve XDR data sharing standards, architectures, APIs, languages, workflows, playbooks and best practices. Mimecast believes these alliances offer significant promise, and already participates in those organized by Exabeam and the XDR Alliance, CrowdStrike and BlackBerry, respectively. At the same time, we recognize that it will take time for these initiatives to bear fruit. We recommend that, wherever possible, organizations look for robust APIs and integrations that already exist — both on the XDR platforms themselves and on the systems they connect with.

What Can You Do Now?

While some analysts expect that it will be at least three years before XDR systems can fully replace prior platforms such as SIEMs, now is the time to start assessing XDR's potential value in your organization. As you evaluate this, you can take steps that increase your chances of long-term success whether you eventually adopt XDR or not. For example:

Focus on integration.

Plan any upcoming security product/service purchases, retirements and vendor consolidation to align with XDR strategy. XDR makes deep integration crucial, so whatever systems you purchase or keep should support easy integration, particularly via open APIs. Deploy an advanced secure email gateway that empowers you to easily interoperate with XDRs, SIEMs, SOARs, SASEs, or other enterprise security systems (e.g., open comprehensive and modern API libraries; streaming APIs, etc.).

Don't overlook the complexities of investigation.

Because protection against threats also involve triage and investigation of threats detected, privilege XDR approaches that use the machine to accelerate all the phases of the threat detection, investigation and response (TDIR), not only detection and response.

Carefully assess vendor roadmaps.

Thoroughly evaluate the current state of any XDR product you're considering, its roadmap and the provider's ability to deliver on that roadmap.

Remember the key role of response.

Because XDR extends point solutions such as EDR or NDR to include other inputs, it's often discussed in terms of its inputs and the analytics based on these. Inputs and analytics are obviously important, but so is XDR's ability to automate and streamline responses. This means your secure email gateway and other linked systems should support the widest range of response actions possible via comprehensive open APIs that expose virtually all of their functionality.

Eliminate organizational siloes.

XDR and other enterprise security platforms will deliver more value if your people can easily work together and your processes facilitate collaboration across all functions involved in cybersecurity; across all security controls, and between SecOps and IT.

Compare "proprietary" vs. "open" XDR. Clearly understand tradeoffs associated with proprietary and open XDR systems, especially the dangers and costs of a single-vendor security monoculture.

Recognize XDR's current limitations. Most XDR systems don't yet solve important compliance and archiving problems traditionally addressed with SIEMs. At least in the short-to-medium-term, some organizations will run SIEMs and XDR systems together, with SIEMs feeding data to XDRs as the newer systems take charge of threat management.

Evaluate MITRE ATT&CK support. Consider how XDR offerings do (or don't) facilitate threat management and hunting with the important MITRE ATT&CK framework for understanding and responding to adversary behavior throughout the attack lifecycle.

XDR™ Alliance

mimecast

ExtraHop

Recorded Future

Google Cloud

netskope

SentinelOne

exabeam

CYBERARK®

ARMIS

expel

mimecast™

Get More Insight for Planning and Strategy

Drawing on our expertise supporting thousands of customers and integrating with 100+ leading third-party cybersecurity products and services, Mimecast can offer more practical guidance for considering XDRs, SIEMs and enterprise cybersecurity strategy as a whole. We're at your service: just contact your Mimecast representative,
or visit Mimecast's Alliance & API Ecosystem.

For information on how to foster a more open approach to XDR,
visit the XDR Alliance.