SOLUTION BRIEF

Managed Detection and Response (MDR) with Tailored and Curated Threat Intelligence

An MDR security platform is considered an advanced 24/7 security control that often includes a range of fundamental security activities, including cloud-managed security for organizations that cannot maintain their own security operations center (SOC). MDR services combine advanced analytics, threat intelligence, and human expertise in incident investigation and response deployed at the host and network levels. As the central component of an MDR, McAfee® MVISION Endpoint Detection and Response (MVISION EDR) is a cloud-delivered service that enables customers to detect advanced threats, investigate, and respond quickly. When implemented in combination with the ThreatQuotient Threat Intelligence Platform, it becomes an indispensable asset to the modern MDR environment.

Organizations are challenged to maximize the impact of their existing staff and still get the advanced EDR skills they need, when they need them.

Globally and across every vertical, utilizing threat intelligence has become a key piece of a well-rounded security program and can provide a homogenous data layer across disparate heterogenous systems. However, with hundreds of different independent sources of threat intelligence available and growing, most companies do not know where to start, what the data means to them, or how they can use it effectively.

Consuming EDR and operationalizing available threat intelligence as a low-maintenance cloud solution and managed service is critical, so analysts can focus on strategic incident response rather than administration overhead.

MVISION EDR, combined with ThreatQuotient's open and extensible threat intelligence platform ThreatQ, accelerates security operations. MVISION EDR guided investigations in concert with the integrated, self-tuning ThreatQ Threat Library, Adaptive Workbench, and Open Exchange allow you to quickly understand threats, make better decisions, and accelerate detection and response.

Prioritized, relevant threat intelligence from more than 80 open source threat feeds, 30 commercial feeds, and information from sources like MITRE ATT&CK are exchanged in real time between ThreatQ and MVISION EDR. This results in unparalleled insights for customers with respect to external threats and what's occurring on their network.

McAfee Compatible Solution

- ThreatQ and McAfee MVISION EDR

Connect With Us

Threat Hunting

Analysts use external threat intelligence sources that are prioritized by relevance to your specific industry and location to provide proactive, manual threat hunting. They leverage the latest indicators of compromise (IoCs) to identify malicious threats impacting your organization.

Incident Response

Real-time actions through MVISION EDR allow analysts to quickly quarantine machines or kill processes when needed.

Investigations

McAfee® Security Innovation Alliance Partner ThreatQuotient enables the delivery of a robust threat intelligence program that natively provides curation and automation of that threat intelligence with MDR.

Combining industry-leading EDR that includes native hunting capabilities with a threat intelligence platform that automatically feeds a curated set of IoCs that require hunting and analysis simply makes sense. This is truly a synergistic combination of technologies that are integrated and architected as a best-in-class MDR offering.

The joint solution's automated hunting capability drives down mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

Case Management

Leveraging the MITRE ATT&CK framework, McAfee MVISION EDR and ThreatQ offer bidirectional, automatic enrichment and the opportunity to perform deeper analysis from a threat perspective.

When this information is associated with an EDR event, this data can be used to provide insights into questions such as: "Who is potentially attacking?", "What attack techniques are being leveraged?", "Is there any related data (such as other types of malware or even legitimate tools) that we can use to inform incident response or threat hunting team actions?"

MITRE ATT&CK tactics, techniques, and procedures (TTPs) identified in an EDR detection provide a common factor for searching the vast ThreatQ indicator data set. This data set is curated for you or your customers' organizations and automatically surfaces other relevant data in the Threat Library so as to offer suggestions for both proactive and reactive responses. The information can be used to identify specific mitigations and signatures that may be deployed to defend against a potential threat.

Key Customer Outcomes

- MVISION EDR provides continuous, real-time monitoring of connected devices, enabling threat identification and immediate and historical search.
- Leveraging the advanced capabilities of MVISION EDR and ThreatQ, analysts review alerts, investigate threats, prioritize incidents, and initiate a response. The MDR service provides highly actionable threat detection and automated hunting with curated threat intelligence without the noise and overhead.
- Artificial intelligence (AI)-guided investigations with ThreatQ correlate and identify relationships with existing threat data within the ThreatQ Threat Library, automatically augmenting the efforts of your expert team.
- Supplement your investigations of events with visual analysis of potential threats in context using ThreatQ investigations.

The added advantages of MVISION EDR and ThreatQ delivered together as a managed offering are:

- MDR with per-tenant curated threat intelligence from ThreatQuotient.
- Combines configuration and policy management of the MVISION EDR solution to help organizations get the most out of their solution based on business-specific needs.
- 24/7 security monitoring of events ensures a first layer of triage and high-level investigation to quickly identify critical alerts that require more in-depth investigation.

