


McAfee MVISION XDR

The first proactive, data-aware, and open extended detection and response solution designed to help organizations stop sophisticated attacks.

Security Operations Realities

The Security Operations Center (SOC) is a core function in an organization's cybersecurity charter. Its key focus is to quickly find and resolve threats to avoid damage to assets and data. If the SOC is struggling, it is likely security outcomes are dubious and organizations are at risk. SOC challenges continue to grow in volume and scale despite increased spending. Three quarters of security professionals say threat detection and response is more difficult today than two years ago according to research firm ESG.¹ So does this mean the adversaries are winning? 

It's fair to say that the SOC function is still maturing. A recent study by SANS² found that only 29% of organizations considering themselves mature or very mature when it comes to threat hunting and only 40% have incident response as part of the SOC function.

59% of organizations have faced a serious cyber incident, however, only 26% say their SOC identified their most significant breach.

(Ernst & Young, 2020)

Connect With Us



SOLUTION BRIEF

Heavy Workloads and Management Complexity in the SOC

In most cases, the SOC is also under-resourced due to the immense cybersecurity skills shortage, and retention is difficult. In addition, the SOC has been deluged with a plethora of siloed tools, adding a level of complexity that hinders the SOC's ability to detect and respond quickly and appropriately. According to ESG,³ 66% of organizations say that threat detection and response effectiveness is limited because it is based on multiple independent point tools.

The implication for the SOC is that the time to detect and respond to threats is taking months, leaving longer dwell times for adversaries to do more damage. What is required is easy visibility and control across all cyber assets, with actionable intelligence to quickly move to threat resolution. The fragmented tool approach needs to integrate and streamline across endpoints, the network, the cloud, and applications to remove complexity. Alert fatigue needs to be alleviated with automated detection and analysis that prioritizes and distills threats. SOCs need to be empowered with smart and efficient detect, investigate, and respond capabilities to preempt attacks or resolve them before significant damage occurs.

Improve SOC Efficiency and Productivity

McAfee® MVISION XDR is the answer to these SOC challenges and operational inefficiencies. It uniquely expands extended detection and response (XDR) capabilities as cloud-based advanced threat management across the entire IT infrastructure by adding distinct coverage across the complete attack lifecycle, with prioritization to protect what matters and simple steps to orchestrate an efficient response. MVISION XDR mitigates risk from device to cloud, quickly improving SOC effectiveness by decreasing reactive cycles while saving up to 95% on the cost of threat campaign assessment⁴ with the first open, proactive, and data-aware XDR.

Remote attacks by external actors targeting cloud services increased 630% in 2020.

(McAfee, 2020)

SOLUTION BRIEF

Key Benefits

SOCs can do more with MVISION XDR, thanks to a unified view across endpoints, the network, and the cloud. MVISION XDR helps:

- Reduce human error that can result from manually pivoting between tools and data
- Prioritize and protect what matters with data awareness that weighs in criticality and sensitivity
- Minimize risk before and after attacks with proactive actionable intelligence, guided and automated investigations, and prescriptive countermeasures
- Enhance visibility and control, and eliminate tedious manual tasks by effortlessly orchestrating security solutions so they work together
- Deliver actionable cyberthreat management without increasing staff and by empowering current staff

