McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Leistungsfähige Erkennung, geführte Untersuchung und Abwehr von Bedrohungen – so einfach wie möglich

Kriminelle agieren im Verborgenen und tarnen ihre Aktionen in vertrauenswürdigen Komponenten, die sich bereits in Ihrer Umgebung befinden. Sie installieren nicht immer greifbare Elemente wie Malware, ihre Spuren sind jedoch immer anhand ihrer Verhaltensweisen sichtbar. Endpoint Detection and Response (EDR) überwacht kontinuierlich Ihre Umgebung und erfasst Daten, die Ihnen den Überblick und Kontext bieten, damit Sie Bedrohungen aufspüren und abwehren können. Die aktuellen Ansätze bedeuten jedoch häufig eine Informationsflut für die bereits überlasteten Sicherheitsteams. Daher bietet McAfee® MVISION EDR Unterstützung bei der Handhabung unzähliger Warnmeldungen, sodass Analysten unabhängig von ihrem Kenntnisstand mehr erreichen und Ereignisse effektiver untersuchen können. Nur in MVISION EDR ist McAfee® MVISION Insights[1] enthalten, die erste Technologie zur proaktiven Priorisierung von Bedrohungen *noch bevor* sie bei Ihnen Schaden anrichten können. McAfee® MVISION Insights kann vorhersagen, ob Ihre Gegenmaßnahmen ausreichend sind, und Empfehlungen geben, was Sie eventuell benötigen.

Stärkere, schnellere und einfachere Erkennung und Abwehr von Endgerätebedrohungen

Mit MVISION EDR können Sie die mittlere Zeit zur Erkennung und Reaktion auf Bedrohungen reduzieren, da alle Analysten die Warnmeldungen verstehen und vollständig untersuchen sowie schnell reagieren können. Durch erweiterte Analysen können Sie mehr Ereignisse erkennen und die Warnmeldungen sinnvoll interpretieren. Durch künstliche Intelligenz (KI) geführte Untersuchungen und Automatisierung können selbst unerfahrene Analysten genauere Analysen durchführen. Zudem können sich Ihre Analyseexperten darauf konzentrieren, verborgene Bedrohungen aufzudecken und die Reaktion zu beschleunigen.

Erkennung hochentwickelter Endgeräte-bedrohungen und schnellere Reaktion

Ohne die erforderlichen Daten, Kontext und Analysefunktionen generieren EDR-Systeme entweder zu viele Warnmeldungen oder übersehen neue Bedrohungen, sodass wertvolle Zeit und Ressourcen

Wichtige Vorteile

- Darstellung qualitativ hochwertiger, umsetzbarer Bedrohungserkennungen ohne False-Positives
- Proaktive Einblicke in Bedrohungen noch vor dem Angriff
- Schnellere Analyse zur Gewährleistung einer zuverlässigeren Abwehr
- KI-geführte Untersuchungen für Erkenntnisse zum Angriff, die von der Maschine generiert werden
- Optimale Nutzung der Stärken des vorhandenen Personals
- Wartungsarme Cloud-Lösung
- Vereinfachte Bereitstellung dank Nutzung bereits vorhandener lokaler McAfee ePO-Software oder SaaS-basierter Lösung MVISION ePO
- Konzentration auf strategische Reaktion auf Zwischenfälle ohne zusätzlichen Verwaltungsaufwand

Folgen Sie uns

verschwendet werden – ohne dass das Unternehmen von verbesserter Sicherheit profitiert. MVISION EDR bietet kontinuierliche Datenerfassung und mehrere Analysemodule für alle Erkennungs- und Untersuchungsstufen, um verdächtiges Verhalten aufzudecken, Warnungen zu erklären und informierte Aktionen zu ermöglichen.

