The Future-Ready SOC
Using XDR to achieve unified visibility and control
Table of contents

Persistent and costly challenges facing CIOs and CISOs .................. 3
The flaws with siloed detection and investigations ......................... 4
Investigations require fuller and richer context .......................... 4
Intrinsic security evolves threat detection, investigation and response  .................. 6
  Extended visibility provides more complete investigation timelines  6
The value of unified telemetry and enforcement .......................... 7
  XDR-enabled, accelerated phishing protection .......................... 7
The future-ready SOC is here ................................................. 8
“VMware is in a unique position to enhance Gartner’s vision of XDR ‘as a unified security incident detection and response platform that collects and correlates data from multiple proprietary security components’ by also offering our customers the ability to consolidate, simplify and accelerate their defenses.”

TOM CORN
SVP, SECURITY BUSINESS UNIT
VMWARE

KEY FEATURES OF XDR FROM VMWARE
- Extends endpoint detection and response (EDR) and network detection and response (NDR) telemetry and enforcement from and to all domains
- Offers native support for cross-domain behavior analysis, threat intelligence, behavior profiling and analytics
- Optimizes incident response, providing surgical precision for threat detection, investigation and containment activities
- Enables operational scalability via more cohesive and automated workflows across your extended enterprise

CIOs and CISOs of globally distributed enterprises face an enormous challenge: how to scale operations to meet the pace of escalating threats while IT and security team members are distributed and rely on a web of disconnected and disparate tools to do their work.

The technology and procedural silos that exist between IT and security operations center (SOC) team members have impeded an enterprise’s ability to effectively mitigate risk. Until and unless this chasm is crossed, SOC teams and their IT counterparts will never achieve their goals. An overwhelmed, distributed workforce and increasing attacker dwell times have raised the stakes for the CIO and CISO. Reducing mean time to resolution (MTTR) is a critical goal because the faster an incident is detected, investigated and resolved, the more likely it will result in a good business outcome. Two critical success factors hold the key to preparing for the future-ready SOC: automation and the cloud.

By unifying detection and response activities across IT and security domains and devices, VMware Carbon Black Cloud™ delivers the essential foundation for XDR (Extended Detection and Response) and takes it even further. VMware Carbon Black Cloud uniquely acts as XDR-ready infrastructure and offers native support for automated, cross-domain, XDR-enabled controls that deliver built-in, context-centric, unified security.

Persistent and costly challenges facing CIOs and CISOs
In their pursuit to secure applications and data, enterprise CIOs and CISOs have invested in technologies and workflows that provide visibility and control into the most critical access points in an organization: user, endpoint, workload, cloud and network. Implemented in the right way, these “camera angles” offer the necessary telemetry to spot trouble and shut it down. The challenge is that these technologies are set up and managed in silos, leaving teams without the big picture view and allowing attackers to hop across each channel undetected—increasing risks as well as costs.

The flaws with siloed detection and investigations
The innovation, speed and adaptability cyberattackers have demonstrated over the past several years requires that teams rethink their detection and investigation efforts. When attackers use legitimate software in malicious ways, it’s no longer sufficient to use threat signatures to detect the presence of known bad software (e.g., using PowerShell to scrape LSASS servers for credentials). Plus, in one-third of attacks, attackers move laterally across the network, with 40 percent of these attacks spreading destructive malware in the process.1 While EDR and NDR have significantly enhanced detection of these kinds of threats, these solutions continue to lack the contextual awareness necessary to drive down the time to resolution.

I now have the ability for a 24x7 SOC to immediately identify and take action on any issues that come up without needing to reach out to my team at all hours of the day/night.”

CODY LAVALLEE
IT INFRASTRUCTURE MANAGER
PROGRESS RESIDENTIAL

PRE-XDR QUARANTINE USE CASE

- Endpoint security product identifies an infected machine and auto-blocks all network communications (other than to patch the server).
- Once patched, it’s allowed to reconnect.
- Upside: Works well for user machines (fully contained systems).
- Downside: Not appropriate for app servers or shared systems where a fail-safe is unacceptable for business operations.

