McAfee MVISION XDR

The industry's only proactive, data-aware, and open XDR

Security Operations Realities

Security operation center (SOC) is a core function in an organization's cybersecurity charter. The SOC's key focus is to quickly find and resolve threats to avoid damage to assets and data. If SOC operations are struggling, it is likely security outcomes are dubious and organizations are at risk. The SOC challenges continue to grow in volume and scale. Three quarters of security professionals advise that threat detection and response is more difficult today than two years ago (ESG 2019). So does this mean the adversaries are winning?

It's fair to say that the SOC function is still maturing, with 68% of organizations needing or having threat-hunting functions that they recognize as immature or just maturing. Only 40% have incident response as part of the SOC function, according to SANS (2019.)

Only 26% say the SOC identified a significant event.

(Ernst & Young, 2020)

Only 51% are satisfied with SOC effectiveness in detecting attacks.

(Ponemon Research)

Connect With Us

In most cases, the SOC is also under-resourced due to the immense cybersecurity skill 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 Research, 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 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 Inefficiencies

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[1] of threat campaign assessment with the first open, proactive, and data-aware XDR.

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

- Remove manual error that can result from 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 industry-first preemptive 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

More than 4 million unfilled positions, 65% organizations reported a shortage of cybersecurity staff, and 61% applicants are not qualified.

(ISC2)

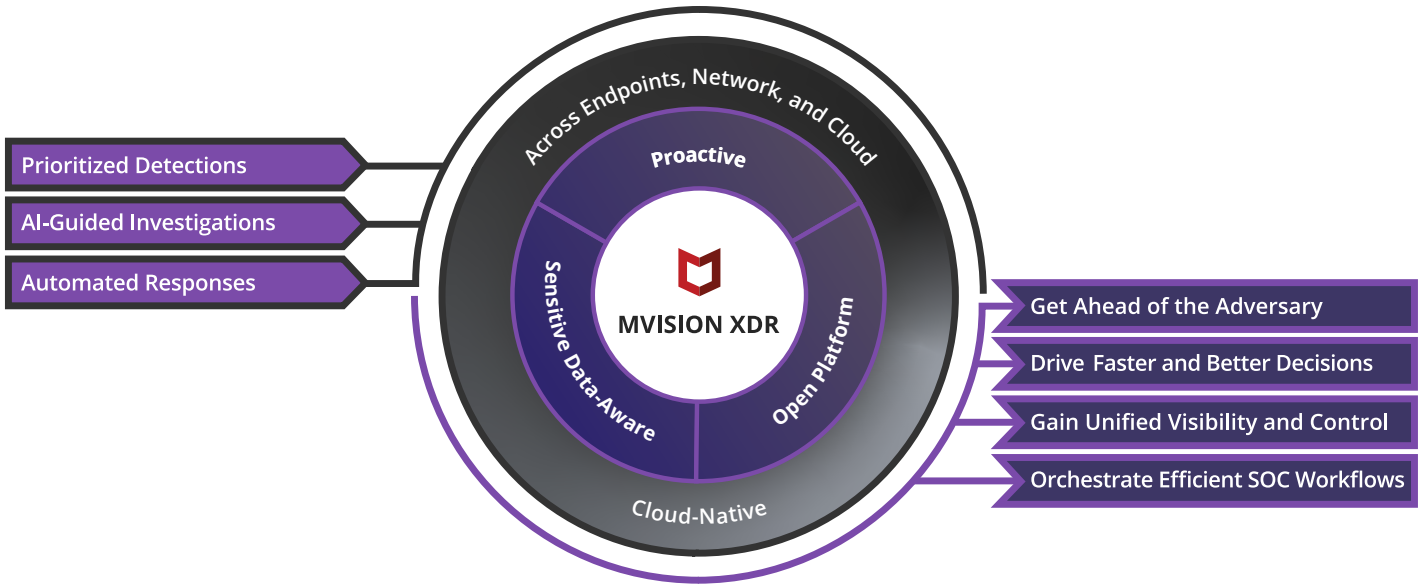

Figure 1. MVISION XDR Advantages.