- **Kontext und Überblick:** Informationen zu Endgeräteereignissen werden in die Cloud gestreamt und liefern den Kontext sowie den Überblick, um verborgene Bedrohungen aufzudecken. Die Endgeräteinformationen stehen für sofortige Untersuchungen und Echtzeitsuchen zur Verfügung, zusätzlich können Verlaufsdaten durchsucht werden. Dank der flexiblen Datenspeicherungsoptionen werden die vielseitigen Anforderungen der Sicherheitsteams und anderer Abteilungen unterstützt.
- **Neuer proaktiver Kontext von MVISION Insights:** Benachrichtigungen auf dem Dashboard oder E-Mail-Warnungen bei Kampagnen mit hoher Priorität werden von den Experten des McAfee® Advanced Threat Research-Teams festgelegt. Es werden jedoch nicht nur Informationen zu Kampagnen bereitgestellt, sondern auch möglicherweise kompromittierte Systeme lokal analysiert, Vorhersagen zu potenziellen Auswirkungen auf Ihre Endgeräteschutzplattform getroffen und Empfehlungen zur Verhinderung von Kompromittierungen als Gegenmaßnahmen gegeben. Dadurch gewinnt der Analyst einen Vorsprung vor den Angreifern, bevor diese losschlagen können. Die Priorisierung, Vorhersage und Empfehlung kostet nur einen Bruchteil der Zeit und Ressourcen, den Penetrationstests und Übungen mit roten/blauen Teams in Anspruch nehmen. Diese drei präventiven Faktoren sind automatisiert und übermitteln unserem Team noch vor dem Angriff Informationen zu Bedrohungen. Prozesse, die früher Wochen dauerten, benötigen nur noch Minuten. Dadurch muss ein SOC-Team nicht mehr ausschließlich reaktiv agieren – stattdessen kann es proaktiv tätig werden.
- **Mehr Erkennungen durch leistungsstarke Cloud-basierte Analysen:** Analysemodule untersuchen Aktivitäten auf Endgeräten auf verschiedenste verdächtige Verhaltensweisen und Bedrohungen von dateibasierter Malware bis zu dateilosen Angriffen, die anderen Sicherheitsmaßnahmen entgehen. Dank der Cloud-basierten Bereitstellung können neue Analysemodule und -techniken schnell implementiert werden.
- **Denken wie ein Angreifer:** Die Ergebnisse der verhaltensbasierten Erkennung werden mit dem MITRE ATT&CK™-Framework abgeglichen. Dadurch können sie konsistent einer Angriffsphase sowie den entsprechenden Risiken und angemessenen Reaktionen zugeordnet werden.
- **Einfache Navigation:** Dank der Priorisierung von Warnmeldungen können Analysten den Schweregrad besser verstehen und angemessene Reaktionen einleiten. Flexible Datenanzeigen und Visualisierungen helfen in dieser Phase den Analysten unabhängig von deren Kenntnisstand dabei, sich in den Daten zurechtzufinden und die Ursachen von Warnungen zu verstehen sowie die nächsten Schritte zu planen: ignorieren, reagieren oder untersuchen.

- **Schnelle Reaktion:** Die in MVISION EDR vorkonfigurierten Reaktionen beschleunigen Aktivitäten. Benutzer können Bedrohungen problemlos eindämmen, indem sie Prozesse stoppen, Geräte isolieren und Dateien löschen. Die mit einem Klick ausgelösten Reaktionen der Analysten können sich auf ein einzelnes Endgerät oder die gesamte Umgebung auswirken.

KI-geführte Untersuchungen

Wenn die sofortige Reaktion auf eine Warnmeldung und die Ursache des Vorfalls nicht offensichtlich sind (was häufig der Fall ist), müssen die Sicherheitsanalysten die EDR-Lösung verlassen und alle Facetten einer komplexen Bedrohung oder Kampagne sowie das damit zusammenhängende Risiko untersuchen. EDR-Lösungen „unterstützen" üblicherweise Untersuchungen, indem sie Rohdaten, Kontext und Suchfunktionen zur Verfügung stellen. Allerdings bedarf es weiterhin erfahrener Analysten, die die eigentlichen Untersuchungen und Analysen durchführen müssen. Diesen erfahrenen Analysten fehlt meist die Zeit, um unzählige Warnmeldungen validieren und untersuchen zu können, während unerfahrene Analysten nicht wissen, wo sie beginnen sollen.

