McAfee Endpoint Threat Defense and Response-Produktfamilie

Erkennung von Zero-Day-Malware, Absicherung von Patient Null sowie Abwehr raffinierter Angriffe

Die rasante Weiterentwicklung der Cyber-Bedrohungen macht eine neue Generation von Endgeräteschutz notwendig. Immer raffiniertere Bedrohungen sowie das wachsende Risiko durch unbekannte Schwachstellen veranlassen Unternehmen dazu, sich überschneidende und nicht verbundene Sicherheitslösungen zu implementieren, die keine ausreichende Übersicht bieten sowie die Komplexität erhöhen. Intel Security löst dieses Problem mit McAfee® Endpoint Threat Defense und McAfee Endpoint Threat Defense and Response. Beide Lösungen können mithilfe statischer und verhaltensbasierter Analysen sowie kombinierter Bedrohungsdaten neue Bedrohungen erkennen, beseitigen, sich anpassen und Schutz bieten. Dank eines offenen, integrierten Ansatzes agieren einheitliche Sicherheitskomponenten als Gesamtheit – sie verbessern die Übersicht, teilen Bedrohungsdaten und vereinfachen Arbeitsabläufe. Vernetzte Sicherheitsfunktionen und umsetzbare Bedrohungsforensikdaten bieten eine sichere Infrastruktur, mit der Sie Bedrohungen schnell und zuverlässig aufdecken und potenziellen Angreifern stets einen Schritt voraus bleiben können.

Hauptvorteile

- Erkennung, Schutz und Behebung mit proaktiver Anpassung Ihrer Schutzmaßnahmen gegen Zero-Day-Malware, Greyware sowie Ransomware
- Effektiverer Schutz mithilfe dynamischer Reputation, Verhaltensanalysen und Machine Learning
- Minimale Beeinträchtigung von Benutzern und vertrauenswürdigen Anwendungen bei verbessertem Schutz
- Schnellere Erkennung und Behebung von mehr Bedrohungen dank Bedrohungsdaten, die über Ihr Sicherheitsökosystem verteilt werden
- Optimierung der Vorfalluntersuchung und -behebung mit einheitlichen Workflows und einer zentralen Verwaltungskonsole: McAfee® ePolicy Orchestrator® (McAfee ePO™)

Abwehr von Zero-Day-Malware, Greyware und Ransomware

Bleiben Sie neuen Bedrohungen stets einen Schritt voraus – mit statischen und dynamischen Bedrohungsanalysen, die mithilfe fortschrittlicher Reputations- sowie Verhaltensanalysen potenzielle Exploits erkennen. McAfee Threat Intelligence Exchange stellt kombinierte Bedrohungsdaten bereit, mit denen Sie Bedrohungen sofort blockieren und isolieren sowie die Bedrohungsreputation auf den neuesten Stand bringen können, um weitere Angriffe zu verhindern.

McAfee Endpoint Threat Defense und McAfee Endpoint Threat Defense and Response wehren Zero-Day-Malware ab, indem sie mithilfe einer Cloud-Suche Ähnlichkeiten zwischen festgestelltem böswilligen Verhalten und den umfassenden Real Protect-Bedrohungsmodellen aufspüren. Die hierfür verwendeten Cloud-Rechenzentren werden in den USA gehostet. Mit dieser Technik zur Verhaltensklassifikation werden aktive Bedrohungen erkannt, die andere Sicherheits-Software umgehen konnten. Die umsetzbaren Bedrohungsdaten werden von der Software

McAfee ePolicy Orchestrator bereitgestellt und ermöglichen die Erkennung und Echtzeit-Behebung von Zero-Day-Bedrohungen. Da die Verhaltensklassifikation durch dynamisches Machine Learning automatisch weiter trainiert wird, werden der Schutz sowie die Effizienz maximiert und Sicherheitslücken minimiert.

Verringerung der Anzahl von Zwischenfällen und schnellere Behebung von Bedrohungen

Konzentrieren Sie sich auf das, was für Sie wirklich wichtig ist: Minimieren Sie die Anzahl der Sicherheitsereignisse, decken Sie mehr Bedrohungen automatisch auf, tauschen Sie Bedrohungsdaten aus, und lösen Sie mithilfe von Warnungen proaktiv automatische Reaktionen aus. Verringern Sie den Aufwand für die Untersuchung sowie Beseitigung von Bedrohungen mit vereinfachten Workflows, die Zwischenfälle schneller beheben, die Sicherheitskapazität steigern und gleichzeitig den Schutz Ihres gesamten Unternehmens verbessern.

Vernetzte Komponenten tauschen über den McAfee Data Exchange Layer automatisch wertvolle Sicherheitsinformationen aus. McAfee Threat Intelligence Exchange ermöglicht das Kombinieren umfassender Bedrohungsinformationen aus Ihrem gesamten Ökosystem (z. B. aus McAfee Global Threat Intelligence sowie externen Quellen) und gibt diese Informationen sofort weiter, um Ihre Schutzmaßnahmen automatisch anzupassen.