Yield Proactive Actionable Intelligence—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, with the inclusion of 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. SOCs 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—which occurs in minutes rather than weeks.

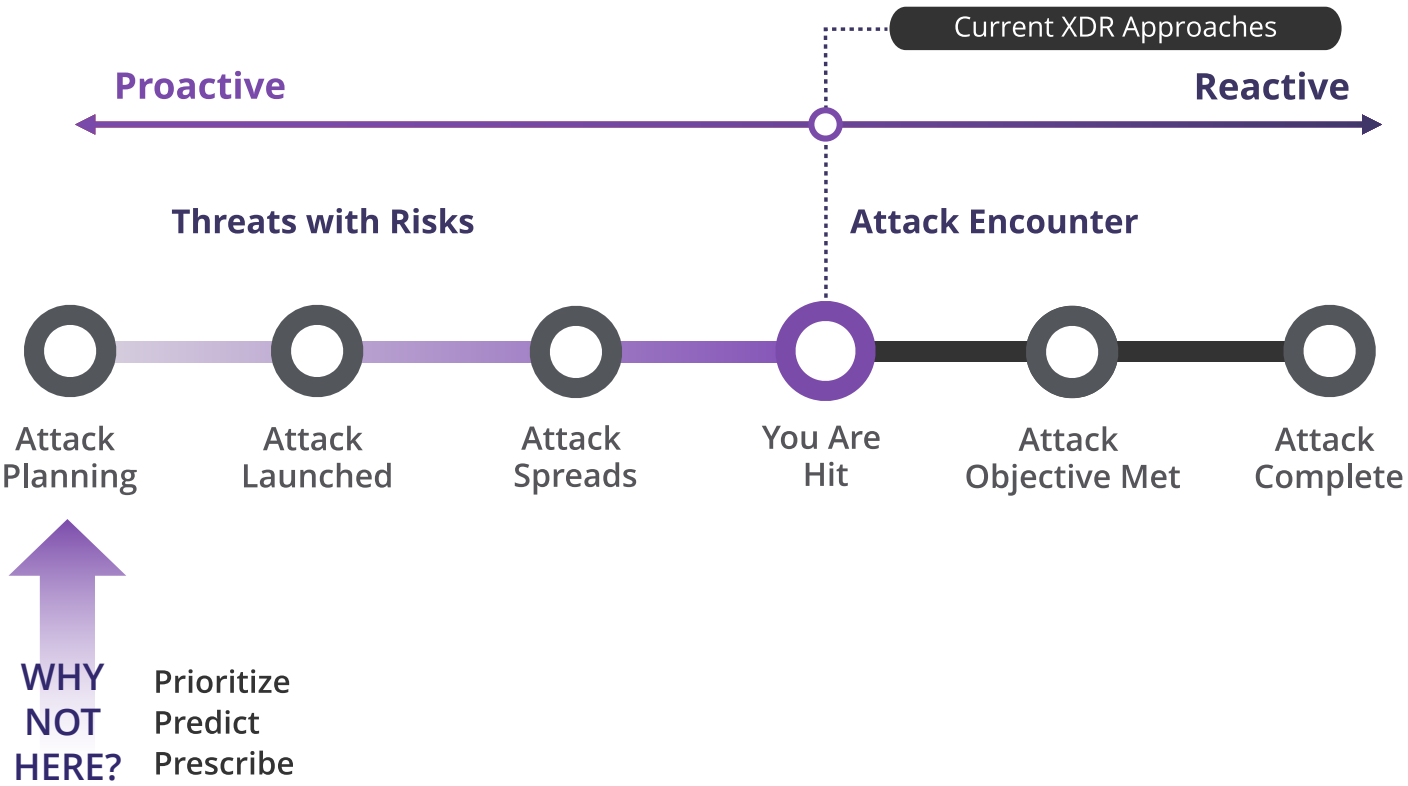

Figure 2. MVISION XDR addresses the entire cyberattack lifecycle.

Gain Unified Visibility and Control Across Multiple 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 may affect multiple vectors across the entire enterprise.