Mit MVISION EDR können Analysten unabhängig von ihrem Kenntnisstand die nächsten Schritte und Untersuchungen durchführen. Statt einfach nur die erforderlichen Suchfunktionen und Daten anzubieten, leitet MVISION EDR die Analysten durch die Untersuchung.

- **Dynamische Anleitung zur Untersuchung:** Die Untersuchungsanleitungen, die auf Erfahrungen und dem Fachwissen der forensischen McAfee-Ermittler sowie künstlicher Intelligenz (KI) basieren, unterstützen den Analyseprozess und untersuchen gleichzeitig mehrere Hypothesen, um maximale Geschwindigkeit und Präzision zu erreichen. Im Gegensatz zu Playbooks, die skriptgesteuerte Aufgaben für bekannte Bedrohungen automatisieren, passen sich die Untersuchungsanleitungen dynamisch an den jeweiligen Fall an und kombinieren unterschiedliche Analysestrategien und Daten. MVISION EDR stellt automatisch Fragen und beantwortet diese, um die Hypothesen zu bestätigen oder zu widerlegen. Dazu werden Beweise aus verschiedenen Quellen von MVISION EDR automatisch gesammelt, zusammengefasst und visualisiert. Im Zuge der Untersuchung wird der Prozess mehrfach wiederholt.
- **Umfassende Datenerfassung und lokale Relevanz:** Das KI-gestützte Analysemodul erfasst und verarbeitet Artefakte sowie komplexe Ereignissequenzen von Endgeräten, SIEM-Systemen (Sicherheits-informations- und Ereignis-Management), proaktiven MVISION Insights-Informationen und McAfee® ePolicy Orchestrator® (McAfee ePO™), um Warnungen verstehen zu können. MVISION EDR vergleicht Nachweise mit für jedes Unternehmen typischen normalen Aktivitäten sowie Informationen aus Bedrohungsdatenquellen, um die lokale Relevanz zu verbessern und die Zahl von False-Positives zu verringern. Untersuchungen können durch Warnungen aus MVISION EDR oder dem SIEM-System angestoßen werden.

- **Unterschiedliche Ansichten für unterschiedliche Benutzer:** Die flexible Anzeige stellt die Daten passend zum jeweiligen Kenntnisstand der Benutzer dar, sodass alle Analysten schnell nachvollziehen können, wie Artefakte und Ereignisse verknüpft sind, ohne zwischen mehreren Bildschirmen wechseln zu müssen.
- **Phishing-Untersuchungen:** MVISION EDR integriert sich unkompliziert in Sicherheits-Workflows von Phishing-Untersuchungen. Verdächtige E-Mails können zur Untersuchung an MVISION EDR übermittelt werden. Falls sie sich als böswillig herausstellen, kann MVISION EDR schnell feststellen, welche Geräte im Unternehmen betroffen sein können.

MVISION EDR verringert die für Untersuchungen erforderliche Expertise sowie den Aufwand und erhöht die Geschwindigkeit, mit der Analysten das Risiko sowie die Ursache des Zwischenfalls ermitteln können. Auf Unternehmensebene sind die Vorteile noch größer. Jeder Analyst kann noch effizienter arbeiten, noch mehr Fälle können auch von unerfahrenen Analysten übernommen werden, und Analysespezialisten können sich auf die schwierigsten Fälle konzentrieren.

Die richtigen Daten zum richtigen Zeitpunkt für die richtige Aufgabe

Neben geführten Untersuchungen können Analysten und Bedrohungsjäger mithilfe der leistungsstarken Such- und Datenerfassungsfunktionen von MVISION EDR sowie der proaktiven Daten von MVISION Insights umfassendere Abfragen durchführen und Ereignisse genauer und systemübergreifend analysieren.