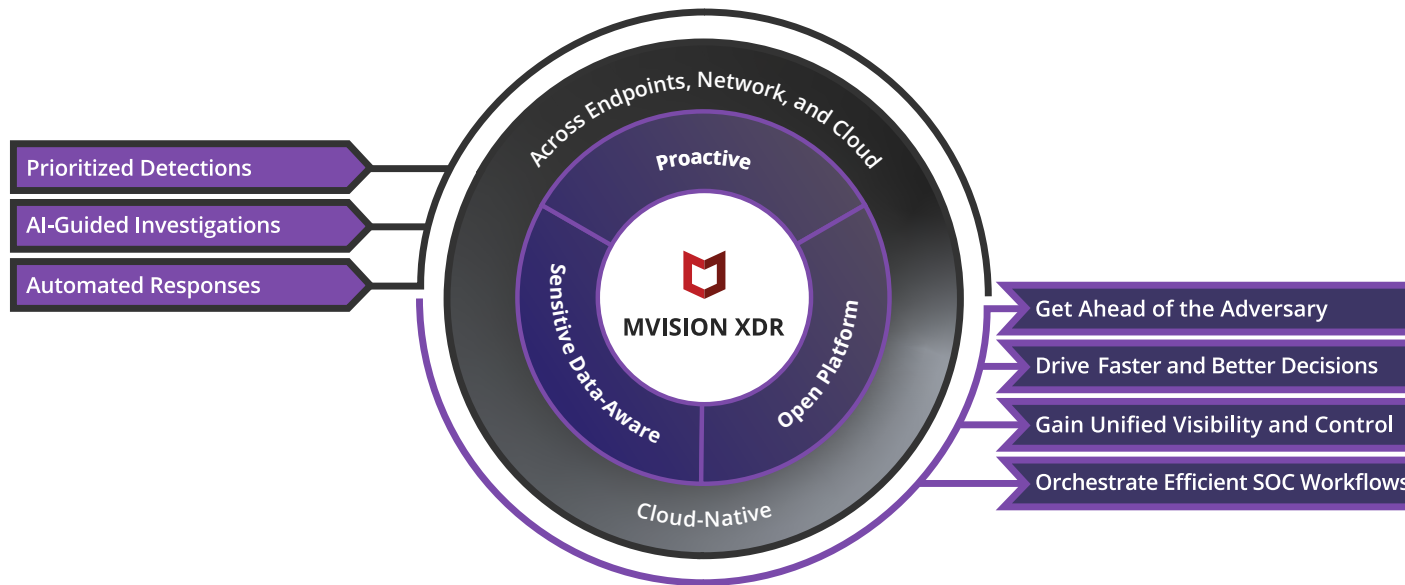


Figure 1. The key advantages and outcomes of MVISION XDR.

SOLUTION BRIEF

Yield Proactive, Actionable Intelligence to Get Ahead of the Adversary

Most XDR solutions only provide capabilities after an attack has entered an organization's environment, creating a highly reactive SOC in constant fire drill mode. MVISION XDR, powered by McAfee MVISION Insights, is the only XDR that addresses the entire attack lifecycle

with stronger reactive workflows after the attack and new proactive capabilities before the attack occurs. SOCs can act on external threats that matter before the attack occurs. Organizations can prioritize threats, predict whether countermeasures will work, and prescribe corrective actions. The outcome is faster detection and response—occurring in minutes rather than weeks.

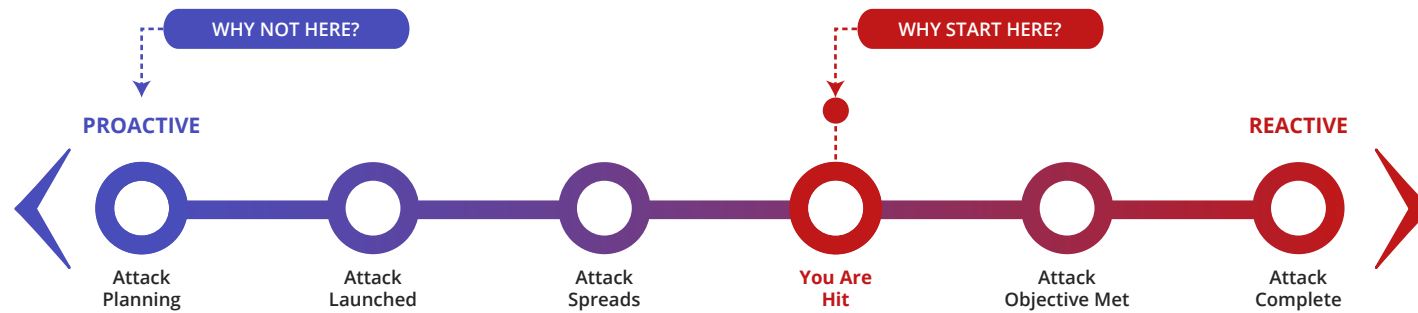


Figure 2. MVISION XDR address the entire attack lifecycle with proactive and reactive capabilities.

