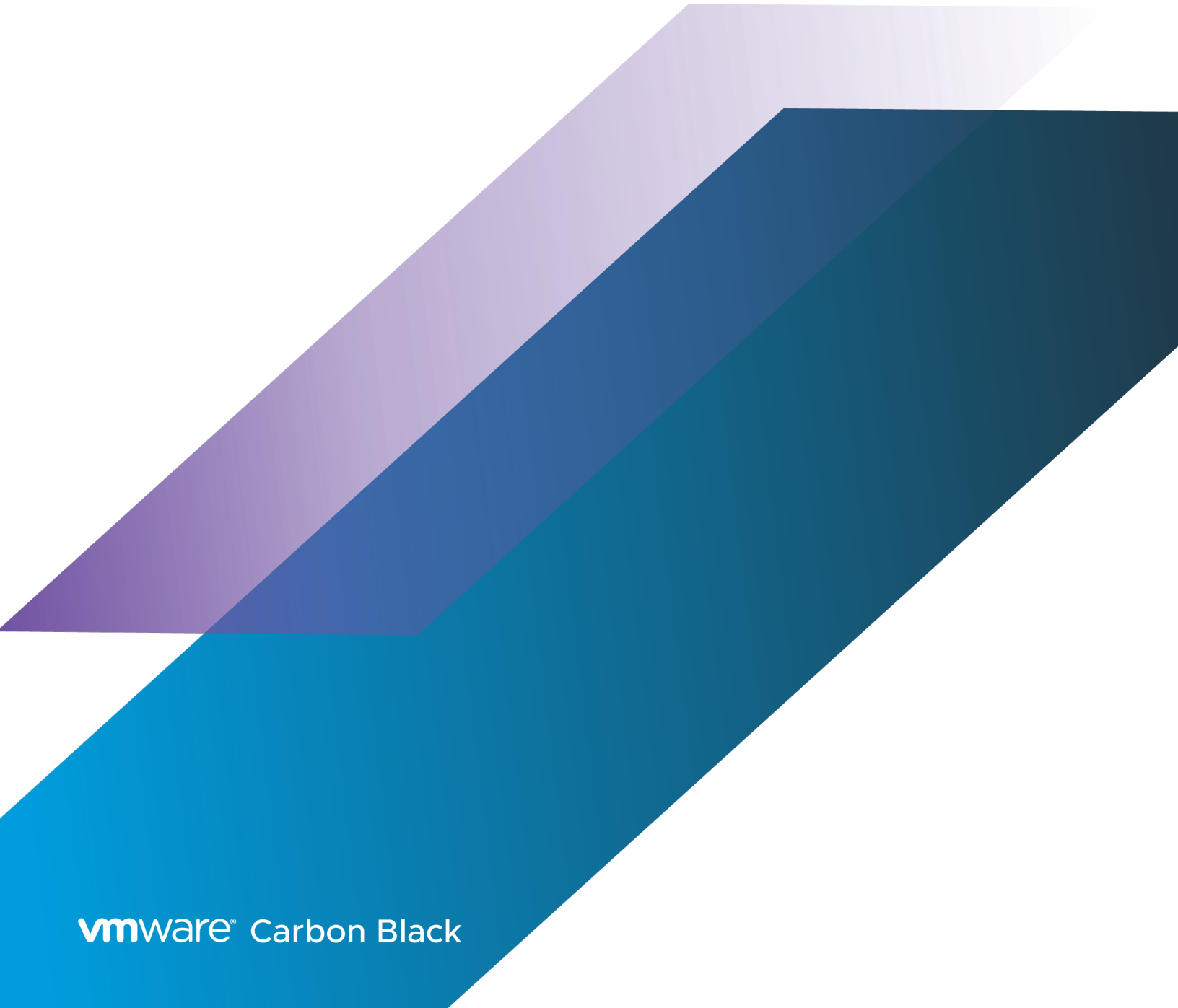
Industry Guide

Redefining the Security Analyst Experience: EDR to XDR

A Comprehensive Security Industry Guide to Extended Detection and Response (XDR)



vmware® Carbon Black

What is XDR?

This VMware Carbon Black Industry Guide provides an overview of the design principle known as "XDR."