- **Suche in Verlaufsdaten:** Die permanent aktive und umfassende Datenerfassung streamt Endgeräte-ereignisinformationen von allen überwachten Systemen in die Cloud. Analysten können diese zentralisierten Daten unabhängig vom aktuellen On- oder Offline-Status jedes Endgeräts nach Kompromittierungs- und Angriffsindikatoren durchsuchen, die möglicherweise in gelöschten Dateien zu finden sind.
- **Echtzeitsuche:** Bei Abfragen zu aktiven Zwischenfällen greift die Echtzeitsuche auf Endgeräte in der Umgebung zu, um schnell aktuelle Informationen abzurufen. Die flexible Syntax ermöglicht eine Reihe von Funktionen, seien es einfache Abfragen wie das Durchsuchen von Workstations nach installierten Anwendungen bis hin zu komplexeren Suchvorgängen. Dazu gehört beispielsweise das Identifizieren eines Benutzers zum Zeitpunkt des Ereignisses, Befehlszeilenausführung sowie der Startzeitpunkt einer verdächtigen Anwendung. Diese Funktion kann ihre Abfragen problemlos über das gesamte Unternehmen auf zehntausende Geräte erweitern.

- **On-Demand-Datenerfassung:** Für einfachere Untersuchungen kann MVISION EDR bei Bedarf einen Snapshot eines Endgeräts erstellen, der eine umfassende Übersicht der aktiven Prozesse, Netzwerkverbindungen, Services und Autostart-Einträge enthält. MVISION EDR zeigt den jeweiligen Schweregrad sowie weitere Informationen an, z. B. Hash-Wert, Reputation und den übergeordneten Prozess/Dienst/Benutzer, der eine verdächtige Datei ausgeführt hat. Die von einem nicht-persistenten Datenerfassungs-Tool erstellten Snapshots können auf überwachten ebenso wie auf nicht überwachten Systemen erstellt werden.
- **Aktuelle Kampagnen:** Bei koordinierten und gezielten Angriffen (basierend auf Region oder Branche) löst MVISION Insights Warnungen aus und identifiziert Kompromittierungsindikatoren (Indicators of Compromise, IoCs), die mit EDR proaktiv gesucht werden können. Dies gibt Analysten die Möglichkeit, proaktive Suchen durchzuführen, noch bevor die Angriffe stattfinden.

Zusammenarbeit erweitert Übersicht, verbessert betriebliche Effizienz und steigert das Ergebnis

MVISION EDR ist eine wichtige Komponente eines integrierten Sicherheitsökosystems. Die McAfee-Lösung erweitert Endgeräteschutz sowie den Überblick und unterstützt die Workflows und Prozesse des Sicherheitsteams, um die mittlere Zeit zur Erkennung und Abwehr von Bedrohungen zu reduzieren sowie die betriebliche Effizienz zu steigern.

- **Korrelation von Daten aus dem gesamten Unternehmen für vollständigen Überblick:** Die Zusammenarbeit und einfache Integration von Datenquellen über das Endgerät hinaus ist unverzichtbar für das Schließen von Datenlücken bei der vielschichtigen Untersuchung von Bedrohungen. Dank der engen Integration in SIEM-Lösungen (Sicherheitsinformations- und Ereignis-Management) wie McAfee® Enterprise Security Manager oder Drittanbieterprodukte kann MVISION EDR Endgeräte-artefakte mit Netzwerkinformationen und anderen vom SIEM-System erfassten Daten korrelieren und so die eigenen Untersuchungsmöglichkeiten und Erkenntnisse ausdehnen.

