SOLUTION BRIEF

McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Powerful threat detection, guided investigation, and response—simplified

Adversaries maneuver in covert ways—camouflaging their actions within the most trusted components already in your environment. They don't always install something tangible like malware, but they always leave behind a behavioral trail. Endpoint detection and response (EDR) continuously monitor and gather data to provide the visibility and context needed to detect and respond to threats. But current approaches often dump too much information on already stretched security teams. McAfee® MVISION EDR helps to manage the high volume of alerts, empowering analysts of all skill levels to do more and investigate more effectively.

Key Benefits

- Provides high-quality actionable threat detection without the noise.
- Faster analysis allows you to mount a more resilient defense.
- AI-guided investigations provide analysts with machine-generated insights into the attack.
- Organizations can maximize the impact of their existing staff.
- It's a low-maintenance cloud solution.
- Simplify deployments by leveraging existing on-premises McAfee ePO software or SaaS-based MVISON ePO.
- Analysts can focus on strategic incident response without burdensome administration overhead.

Connect With Us

Strengthen, Speed, and Simplify EDR

MVISION EDR reduces mean time to detect and respond to threats by enabling all analysts to understand alerts, fully investigate, and quickly respond. Advanced analytics broaden detection and make sense of alerts. Artificial intelligence (AI) guided investigations and automation equip even novice analysts on how to analyze at a higher level and free your more senior analysts to apply their skills to the hunt and accelerate response time.

Detect Advanced Endpoint Threats and Respond Faster

Without the right data, context, and analytics, EDR systems either generate too many alerts or miss emerging threats, wasting precious time and resources without improving security. MVISION EDR offers always-on data collection and multiple analytic engines throughout the detection and investigation stages to help accurately surface suspicious behavior, make sense of alerts, and inform action.

- **Gain context and visibility:** Endpoint event information is streamed to the cloud, providing the context and visibility necessary to uncover stealthy threats. Endpoint information is available for immediate inspection and real-time search, in addition to historical search. Flexible data retention options support the varied needs of diverse security operations teams and organizations.
- **Uncover more with powerful cloud-based analytics:** Analytic engines inspect endpoint activity to uncover a broad spectrum of suspicious behavior and detect threats—from file-based malware to file-less attacks—that have slipped by other security defenses. Cloud-based deployment enables rapid adoption of new analytic engines and techniques.
- **Think like an attacker:** Behavior-based detection results map to the MITRE ATT&CK™ framework, supporting a more consistent process to determine the phase of a threat and its associated risk and to prioritize a response.
- **Easily navigate:** Alert ranking further helps analysts understand risk severity and appropriate response. Flexible data display and visualization at this stage help analysts with different levels of experience easily navigate the data to quickly understand why an alert was raised and determine next steps: dismiss, respond, or investigate.
- **Respond with speed:** MVISION EDR preconfigured responses enable immediate action. Users can easily contain threats by killing a process, quarantining a machine, and deleting files. Analysts can act on a single endpoint or scale response to the entire estate with a single click.

AI-Guided Investigation

If immediate response to an alert and root cause of the incident is not obvious—and often it is not—security analysts must step outside their EDR solution and investigate to truly understand all the facets of a complex threat or campaign and the associated risk. EDR solutions traditionally “enable” investigation by providing raw data, context, and search functions but still require knowledgeable analysts to perform the inquiry and analysis. Experienced analysts often do not have time to validate and investigate numerous alerts, while inexperienced analysts may not know where to start.

With MVISION EDR, analysts at any level can take the next step and investigate. Rather than simply enabling an investigation with search functionality and data, MVISION EDR guides the investigation.