POST-XDR QUARANTINE USE CASE

- Endpoint security product identifies an infected machine and auto-blocks risky network communications based on analysis from adjacent controls.
- Telemetry from XDR-enabled controls beyond the endpoint allows for more granular enforcement and surgical threat mitigation.
- For example: Apply quarantine controls to the specific workload or guest OS that’s impacted, and allow all other connections and processes.

Investigations require fuller and richer context

When attackers target organizations, they don’t restrict their activities to specific channels or domains. Rather, they employ a variety of different methods and tools at different stages across the MITRE ATT&CK framework. That’s why it’s essential for incident responders to have visibility into the entire attack campaign, including all the machines that have been affected, how the attacker got in, what they changed, and where they left persistence mechanisms (i.e., backdoors). To do investigations effectively, teams need to:

1. Search across the environment (e.g., show me everywhere we’ve seen this kind of activity)
2. Search backward and forward in time (e.g., rewind the cameras and show me what has led up to that activity, and what’s happened since).

The key to be able to do this is having access to all the data about all the activity and being able to connect the dots along the timeline in a way that’s actionable as well as complete.

<table>
<thead>
<tr>
<th>CHALLENGES OF THREAT DETECTION, INVESTIGATION AND RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The analytics challenge</td>
</tr>
<tr>
<td>The data challenge</td>
</tr>
<tr>
<td>The domain challenge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TIME AND SPACE CONSTRAINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The time challenge: Acting quickly is the difference between dealing with infiltration or dealing with exfiltration. With talent shortages and budget crunches, doing more with less is a must.</td>
</tr>
<tr>
<td>The way forward: Automation</td>
</tr>
</tbody>
</table>

The distributed environment challenge: IT and SOC teams are more distributed than ever before, with most detection, investigation and response activities happening outside of enterprise infrastructure.

The way forward: Cloud analytics
Once the full attack campaign is understood, these critical steps come next:

1. Contain the threat – Inhibit the attacker from moving into any other systems, cleaning the tracks, or exfiltrating any data.
2. Clean the environment – Remove and disarm any command and control systems and connections.
3. Inoculate systematically – After removing any command and control systems, we need to alter our hardening and prevention policies so this can never happen again. There is no value hunting the same threat more than once.

While traditional EDR does this today for endpoints and workloads, being able to respond across domains brings tremendous time and cost advantages.

VMware Carbon Black Cloud provides the essential foundation for enterprise XDR initiatives. By consolidating and correlating cross-domain telemetry and enforcement data onto a single platform, our approach speeds and simplifies incident response at scale. Rather than trying to architect the right data flows among disparate technologies, VMware customers and partners are already equipped with XDR-ready architecture where each component already shares a common dataset optimized for this purpose.

VMware Carbon Black Cloud offers globally distributed teams the fastest and most cost-effective way to gain the benefits of XDR without the overhead. Alternative XDR solutions offer productivity benefits, but they come at a cost. Other vendors offering XDR solutions leave their customers with the significant compute costs of building and maintaining the data lake required for XDR use cases (note: data storage and analytical processing costs are just the starting point). With VMware, customers and partners realize all the XDR benefits, without the overhead.
The Future-Ready SOC

“VMware solutions with intrinsic security will allow us to deploy faster, reduce costs, use less space and better protect our members’ personal and financial information.”

MARK FORNIER
INTERIM CIO
UNITED STATES SENATE FEDERAL CREDIT UNION

U.S. SENATE FEDERAL CREDIT UNION CASE STUDY

• Reduced data center costs by 70 percent
• Intrinsic security components:
  – VMware Carbon Black
  – VMware NSX
  – VMware AppDefense™
  – VMware vSAN™
  – VMware vSphere®
  – VMware Workspace ONE
  – VMware Horizon
• Improved employee and customer satisfaction
• Reduced end-user computing support costs by 66 percent

Intrinsic security evolves threat detection, investigation and response

Gaining as many insights as quickly as possible from threat detection data is the goal because it allows teams to adapt defenses as an attacker’s techniques adjust. Consider the value of combining EDR telemetry data with workload and NDR telemetry data. A network anomaly detection tool might detect a new or suspicious connection between two workloads but is blind to what’s happening within that workload. With kernel-level visibility into the workload and the endpoint, you can make more informed decisions faster, without putting availability at risk.