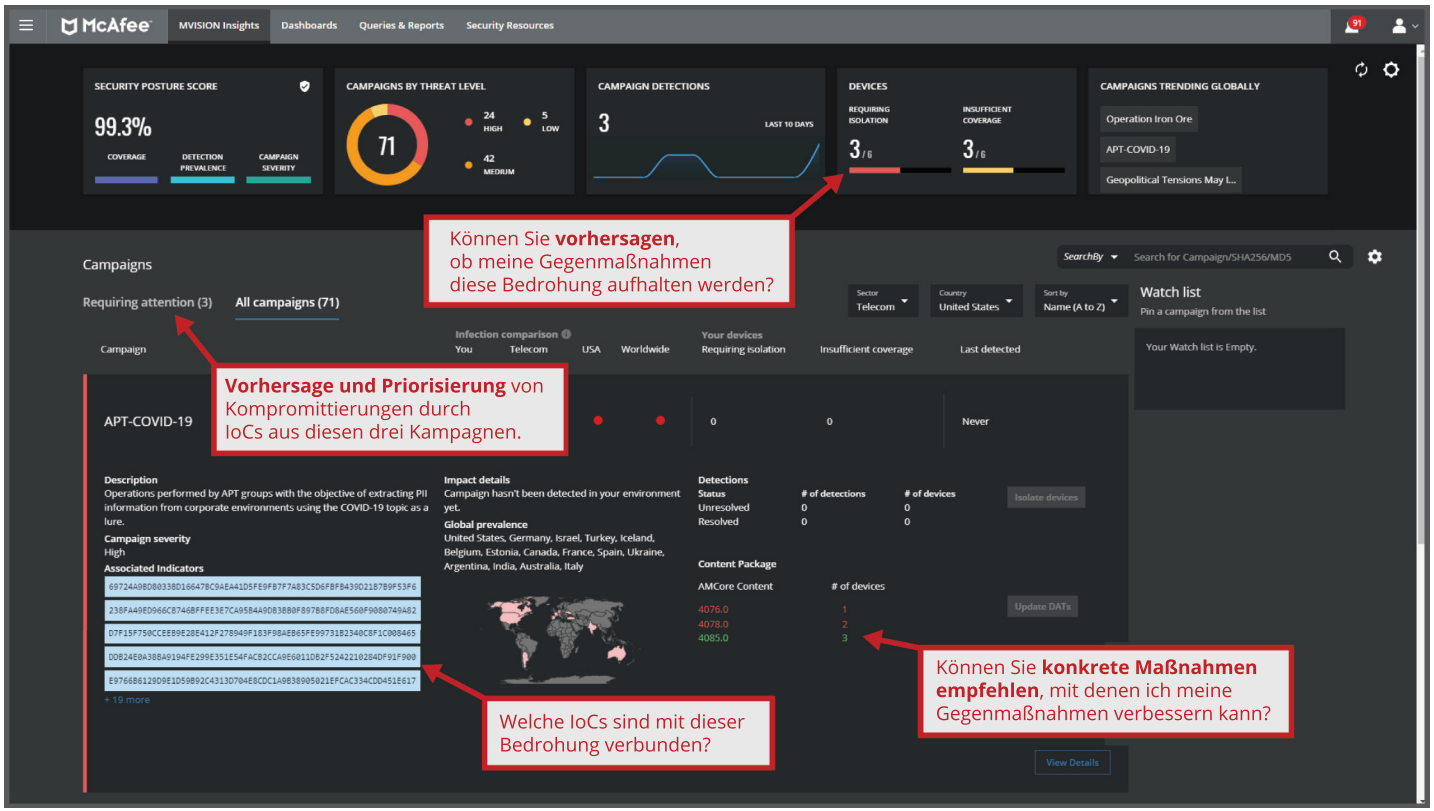

Abbildung 1. Dashboard von MVISION Insights: MVISION Insights bietet automatisch wertvolle Einblicke zu schwerwiegenden Bedrohungen sowie Empfehlungen zu Maßnahmen, noch bevor ein Angriff startet. Dank zusätzlicher Erkennungs- und Reaktionsmöglichkeiten für Endgeräte (EDR) werden Untersuchungen erleichtert und beschleunigt.

- MVISION EDR nutzt proaktiven Kontext zu neuen externen Bedrohungen, der von MVISION Insights bereitgestellt wird, um Untersuchungen sowie Behebungsmaßnahmen zu beschleunigen.
- MVISION Insights warnt bei potenziellen Kampagnen und weist Prioritäten basierend darauf zu, ob sie sich gegen Ihre Branche oder Ihre Region richten. Die Lösung sagt voraus, bei welchen Endgeräten Schutzmaßnahmen vor diesen Kampagnen fehlen, und bietet Hinweise zur Verbesserung der Erkennung. Sie informiert Analysten über die Angriffsabläufe der Kampagne sowie das Angriffsziel und gibt Hinweise zur Abwehr, die sowohl Strategien als auch konkrete Maßnahmen umfassen. MVISION Insights stellt einen vollständigen Satz an Kompromittierungsindikatoren bereit, nach denen

in MVISION EDR gesucht werden kann. Dies gibt Analysten die Möglichkeit, proaktive Suchen durchzuführen oder Indikatoren mit anderen Tools zu überprüfen.