SOLUTION BRIEF

Gain Unified Visibility and Control Across Multiple Attack Vectors

The ability to see and connect the dots on the adversary's work across vectors is critical, given how erratic adversary movements can be. More importantly, once the threat situation is apparent, analysts must act across the vectors to resolve the threat.

MVISION XDR combines telemetry from on-premises and cloud sensor grids to seamlessly deliver a holistic view of enterprise data, along with adversarial behaviors.

By converting a large stream of alerts from across the enterprise into a smaller number of incidents, MVISION XDR reduces noise and leads analysts closer to resolution.

From an intuitive dashboard, SOC analysts are provided with key findings related to their environment, trending campaigns, and recommended priorities based on automatic investigative work and analysis.

From this overview, analysts can drill down and easily investigate and assess the necessary actions to take. The response options make affect multiple vectors across the entire enterprise.

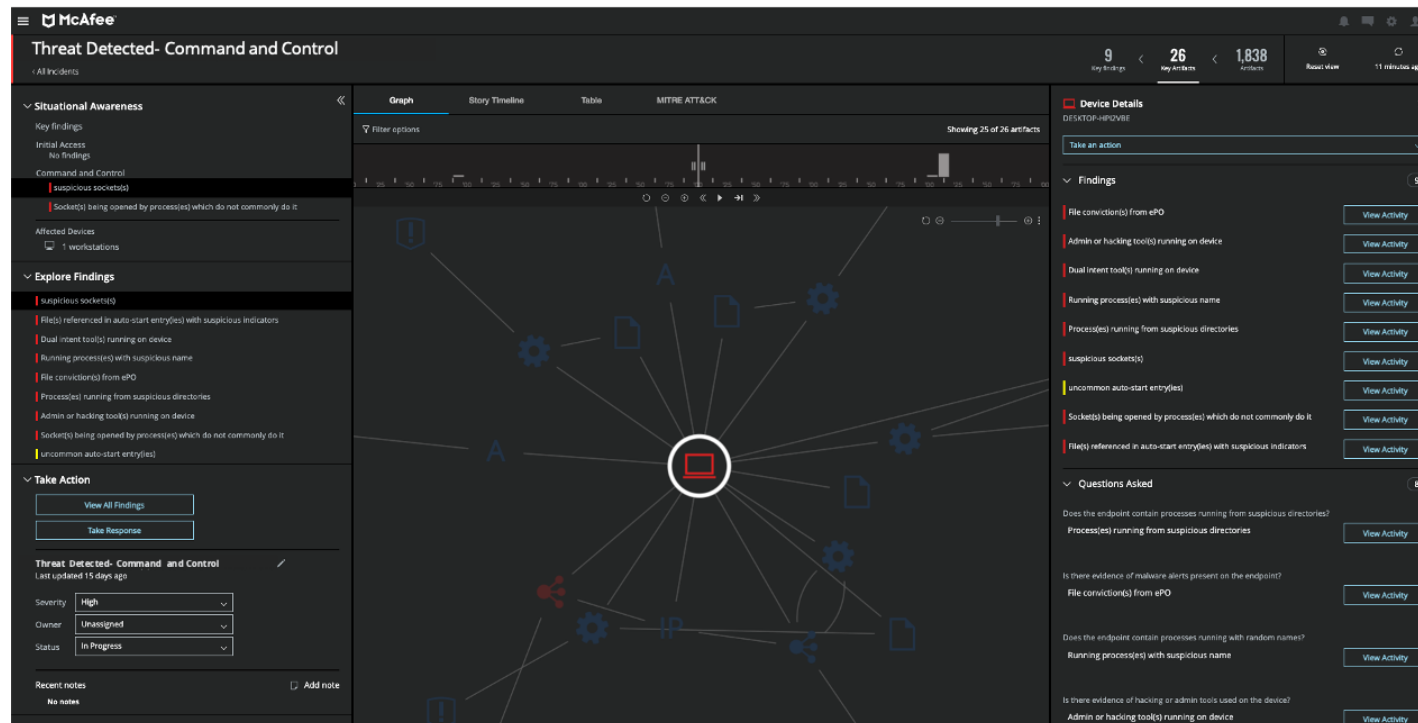


Figure 3. Prioritized incidents with guided, drill-down investigation and response workflows reduces alert overload and speeds resolution.

SOLUTION BRIEF

Drive Faster, Better Decisions

SOCs must reach decisions quickly in order to resolve threats and minimize damage. Steps to faster decisions include accelerating the investigation effort and prioritizing what is critical. MVISION XDR speeds investigations with AI-guided and automatic investigations. AI-guided investigations walk SOC analysts through by automatically asking and answering

questions while gathering, summarizing, and visualizing evidence from multiple sources. This helps SOC analysts continually learn as they fine-tune their investigation and response skills. In addition, automatic investigations derived from proven triage logic may be conducted anytime. Both options eliminate the need to manually gather and analyze evidence. They also remove alert noise and empower analysts to get to a response decision swiftly.