Extended visibility provides more complete investigation timelines

Manually combining artifacts from disparate consoles into a single timeline slows down investigations, giving attackers more time to wreak havoc in an enterprise environment. VMware Carbon Black Cloud accelerates investigations by serving as the core XDR platform for unified timelines and orchestrated workflows.

<table>
<thead>
<tr>
<th>TEAM</th>
<th>XDR USE CASE EXAMPLE</th>
<th>BENEFITS</th>
</tr>
</thead>
</table>
| IT Security/SOC       | Surgical threat hunting – With telemetry from NSX feeding VMware Carbon Black® Cloud Enterprise EDR™, threat hunters are armed with high-fidelity intel to track and disrupt island-hopping activity far earlier in the attack timeline—before an intruder can leak sensitive information or gain access to a high-value asset or set of credentials. | • Reduced dwell times with less staff involvement  
                          |                                                                                       | • Faster, more accurate incident response      |
| Network Operations    | All of the IT and security domains (aka camera angles) are essential. Like CCTV systems, zooming in, out and across are required. Analysts need access to every control point (users, workloads, cloud, endpoints and networks), a way to share these angles, and access to their IT peers in other domains, along with a unified way of seeing it all at once. | • Reduced MTTR  
                          |                                                                                       | • Increased uptime  
                          |                                                                                       | • Improved service levels with fewer resources |
The Future-Ready SOC

The value of unified telemetry and enforcement

Today’s cyberattacks are successful because an attacker’s activity is hidden between the cracks of IT and IT security technology silos and workflows. When no one in the enterprise can see the big picture or make a data-driven enforcement decision, the attackers continue to persist in breaching our defenses. VMware’s intrinsic security approach offers the best way to meet these challenges at scale.

XDR-enabled, accelerated phishing protection

Imagine a phishing attack with XDR in place. After the user clicks on the bad link or attachment, VMware Carbon Black Cloud identifies the malicious code installed on the endpoint and correlates it with outbound network connections to a command-and-control server flagged by NSX, and ties this to subsequent suspicious activity on a domain controller (e.g., credential theft). Rather than trigger alerts on each of these disparate systems to be followed up later by different team members, one single view shows the full attack across each domain for rapid response. Plus, each team member is empowered to act from a common system of record.

| Infrastructure Operations | Secure critical workloads—Protect mission-critical workloads with kernel-level granularity across your vSphere environment thanks to native integration with VMware Carbon Black Cloud. Detect and contain threats within workloads and avoid impacting operations while also reducing risk at the source. | • Reduced attack surface
• Kernel-level visibility from a single agent
• Simplified operations |
| --- | --- | --- |
| DevOps | Reduce risk pre-deployment—Mitigate risks before deployment with granular visibility into insecure, vulnerable and misconfigured containers. Leverage the tight integration with VMware Cloud Foundation™ and VMware Tanzu™ to understand how containers are connected, and the risks they pose to build and apply prevention policies at scale. | • Increased visibility into container security
• Optimized vulnerability and risk mitigation |
| End-user services/help desk | Secure-by-design VDI Environments - Integrating VMware Workspace One, Horizon, and NSX with Carbon Black Cloud enables staff to simplify and streamline workspace management and security—no matter how large the virtual desktop environment or how distributed the team. | • Standardized, secure desktop configurations at scale
• More automated workflows |
The Future-Ready SOC

The future-ready SOC is here

While nothing is certain, the likelihood that IT and security teams will continue to be distributed across geographies and time zones remains high. Staying coordinated is a critical success factor under these conditions. In fact, more than 60 percent of IT and security respondents in a recent survey said that establishing a consolidated strategy with unified metrics and goals is one of their top collaboration initiatives.²

Using VMware Carbon Black Cloud as their XDR platform offers these teams a purpose-built, common system of record, powered by cloud-based automation—all the necessary ingredients for the future-ready SOC.

For more information on cloud computing and VMware vCloud® powered services, please visit cloud.vmware.com or contact your VMware representative.

---