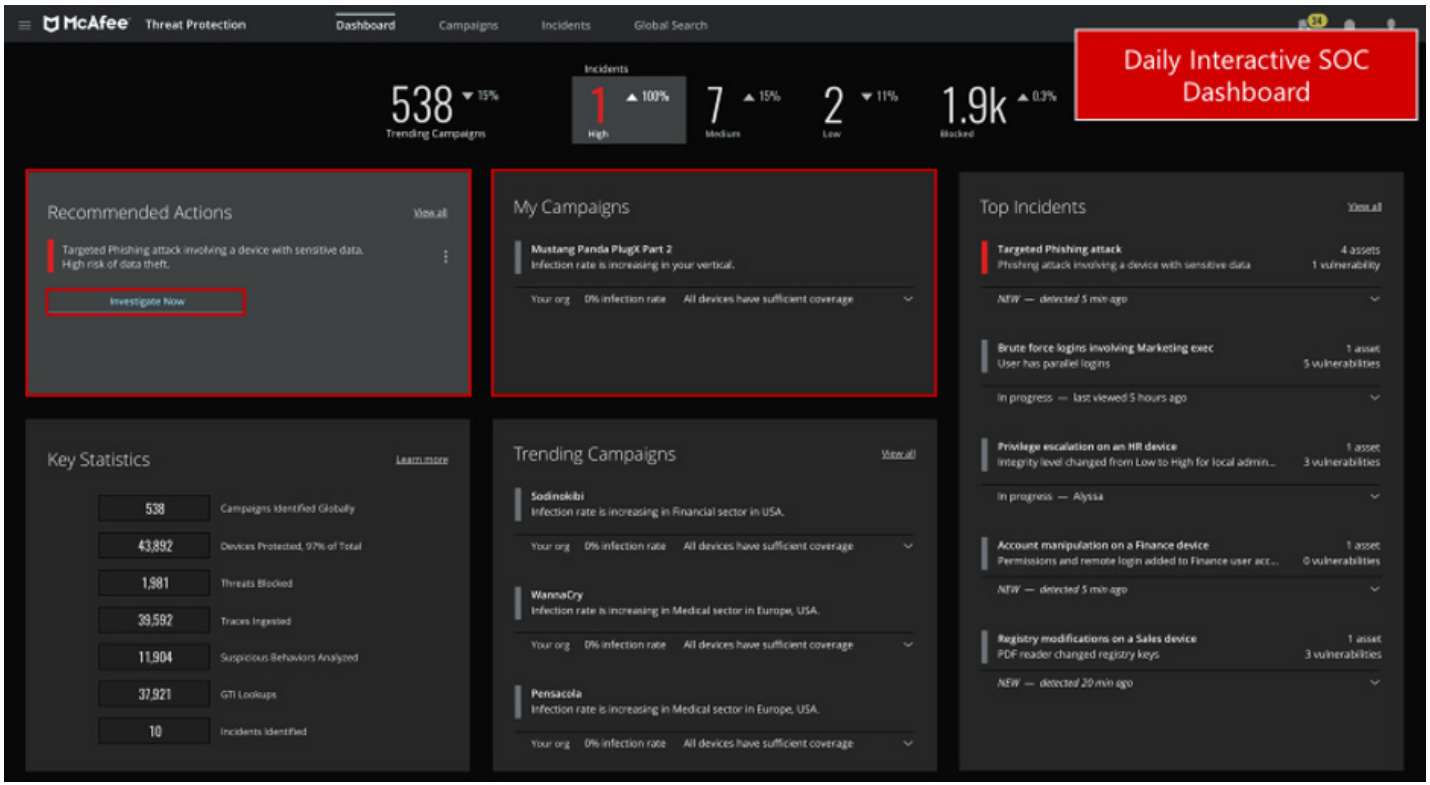

Figure 3. MVISION XDR's intuitive and interactive dashboard.

Drive Faster and 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/or 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 threat 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.