XDR refers to eXtended Detection and Response, which is a cybersecurity toolset more rapidly and accurately detects and responds to attempted cyber attacks. The building blocks of effective XDR include Endpoint Detection & Response (EDR), Network Detection & Response (NDR), plus Detection & Response across the multi-cloud operating environment, and modern applications (including container-based applications). XDR may also include user and system authentication and session authorization information, email & messaging system security state data, and log events collected by SIEMs.

What does this guide offer?

Readers of this guide can expect to learn:

- An overview of how XDR can improve the efficiency and effectiveness of a security team or Security Operations Center (SOC);
- A general overview of the core elements to be considered in XDR;
- Recommendations for organizations to achieve a modernized SOC environment that balances evolving risk reduction and management of change over time.

This document is intended for readers from a business background with moderate knowledge of cyber and technical terms and concepts and does not require highly technical information technology or cybersecurity skills and knowledge.

This Industry Guide does not recommend specific VMware Carbon Black technology or services and readers should refer to other documentation and to VMware Carbon Black experts for details on how to best architect and configure VMware Carbon Black solutions. Please see "Additional Resources" in this guide for a list of recommended documentation and information assets.

Table of Contents

Introduction

From EDR to XDR

July of 2013 saw Anton Chuvakin of Gartner coin the term endpoint threat detection and response, later shortened to endpoint detection and response (EDR).[1] With his insight, Anton christened an industry wide evolution to a select but burgeoning set of industry software tools, and signaled that traditional endpoint protection platforms had outlived their usefulness.

EDR was seen by Gartner as offering the promise of detecting and investigating suspicious behavior and activities on hosts and endpoints. EDR was an important new solution that defenders of corporate environments could use to better defend themselves from cyberattacks.

The EDR sector began a rapid (and still growing) one as security operations centers (SOCs) added the toolset to provide additional telemetry to feed into their security information and event management (SIEM) platforms. Today, along with the SIEM, EDR is regarded as a bedrock of any SOC, and whether an organization chooses to operate EDR as an in-sourced solution or consume it as a managed service, few organizations would downplay the significant benefits it offers to security visibility.

Threat actors find inroads

Meanwhile, our cyber adversaries have continued to evolve and adapt. Threat actors are motivated by financial, geo-political, and ideological goals and have continued to demonstrate new and novel ways to attack, exploiting the rapidly expanding range of information systems and applications that power the modern economy.

Despite best efforts by defenders, and the tremendous value and capabilities of EDR, and other security detective and preventative tools in use, threat actors are finding ways to slip through undetected, and remain in our critical systems. Just as EDR was developed to allow defenders to see deep into the inner workings of an endpoint (and server), defenders now require visibility across other elements to better secure their environments.

How does XDR differ from EDR?

EDR gives sight of the breadcrumbs left by attackers in the endpoint, while XDR gives sight of the breadcrumbs left as attacks traverse (or move laterally) across the network, communicate from the network to the internet, and probe for weaknesses in corporate systems including email, applications, and virtual identities.

XDR builds on the capabilities and techniques of EDR; deep and broad telemetry data capture, AI/ML analytics across the data set assisted by human intelligence, and extends (the ‘X’ in XDR) telemetry capture to the network, container-based workload, cloud, email, and identity realms. XDR rebalances the equation in favor of the defenders and provides the SOC the means to see more and stop more attacks.

XDR and the modern security team

Organizations both large and small require the means to rapidly identify attacks, protect their environments, detect threats efficiently, respond rapidly, and recover when necessary. These basic five functions are defined by the United States National Institute of Standards and Technology in their "Cyber Security Framework 1.1."[2]

Depending on an organization's approach to cybersecurity, a security team or SOC functions may be operated internally by a dedicated team or consumed as a managed service from a specialist managed security services provider (MSSP) or managed detection and response (MDR) vendor.

Regardless of the operational delivery model, top security teams will generally rely on a ubiquitous set of tools; an SIEM, a security orchestration and automated response (SOAR) platform, threat intelligence (TI) feeds, EDR, and specialist tools to monitor and manage specific aspects of the computing environment including vulnerability management, corporate email and messaging systems, applications, the cloud environment, user access, and security controls such as firewalls.[3]

SOC and NOC strengths—and shortcomings

Historically one critical element of the computing environment, the network, was not generally monitored directly by the SOC. While this may seem to be an unbelievable oversight (no pun intended), the reality is that this approach reflected the fact that the health of the network was so critical that it required the specialist to focus on a dedicated team. That dedicated team was to be found in the network operations center (NOC), tasked with ensuring the availability and health of the network glue that ties everything together.