- Wenn die Telemetrie von MVISION Insights anzeigt, dass Sie möglicherweise Ziel einer Kampagne sind, wechselt die Lösung elegant zu MVISION EDR. Analysten übernehmen die fraglichen Kompromittierungsindikatoren, müssen diese Informationen nicht manuell übertragen und sparen dadurch Zeit und Aufwand. Zu jeder Kampagne wird ein vollständiger Satz an Kompromittierungsindikatoren bereitgestellt, was die Untersuchung potenzieller Kompromittierungen erheblich beschleunigt.

- **Unterstützung von Teamzusammenarbeit und Workflows:** MVISION EDR integriert sich in laufende Sicherheitsprozesse sowie Workflows und unterstützt die Zusammenarbeit, indem die Lösung Analysedaten und Updates mit Plattformen zur Reaktion auf Sicherheitszwischenfälle austauscht.
- **Skalierbar und einfache Implementierung:** MVISION EDR ist als SaaS-Anwendung verfügbar. Die Verwaltung mit McAfee ePO – der branchenweit ersten zentralisierten Sicherheitsverwaltungs-plattform – vereinfacht die Bereitstellung sowie die laufende Wartung von MVISION EDR und Ihrer gesamten Sicherheitsinfrastruktur. McAfee ePO ist jetzt sowohl lokal als auch in der Cloud verfügbar und ermöglicht die flexible Verwaltung, um unterschiedliche betriebliche Anforderungen zu erfüllen.

Informationen zu MVISION EDR erhalten Sie von Ihrem McAfee-Vertreter oder unter www.mcafee.com/enterprise/de-de/solutions/mvision.html.

Suchen Sie verwaltete Erkennungs- und Behebungsmöglichkeiten für Endgeräte?

Managed Detection and Response (MDR) bezeichnet ausgelagerte Cyber-Sicherheits-Services, die Ihre Daten und Ressourcen selbst dann schützen, wenn eine Bedrohung die üblichen unternehmensinternen Sicherheitskontrollen unterläuft.

Eine MDR-Sicherheitsplattform gilt als hochentwickelte, rund um die Uhr aktive Sicherheitskontrolle, die verschiedenste grundlegende Sicherheitsfunktionen erfüllt, beispielsweise in der Cloud verwaltete Sicherheit für Unternehmen, die kein eigenes Sicherheitskontrollzentrum (SOC) betreiben können. MDR-Services verbinden hochentwickelte Analysen, Bedrohungsdaten sowie menschliche Expertise bei der Untersuchungen und Behebung von Vorfällen und werden auf Host- und Netzwerkebene eingesetzt. Von McAfee zertifizierte Service Provider-Partner bieten rund um die Uhr Überwachung kritischer Warnungen, verwaltete Bedrohungssuche sowie erweiterte Untersuchungen und Abwehr von Bedrohungen, mit denen sie die Bedrohungserkennung und -abwehr von Unternehmen erheblich verbessern.

Weitere Informationen zu McAfee-MDR erhalten Sie unter www.mcafee.com/MDR.

1. Damit MVISION Insights ordnungsgemäß funktioniert, müssen Sie die Erfassung und Übertragung von Telemetriedaten in McAfee Endpoint Security erlauben. Wenn Sie diese Telemetriedaten nicht zur Verfügung stellen möchten, sollten Sie das Produkt nicht wählen, da Sie nicht den vollen Funktionsumfang nutzen können.