Security organizations are struggling to find SOC analysts and are burdened with a growing number of threats and alerts. Even with a strong SOC team in place, it is still challenging to respond to threats when they occur. Cybercriminals are deploying new and ever-evolving exploit techniques that target endpoints, underscoring the need for full visibility into your endpoint estate and knowing how to use this visibility to react quickly and efficiently.

Managed Endpoint Protection

Here's how MDR enhances the McAfee partnership with ThreatQuotient in relation to Managed Endpoint Protection (MEP).

- MEP provides a first line of defense and service protection against high-volume threats, including malware, spam, phishing, known vulnerabilities, and hostile exploits.
- MEP proactively protects your endpoints with antivirus and antispyware, host firewall, intrusion-prevention services, and application and device control.
- Laptop and desktop encryption enforces full disk encryption and removable media encryption. It helps you avoid loss of sensitive data in the event of theft or loss of the device and assists with regulatory compliance.
- Security Advisory Services assist with infrastructure audit, security architecture design, and deployment of threat management and cyber hygiene solutions to protect endpoints from internal and external known and unknown threats.

Managed Detection and Response

Analysts use this information to open cases and compile actionable intelligence to fuel investigations. Automated playbooks help drive investigations with MVISION EDR. Our ability to collect data from the McAfee® ePolicy Orchestrator® (McAfee® ePO™) management console and additional data sources (with our Tier 1 offering) allows correlation with additional threat intelligence (such as McAfee® Global Threat Intelligence and VirusTotal) to help reduce false positives and streamline investigations. Behavior alerts are then mapped to the MITRE ATT&CK framework.

Analysts take these prioritized alerts and leverage the real-time and historical search, as well as on-demand data collection functionality, to aid investigations and provide the actionable intelligence required to mitigate threats.

Key Customer Outcomes (continued)

- Achieve faster analysis and understanding against the MITRE ATT&CK framework from MVISION EDR in context. By discovering who is attacking you, what software or malware they might be using, and what mitigations to apply, you can mount a more resilient defense and minimize breach impact.
- Trigger deeper analysis within MVISION EDR directly from the ThreatQ interface. This enables an MVISION EDR investigation that performs process analysis and provides additional Investigation Guides.
- Leverage ThreatQ Operations to query MVISION EDR for useful data on demand, including query NetFlow using source or destination and querying hash data.