An underlying assumption to this approach was that when the SOC teams needed information about network traffic patterns, they could call upon the cooperation of their NOC brethren. Similarly, when the NOC teams required assistance to diagnose behavior of an endpoint or application that was exhibiting activity deleterious to the overall performance and stability of the network, they could call open the SOC.

While this model worked in principle, over time it has proven unreliable, leading to operational inefficiencies and blind spots. Adversaries have taken advantage of this to gain an initial foothold and then move laterally across the network from machine to machine, workload to workload, as they further their attack towards its ultimate goal.[4]

Furthermore, the operational inefficiencies inherent when multiple teams must collaborate in high-pressure working environments characteristic of a SOC or NOC leads to team member stress and burnout.[5]

XDR offers efficiency, visibility, and context

By integrating EDR and network detection and response (NDR) with the ability to ingest even more data, and perform AI/ML-based analytics, XDR offers a pathway to a more efficient, modernized security team; a security team that can see more, detect faster, respond with confidence, and ultimately stop more attacks.

XDR removes the requirement to pivot between contextual frameworks as information is presented in a single place, and the various elements of telemetry (the breadcrumbs left behind by the attacker) are automatically woven together to provide a cohesive view of the emerging threat.

Developing an Effective Strategy to Modernize Security Teams

Key considerations

Effective security involves balancing the three legs of "the security triad;" people, process, and technology. Added to that is a fourth dimension—budget. Organizations are of course budget restrained to one degree or another, and must balance cybersecurity investment with the degree of risk acceptable to the business and the needs of other competing investment priorities.

The concept of the security triad recognizes that we must have adequate skills (people) available to design, implement, and operate security solutions. Such skills may be on the payroll as full-time employees (FTEs), contractors, or sourced from external managed service providers. The triad also recognizes that outcomes are more predictable and repeatable when pre-planned and tested procedures (processes) are followed. Lastly, the triad recognizes that cybersecurity involves software and hardware tools (technology).

People matter

While the legs of the triad are equal, people are generally regarded as paramount. Without skilled people to follow and improve processes, or to operate the technology, we have nothing. Unfortunately, we have a global shortage of cyber skills, and the people we do have are reporting high levels of job-related stress and burnout. Not only are there not enough people and skills, but organizations also run the real risk of trusted employees abandoning their posts simply to better look after themselves.[6]

While contributing factors of burnout are varied, it is recognized that a poor analyst experience is a significant contributing factor. Whenever an analyst must argue priorities with NOC personnel, pivot between contexts as they move from one console and user interface to another, and attempt to translate the language and data presented in one tool with the different vocabulary of another tool, stress levels are bound to rise.

Furthermore, there are only so many hours in a day, and only so many alerts an analyst can investigate. Time wasted investigating a false alarm (termed a "false positive") is a futile effort, where an analyst invests time gathering information and investigating before ultimately concluding there is no threat.

Meanwhile SOCs exist, processes have been built, tested, and proven, and money has been invested in technologies and tools. Therefore, a critical consideration is that as XDR is deployed, it supports the ecosystem of tools already in place. A "rip and replace" approach is not a budget-effective option.

The security analyst experience

Considering the alarming levels of stress and burnout reported by frontline cyber defenders, a high priority needs to be placed on improving the security analyst experience by focusing on a handful of key areas.

Reduce false positives. It is imperative that false positive rates are reduced to an absolute minimum, an outcome which is best achieved through a combination of:

- Capturing of a deep and broad set of telemetry from across the cybersecurity spectrum which provides data about endpoint, server, and network activity. Telemetry capture is generally a native capability of EDR, NDR, and XDR tools, paired with unique selection criteria;
- Telemetry analytics leveraging artificial intelligence and machine learning models, informed through threat intelligence and research by human experts. Outside of specific cases, analytic interpretation of telemetry data is usually performed in the cloud to provide computing for machine learning and data storage at scale and in a cost-effective manner;
- Careful tuning of policy to cater to those unique aspects of any given organization's environment. It is critical to avoid policy settings in SOC tools that disregard true positives. In other words, do not set the bar for alerting so high that the figurative fire alarm does not ring even when the building is burning down.