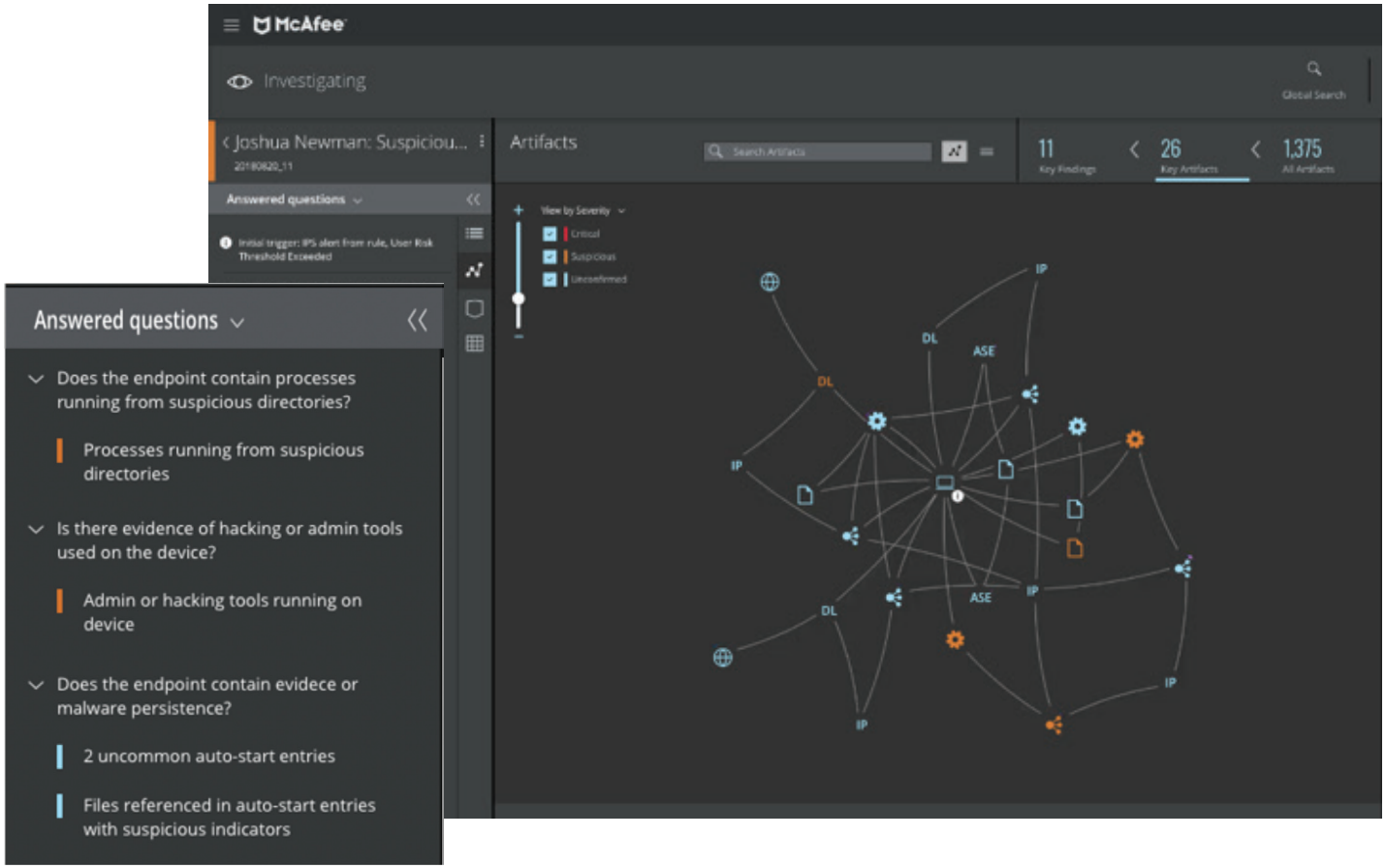

Abbildung 2. MVISION EDR ermittelt für Sie. Die Lösung erfasst automatisch Artefakte und zeigt eine Übersicht der wichtigsten Erkenntnisse. Durch die Visualisierung werden die Beziehungen zwischen den Artefakten dargestellt und der Erkenntnisgewinn der Analysten beschleunigt. MVISION EDR stellt die richtigen Fragen und beantwortet diese, um die Hypothesen zu bestätigen oder zu widerlegen.