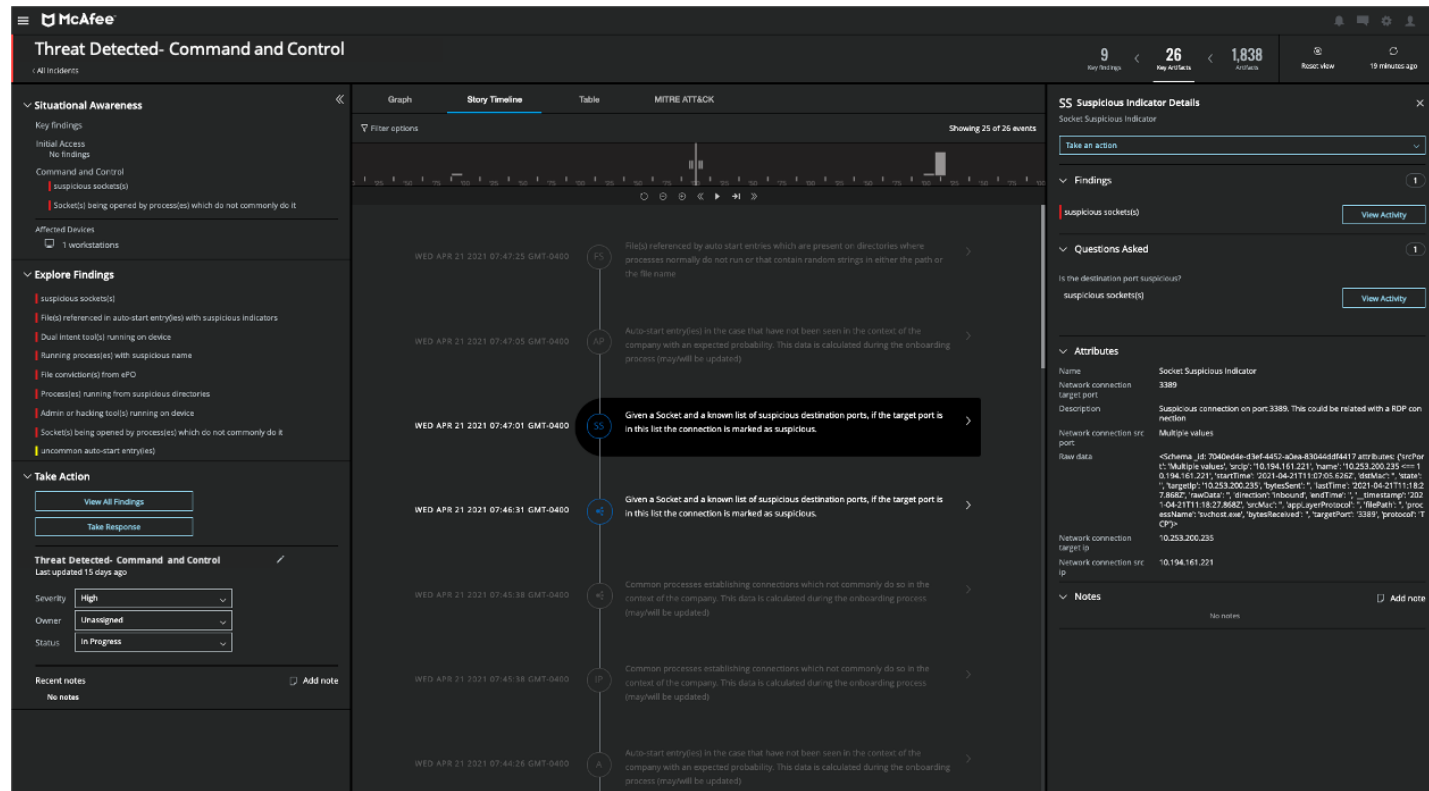


Figure 4. Actionable story timeline provides a detailed look at the events that make up the entire breadth of an attack.

SOLUTION BRIEF

MVISION XDR ingests threat intelligence from a range of sources, such as security information and event management (SIEM) solutions, and offers an easy search on the who and where of the incident or threat. The adversary's story is simply displayed in a timeline with incidents and correlating data and behaviors. Analysts can drill down on findings and evidence to further access the event using their knowledge and intuition. Recommended actions are offered based on previous efforts made by the organization and insights into how others in the same industry responded.

MVISION XDR offers a range of prioritization to rapidly get to a critical decision. Threats and incidents may be prioritized based on the organizational impact such as data loss or damage. A threat that meets certain criteria based on data protection categories, identity, and device type may be set as a higher priority. For example, a financial executive's device storing highly sensitive data that is in jeopardy will take precedence.