Minimizing the false positive rate will limit the time security analysts spend investigating a non-threat. Conversely the mean time to detect (MTTD) and mean time to respond (MTTR) metrics improve as confidence improves thanks to improved telemetry and the reduced false positive rate. MTTD and MTTR are key SOC performance metrics and are directly linked to the ability to reduce the business risk of an attempted cyberattack.

Use preferred tools. Stress levels rise when analysts are forced by technology to perform aspects of their job using tools unfamiliar to them. When moving through the investigation workflow (review data, triage, classify, investigate, respond), analysts prefer to use the console they are most familiar with. Of course, there are occasions when an aspect of the workflow will require the use of more than one console, but the goal should be to provide a simplified workflow experience.

XDR contributes to this goal in three significant ways:

1. Combining endpoint telemetry data (EDR) with network telemetry data, natively correlated in the right context with naturally aligned timestamping to create a simple to investigate incident trail.
2. Integrating endpoint and network telemetry with other tools the security analyst may use (for example, the SIEM platform).
3. Effectively respond to detections in a variety of ways. Common response actions include: banning file hashes (a means to 'fingerprint' a specific file), next-generation antivirus (NGAV), managing host-based firewall (HBFW) policy, quarantining a device from the network, remotely issuing commands and queries to a device, and interacting with the SOC ecosystem of tools via two-way APIs.

Automate. Automation eliminates (or at least minimizes) the burden of repetitive tasks, while also ensuring consistent outcomes. Assisted by automation, less experienced analysts may also be able to perform more

efficiently, thereby uplifting overall team productivity. Security orchestration, automation and response (SOAR) platforms are often used in an SOC environment to centralize automation. Automation should also be distributed and performed as close as possible to the telemetry analytics source. This approach will eliminate the hair-pinning of security data and decision-making back to the centralized SOAR platform, which risks introducing unnecessary overhead in a hybrid working and/or cloud-native environment.

The evolving network battleground

The tools traditionally used by NOC teams generally relied on hardware-based add-ons to the network. In effect, network flight recorders tapped the network at key traffic control and traffic chokepoints and reported back important diagnostic data.

Unfortunately, such approaches have limitations, chief of which is that as workloads move from the datacenter to the cloud, the network is software-defined and boundaryless. Applications are often cloud-native and SaaS in architecture, while employees are now spread out across home offices, remote and branch offices, connecting to the network, anywhere at any time.

In such an environment there is often no physical network to be tapped. Effective and scalable monitoring of the network from a security point of view, relies on going where the endpoints and workloads are.

Key considerations for effective XDR

XDR therefore must solve for the following key considerations:

- Help reduce security analyst burnout;
- Improve the security analyst experience and improve operational confidence;
- Support the existing ecosystem of tools;
- Slot neatly into the existing ecosystem of SOC tools and the process workflows, and extend their effectiveness;
- Reduce operational friction;
- Reduce time to detect and time to respond by allowing the security analyst to see more across the security spectrum, and stop more attacks; and
- Go where the endpoints and workloads go without requiring expensive, hardware-based network taps.

XDR helps close the Risk Gap

Traditional "status quo" solutions tend to lack full visibility across multiple security layers, which security teams need to detect and respond to threats throughout their environment.

This is the Risk Gap—the growing distance between an organization's status quo defenses and its exposure to directed attacks and the associated burden of meeting compliance and governance requirements. By unifying security tools to enable pervasive visibility, the right XDR solution delivers the comprehensive context necessary to know what's happening and to stop attacks before they move laterally.

How does a security team close the Risk Gap?