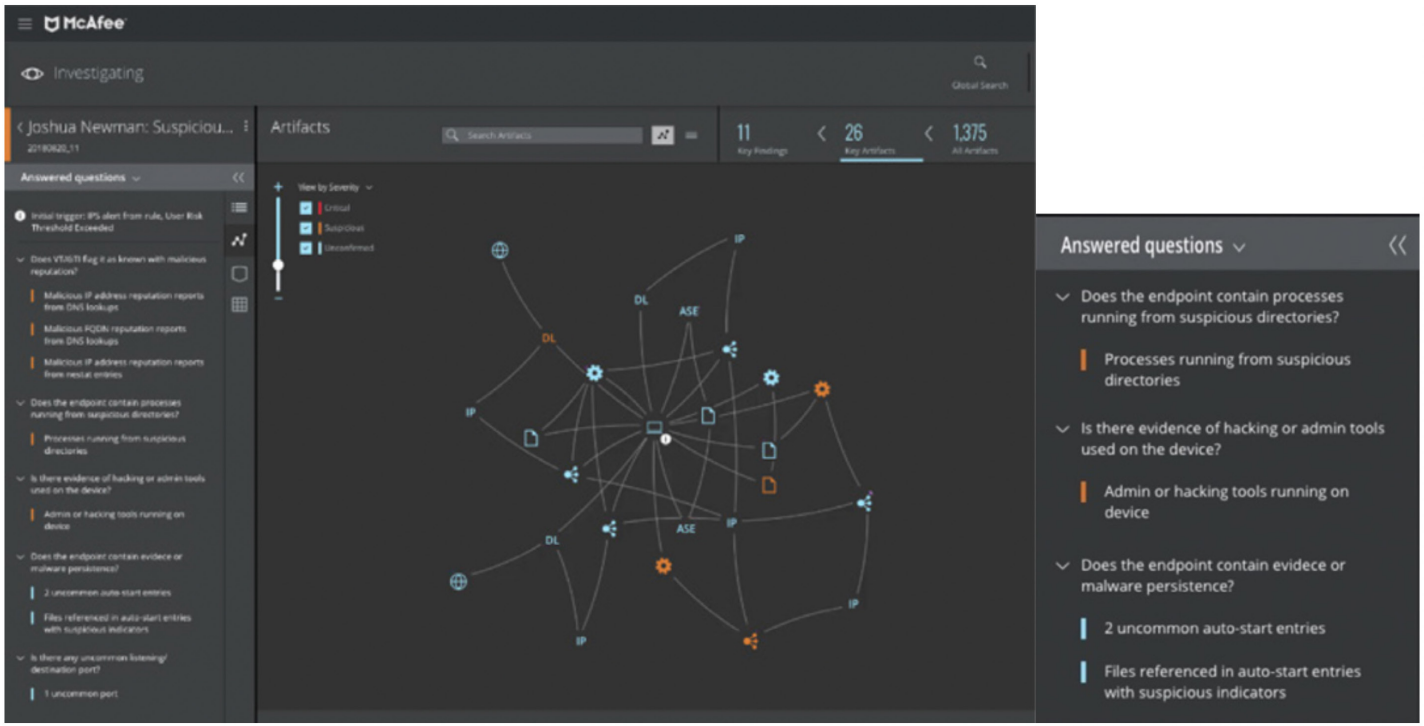

Figure 1. MVISION EDR investigates for you. It automatically collects artifacts and presents the key findings. Visualization displays relationships and speeds analyst understanding. MVISION EDR asks and answers the right questions to prove or disprove hypotheses.

Figure 2. ThreatQ Investigations allows a team to collaborate within a shared view. The team gains a shared understanding of the strategic, operational, and tactical situation by combining third-party intelligence with context from EDR. From this investigation, a team can pivot to EDR for additional information or to conduct a response.

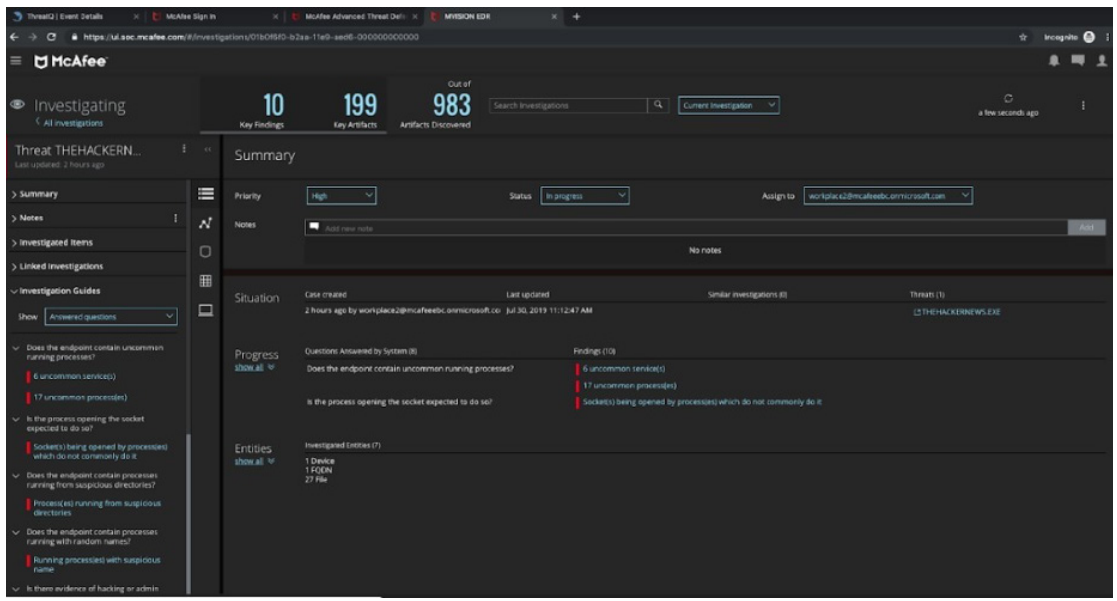

Figure 3. EDR gives the analyst tactical information about the sighting and the power to respond.