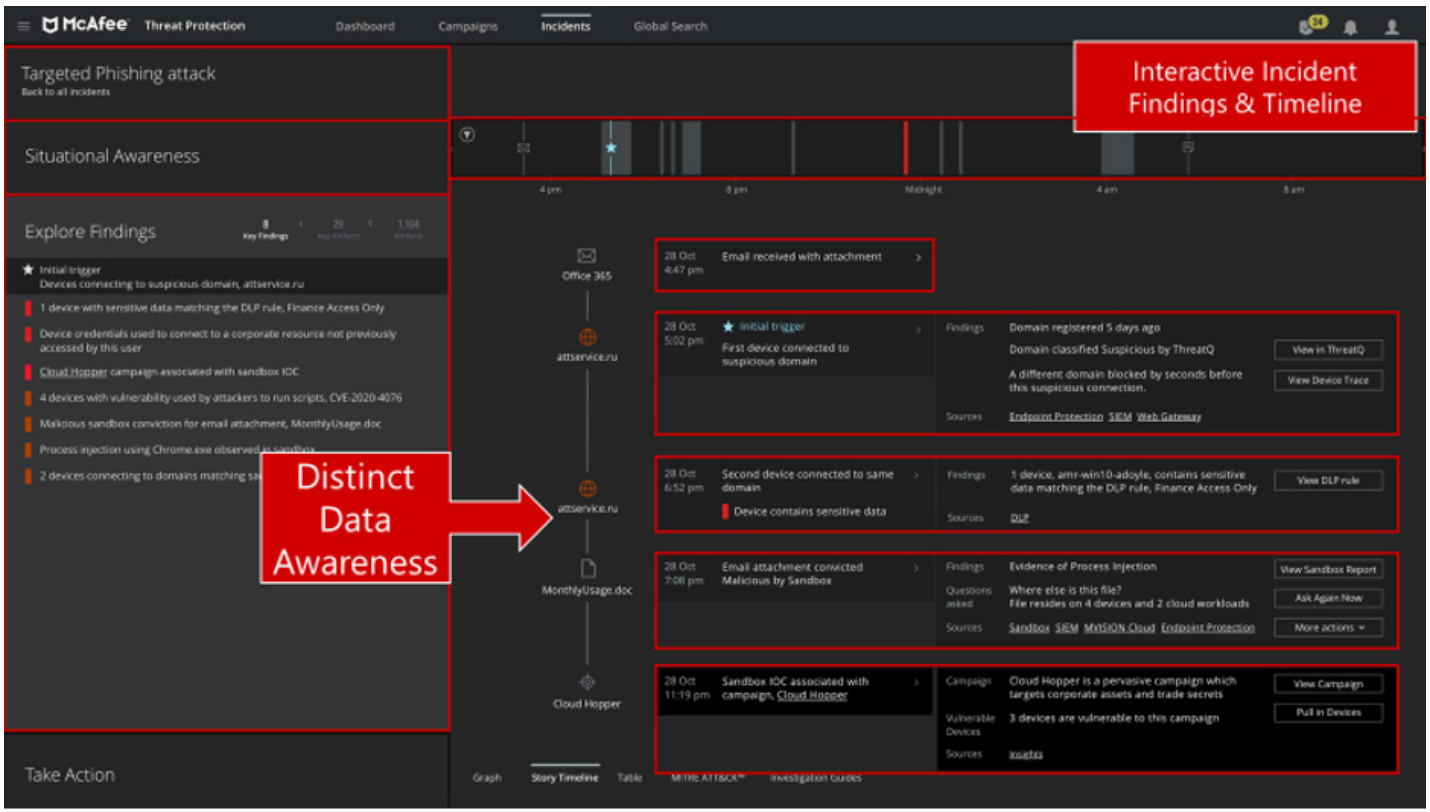

Figure 4. MVISION XDR incident findings and timeline call out a risk to sensitive data.

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 assess 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.

Easily Orchestrate Efficient SOC Workflows

MVISION XDR is an open, integrated platform scaling across multiple vectors and connecting other security functions. This allows security tools to work together in a unified fashion to mitigate the adversary. There's no need to manually jump between tools and cut and paste data, reducing time and the potential for 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.

MVISION XDR, the only proactive, data-aware, and open XDR, empowers the SOC to quickly detect, respond, and mitigate threats with high confidence. SOCs can move quickly through triggers, and incident and root cause analysis to threat remediation and proactive prevention of the threats that matter most.

1. 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.

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