- **Dynamic investigation guides:** Built by combining the experience and expertise from McAfee forensic investigators with artificial intelligence (AI), investigation guides force-multiply the investigation process and explore many hypotheses in parallel for maximum speed and accuracy. Unlike playbooks that automate scripted tasks for known threats, investigation guides dynamically adjust to the case at hand, combining different investigation strategies and data. MVISION EDR automatically asks and answers questions to prove or disprove the hypotheses. MVISION EDR automatically gathers, summarizes, and visualizes evidence from multiple sources and iterates as the investigation evolves.
- **Broad data collection and local relevancy:** The AI-powered investigation engine gathers and processes artifacts and complex event sequences—from endpoints, security information and event management (SIEM) systems, and McAfee® ePolicy Orchestrator® (McAfee ePO™) software—to help make sense of alerts. MVISION EDR compares evidence against known normal activity for each organization and threat intelligence sources to improve local relevancy and reduce false positives triggered against normal activity. Investigations can originate from either MVISION EDR or SIEM alerts.
- **Different views for different users:** The flexible data display applies the appropriate lens for users with different levels of experience, so all analysts can quickly understand how artifacts and events are connected without pivoting to multiple screens.
- **Phishing investigation:** MVISION EDR easily plugs into security operations phishing investigation workflows. Suspicious emails can flow to MVISION EDR for inspection. If found to be malicious, MVISION EDR can quickly determine which machines across the organization may be impacted.

MVISION EDR reduces the expertise and effort needed to perform investigations and increases the speed with which analysts can determine the risk of the incident and root cause. At an organizational level, the benefits multiply. Each analyst can be more efficient, more cases can be dispositioned by junior analysts, and senior analysts can spend time on the highest value activities.

The Right Data—at the Right Time—for the Task at Hand

In addition to guided investigation, analysts and threat hunters can use the powerful MVISION EDR search and data collection capabilities to expand inquiries and look deeply into and across systems.

- **Historical search:** The always-on and comprehensive data collection streams endpoint event information from all monitored systems to the cloud. Analysts can search this centralized data—regardless of current online or offline status of each endpoint—to find indicators of compromise (IoCs) and indicators of attack (IoAs) that may be present along with deleted files.

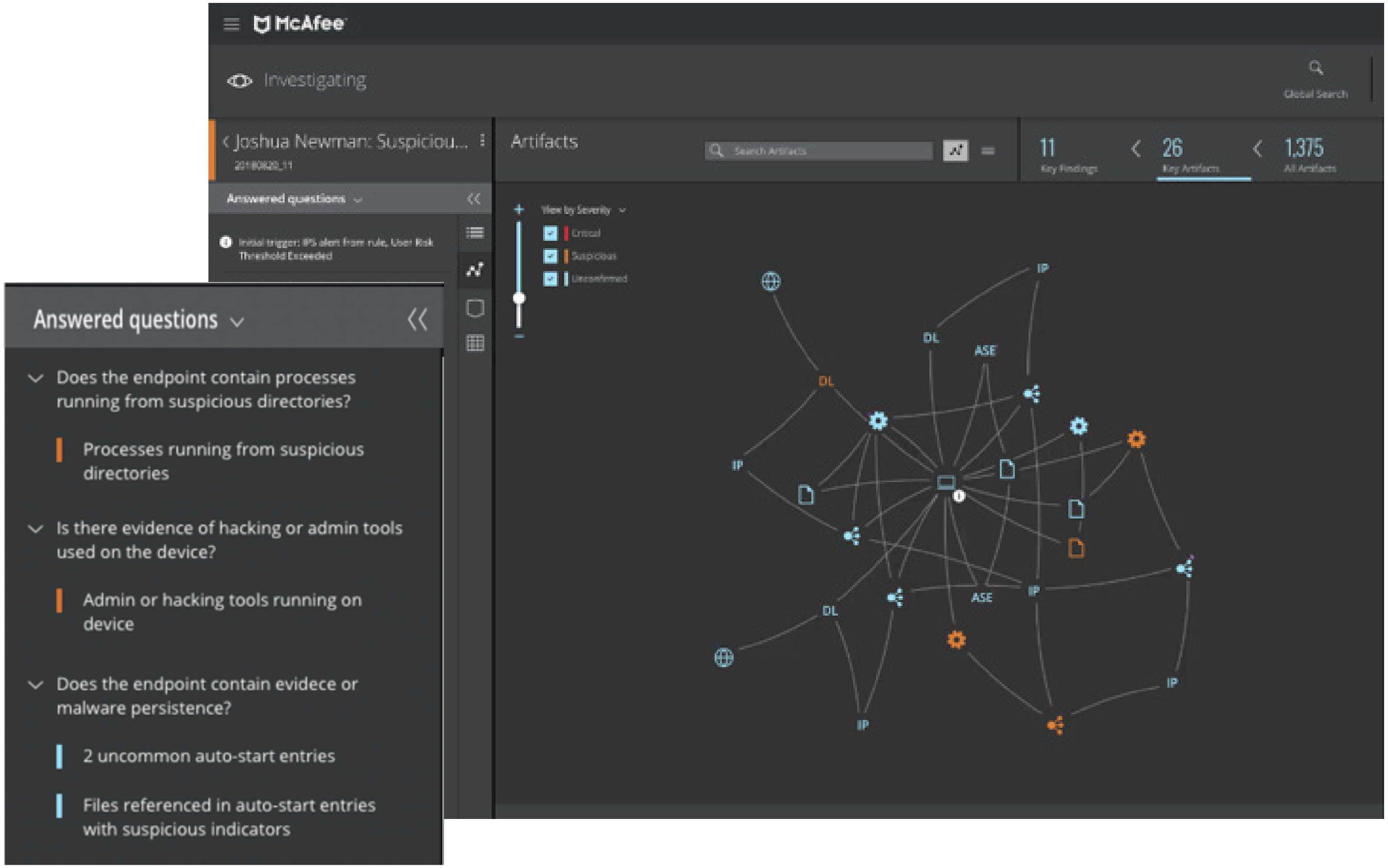
- **Real-time search:** For active incident inquiries, real-time search reaches out to endpoints across the estate to quickly query for up-to-the-moment information. Flexible syntax enables a range of capabilities, from simple queries, such as searching workstations for installed applications, to more complex searches that return more data from the workstation, such as identifying a user at the time of event, command line execution, and when the suspected application was started. This capability can easily scale queries across the enterprise to tens of thousands of machines.
- **On-demand data collection:** To support investigations, MVISION EDR can take a snapshot of an endpoint on demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. MVISION EDR provides associated severity and additional information, such as hash, reputation, and the parent process/service/user that executed a suspect file. Enabled by a non-persistent data collection tool, snapshots can be captured on both monitored and non-monitored systems.