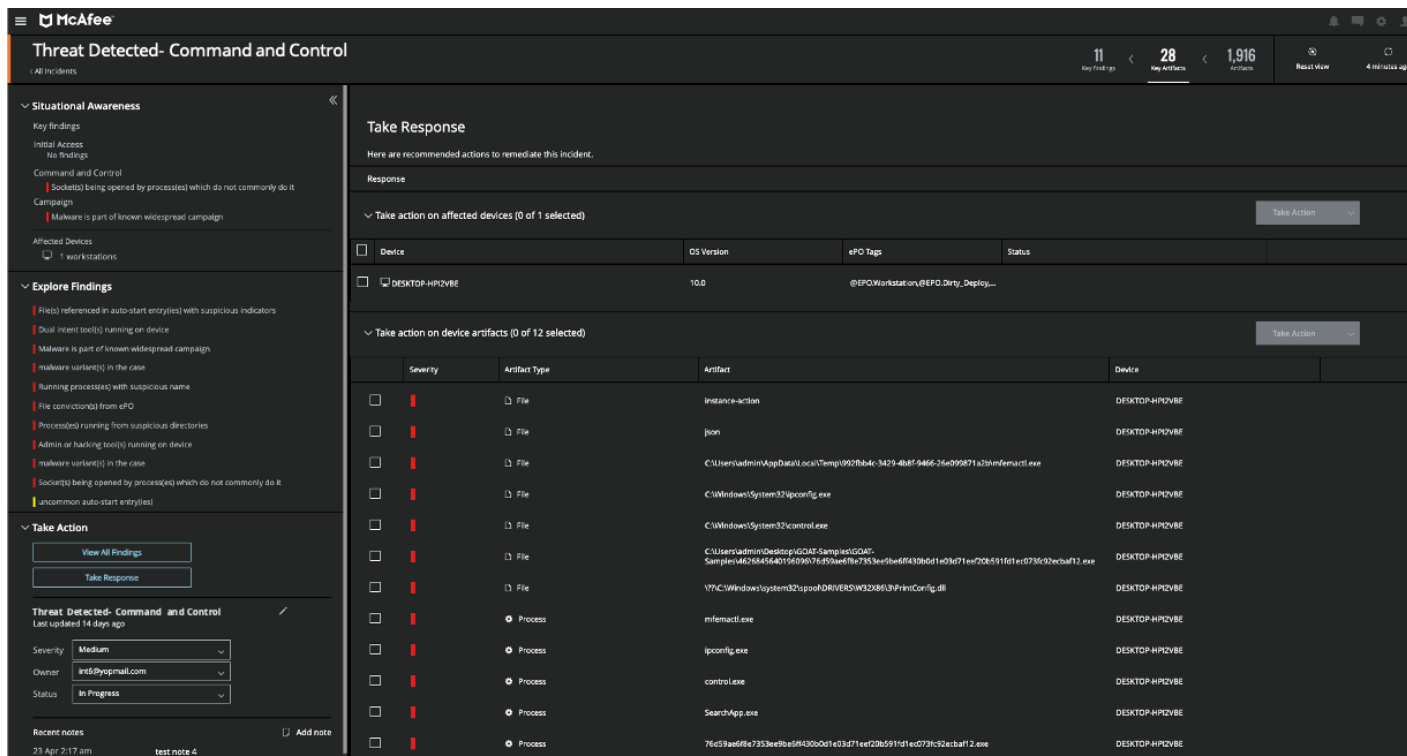


Figure 5. Recommended actions help you move quickly to remediate incidents and contain threats.

SOLUTION BRIEF

Orchestrate Efficient, Automated Workflows

MVISION XDR is an open, integrated platform scaling across multiple vectors and connecting other security functions. This allows security tool to work together in a unified fashion to mitigate the adversary. There's no need to manually jump between tools and copy/paste data, saving time and reducing human error. It also enables correlation of detections among security tools to arrive at a high-confidence alert and decision. The open application programming interface (API) allows organizations to simply create workflows (hunt, investigate, respond, mitigate) with McAfee and/or third parties from the easy-to-use marketplace, resulting in streamlined cyberthreat management.

Other third-party solutions may include IT ticketing, security orchestration automation response (SOAR), SIEM, and threat intelligence. MVISION XDR allows you to leverage existing investments, whether they are McAfee or non-McAfee. There's no need to rip and replace your current cyberdefenses.

The MVISION XDR journey allows you to phase into the capabilities and workflows at your pace. The McAfee commitment to open, integrated security, which makes sharing information and coordinating protection easier, is reflected in our role as a co-founder of the Open Cyber Security Alliance (OCA), an industry-wide security initiative and contributing OpenDXL ontology, a common transport mechanism and information exchange protocol.

In Summary

MVISION XDR is the industry's first proactive, data-aware, and open XDR solution that empowers SOC teams to:

- Connect the dots across disparate alerts to see the complete attack lifecycle, prioritize threats that matter, and get ahead of adversaries.
- Automate investigation and response processes to eliminate manual tasks and save time to focus on other tasks that better leverage their knowledge.
- Proactively hunt threats and adversarial activity targeting their organization and mitigate risks to unprotected assets and data.

Learn More

For more information, visit us at mcafee.com/xdr.

1. Threat Detection and Response Landscape Survey, ESG, 2019
2. "Is Your Threat Hunting Working?", SANS, 2020
3. Threat Detection and Response Landscape Survey, ESG, 2019
4. McAfee internal customer research.

This document contains information on products, services and/or processes in development. The benefits described herein depend on system configuration and require enabled hardware, software, and/or service activation. All information provided here is subject to change without notice at McAfee's sole discretion. Contact your McAfee representative to obtain the latest forecast, schedule, specifications, and roadmaps.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2021 McAfee, LLC. 4742_0521 MAY 2021



6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com