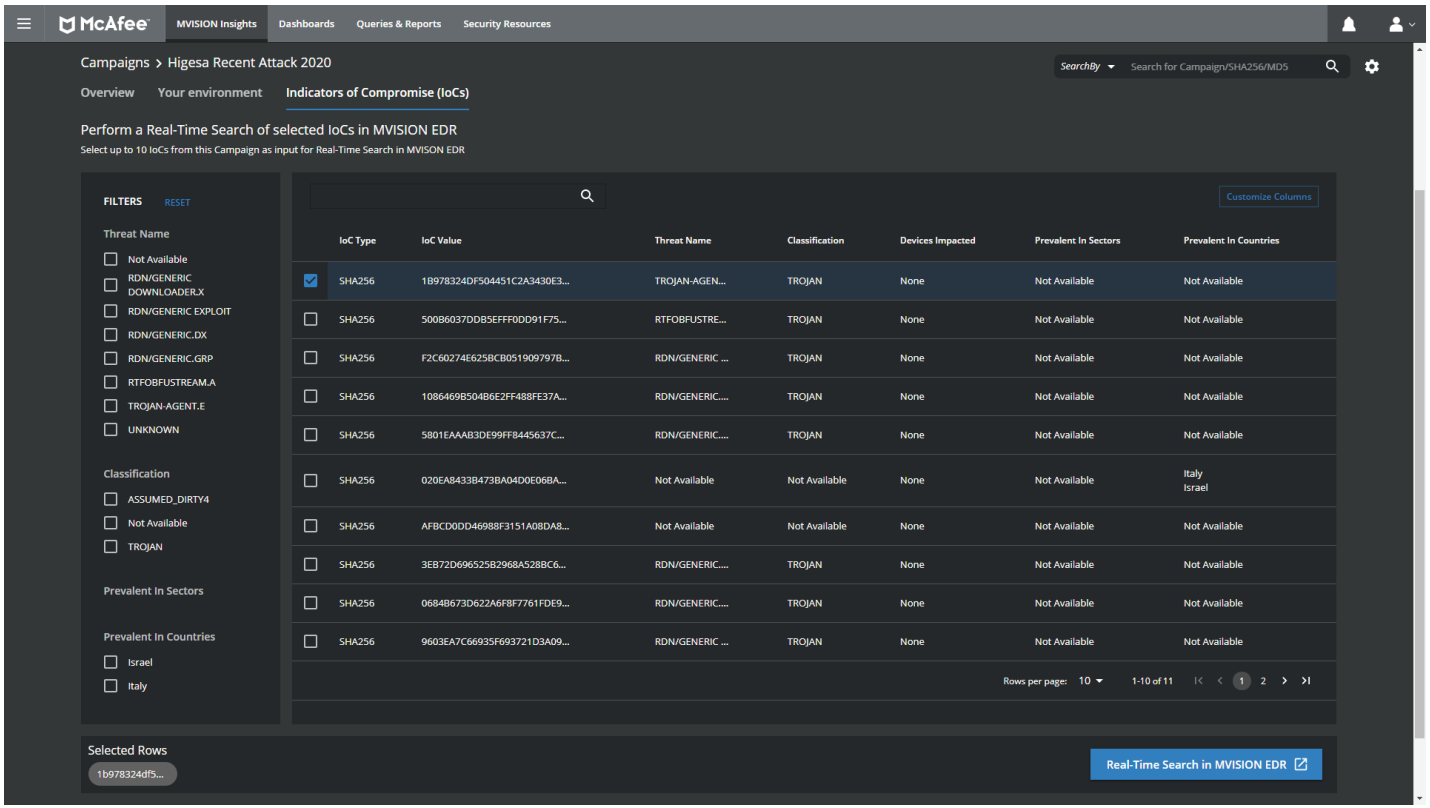

Abbildung 3. MVISION Insights bietet Kompromittierungsindikatoren zu schwerwiegenden Bedrohungen sowie die Möglichkeit, in EDR-Lösungen danach zu suchen.

McAfee

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de