Collaboration Expands Visibility, Increases Operational Efficiency, and Improves Outcomes

MVISION EDR is a key component of an integrated security ecosystem. It extends endpoint protection capabilities and expands visibility while supporting the workflows and processes of the security team to help reduce mean time to detect and respond and increase operational efficiency.

- **Correlate data from across the enterprise for complete visibility:** Collaboration and easy integration with data sources beyond the endpoint is key to closing data gaps for multifaceted threat investigations. Tight integration with security information and event management (SIEM) solutions, such as McAfee® Enterprise Security Manager or third-party products, enables MVISION EDR to expand investigation capabilities and insight by correlating endpoint artifacts with network information and other data collected by the SIEM.
- **Support team collaboration and workflows:** MVISION EDR plugs into current security operations workflows and supports collaboration by sharing investigation data and updates through security incident response platforms.
- **Scalable, simple deployment:** MVISION EDR is available as a SaaS application. Management with McAfee ePO software—the industry's foremost centralized security management platform—simplifies deployment and ongoing maintenance of MVISION EDR and your entire security infrastructure. Now available both on premises and in the cloud, McAfee ePO software offers management flexibility to fit diverse organizational needs.

For information on MVISION EDR, contact your McAfee representative or visit www.mcafee.com/mvision.



McAfee

Investigating

Global Search

Joshua Newman: Suspiciou...

20180820_11

Artifacts

Search Artifacts

11 Key Findings

26 Key Artifacts

1,375 All Artifacts

Answered questions

Initial trigger: IPS alert from rule, User Risk Threshold Exceeded

View by Severity

☑ Critical

☑ Suspicious

☑ Unconfirmed

Answered questions

- Does the endpoint contain processes running from suspicious directories?
  - Processes running from suspicious directories
- Is there evidence of hacking or admin tools used on the device?
  - Admin or hacking tools running on device
- Does the endpoint contain evidece or malware persistence?
  - 2 uncommon auto-start entries
  - Files referenced in auto-start entries with suspicious indicators

Figure 1. MVISION EDR investigates for you. It automatically collects artifacts and presents the key findings. Visualization displays relationships and speeds analyst understanding. MVISION EDR asks and answers the right questions to prove or disprove the hypotheses.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com