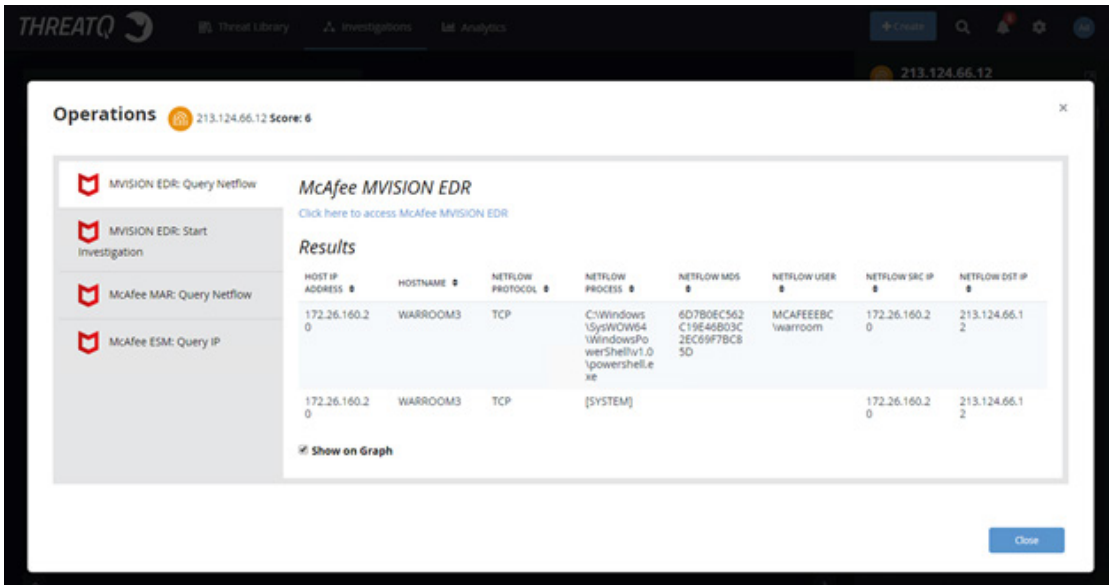

Figure 4. Easily query the environment for sightings of a reported IoC. Results are presented and the analyst can easily pivot into the EDR console for a rapid response.

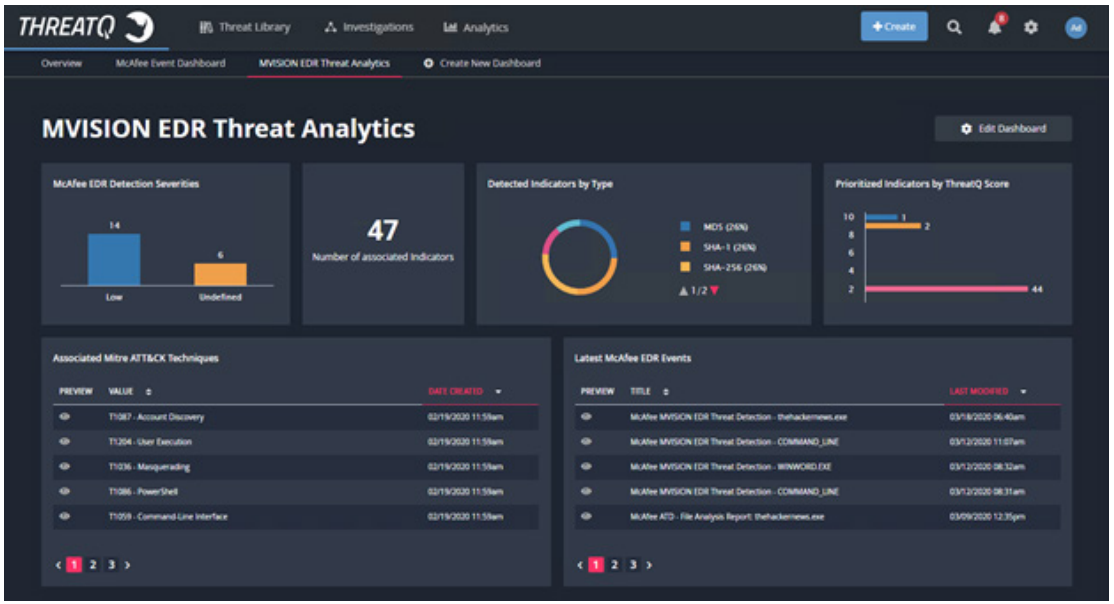

Figure 5. Custom Dashboards in ThreatQ help visualize the data collected from EDR alongside any other information about your threat landscape.

About ThreatQuotient

ThreatQuotient understands that the foundation of intelligence-drive security is people. The company's open and extensible threat intelligence platform, ThreatQ, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization, and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit threatquotient.com.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all. www.mcafee.com

Learn More

For more information, visit www.mcafee.com.

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