- **Tailor detection and response to unique business needs.** This is granular customization based on organizational policies, vulnerabilities, integrations and intelligence.
- **Acquire deep context on the data that matters, leading to better evidence.** This will allow analysts to more rapidly detect and investigate incidents, while providing complete auditable visibility.
- **Deploy high enforcement everywhere it makes sense.** Consider introducing a positive security model featuring a default/deny approach. This leads to tight control and governance and a trusted environment, generating less noise that can overwhelm and distract SecOps teams.
- **Engage a force multiplier for security teams.** Deploy the right solution so teams will know what's working. Enrich existing workflows with better data and open APIs to help surface the incidents and conditions that really need attention and achieve data-driven control.
- **Get proactive.** A proactive, layered approach to cybersecurity allows teams to make better decisions faster.

This is not impossible to achieve. And focusing on XDR provides an ideal first step in that journey.

Summary and Additional Resources

Today, organizations can no longer assume that SIEM/SOAR tools and EDR are enough to rapidly detect and respond to cyber adversaries.

Attackers continue to evolve and recognize the operational blind spots created by a lack of security visibility, allowing them free reign to move laterally across networks. Meanwhile, the Risk Gap continues to widen in many organizations.

Recognizing that security teams already rely on trusted third-party tools including SIEM, SOAR, and other security controls, a cost effective and sensible approach to XDR is one that supports the integration of preferred toolsets and protects existing security investments.

XDR is the bedrock of capability

The evolved SOC thus relies on XDR as a bedrock of capability, empowering security analysts to see and stop more attacks, drive data-driven decisions faster, smooth out workflow inefficiencies, reduce stress, and execute with precision. Organizations can harness security resilience and navigate the future with confidence, ultimately ushering in an era where security analysts feel supported, capable, and secure. As risk continues to rise, so does the need for a modernized SOC and security analyst experience—and XDR is the first step in that evolution.

Additional resources

Brief: How to Make Sense of XDR
https://content.carbonblack.com/products/c/make-sense-xdr

VMware Carbon Black XDR:
https://www.vmware.com/solutions/xdr-security.html

Implementation Best Practices for XDR:
https://carbonblack.vmware.com/carbon-black-xdr-activity-path

Other VMware Carbon Black industry and solution guides

VMware Industry Guide: Securing Modern Applications:
https://carbonblack.vmware.com/resource/securing-modern-applications-industry-guide

VMware Industry Guide: Ransomware Protection:
https://carbonblack.vmware.com/resource/ransomware-protection-vmware-security-solutions-guide

VMware Solution Guide: Security Multi-Cloud:
https://carbonblack.vmware.com/resource/securing-multi-cloud-solution-guide

Appendices

Changelog

The following updates were made to this guide:

Date	Description of Changes
January 2023	• Initial publication.
October 2023	• Updated for accuracy and new resources.

Feedback

Your feedback is valuable.

To comment on this paper, contact VMware Carbon Black Technical Marketing
techzone-sbu@vmware.com

Citations

[1] https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/
[2] The Information Technology Laboratory (ITL) at the USA's National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. NIST standards are mandated in some U.S. industry sectors, and are highly regarded as defining best practice globally. Refer to https://www.nist.gov/cyberframework/online-learning/five-functions.
[3] SIEMs are generally used an aggregator of security and non-security related log based information. SOAR platforms as a means of automating repetitive tasks related to information gathering, reporting, and response efforts. TI provides valuable intelligence regarding emerging threats, often specifically related to the industry sector the organization operates within.
[4] The goal of an attack will vary depending on the specific adversary, and includes espionage, financial gain, disruption to IT and physical systems, manipulation of data to sow confusion, and denial of access to information and applications.
[5] https://blogs.vmware.com/security/2021/08/combating-cybersecurity-burnout-through-self-care-empathy-and-empowerment.html and https://blogs.vmware.com/security/2022/04/how-not-to-build-a-soc.html
[6] https://blogs.vmware.com/security/2021/08/combating-cybersecurity-burnout-through-self-care-empathy-and-empowerment.html

VMware Carbon Black

VMware Carbon Black empowers top security teams to close the Risk Gap they face today. Specific directed attacks are now the cybercrime norm, and no business is exempt. There's increasing cyber-insurance scrutiny, and government regulations continue to get stricter. In this context, security teams can no longer rely on general security platforms alone. Rather, teams must be empowered with deeper visibility and more control to tailor response to their unique environment. With Carbon Black, security teams have unprecedented ability to see directed attacks, contain potential impact, change policies with no user interruption, prevent repeat incidents, and measure what they stopped.

vmware® Carbon Black