Absicherung von Patient Null

Erkennen Sie Zero-Day-Malware, und verhindern Sie, dass diese Veränderungen an den Endgerätesystemen vornimmt. Die Funktion zur dynamischen Eindämmung von Anwendungsprozessen überwacht das Verhalten von Greyware und verhindert böswillige Veränderungen, um Exploits auszuschalten, noch bevor diese mit ihrem Angriff beginnen können. Sichern Sie Endgeräte inner- und außerhalb des Netzwerks ab, und dämmen Sie böswilliges Verhalten mit Sicherheitsmaßnahmen ein, die für Ihre Benutzer transparent sind.

Nutzung von Sicherheitsprozessen für Skalierung und Anpassung

Richtlinienerzwingung, Untersuchungen von Zwischenfällen und Behebung werden über die Software McAfee ePolicy Orchestrator (McAfee ePO) optimiert. Diese zentrale Verwaltungskonsole bietet einen Überblick über alle Systeme, damit Sie problemlos die Sicherheit Ihrer Endgeräte überprüfen und in Echtzeit Schutzmaßnahmen ergreifen können. Dank einheitlicher Workflows und Behebung mit einem einzigen Mausklick – ob für ein einziges Endgerät oder die gesamte Infrastruktur – können Sie den Aufwand für die Überwachung, Suche und Reaktion reduzieren. Mit McAfee Endpoint Threat Defense und McAfee Endpoint Threat Defense and Response stehen Ihnen automatisierte Machine-Learning-Funktionen zur Verfügung, die Verhaltensklassifizierungsmodelle mit neuesten Informationen versorgen. Zudem können Sie Bedrohungsdaten sofort an alle Sicherheitskomponenten weitergeben, damit diese als einheitliches Gesamtsystem gegen neue Bedrohungen vorgehen können. Verhindern Sie zukünftige Angriffe, und dämmen Sie potenzielle Bedrohungen mithilfe vorkonfigurierter Reaktionen ein. Das entlastet Ihre Mitarbeiter und gibt ihnen die Möglichkeit, sich auf andere Sicherheitsverwaltungsaufgaben zu konzentrieren.

Erkennung, Priorisierung und Behebung raffinierter Angriffe

McAfee Endpoint Threat Defense and Response unterstützt Sie bei der Erkennung des Ursprungs, Umfangs und der Auswirkungen eines Angriffs. Die Lösung stellt mithilfe der McAfee Active Response-Technologie eine Übersicht älterer sowie aktueller Ereignisse auf den Endgeräten in Ihrer Infrastruktur dar. Angriffsindikatoren werden erkannt, priorisiert und um umfassende Kontextdaten ergänzt, um schnellere Reaktionen zu ermöglichen.

Suchen Sie proaktiv, schnell, flexibel und erfolgreich nach Bedrohungen, die sich aktiv verbreiten, im Verborgenen warten oder ihre Spuren verwischen, um der Entdeckung zu entgehen. Dank der wissensgestützten Transparenz und Kontrolle kann ermittelt werden, wo die Bedrohungen Fuß zu fassen versuchen, sodass Ihre Sicherheitsverantwortlichen sofort Maßnahmen zur Eindämmung sowie Behebung starten können und die Sicherheitslücke von Monaten auf Minuten oder sogar Millisekunden verringert wird.

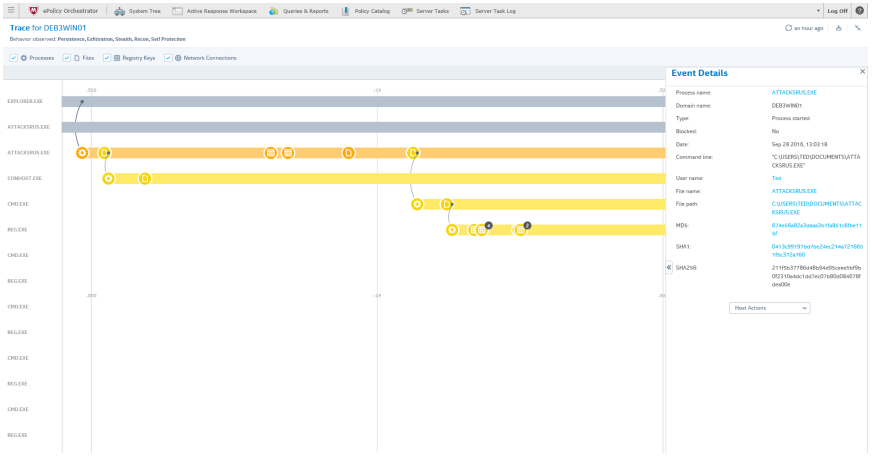

Abbildung 1. Der Bedrohungsüberblick spürt die Ursprünge und das Verhalten verdächtiger Vorfälle auf, um die Reaktion zu beschleunigen.

Funktionen der McAfee Endpoint Threat Defense and Response-Produktfamilie

Komponente	Vorteil	Kundenvorteile	Differenzierung	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Dynamische Eindämmung von Anwendungs-prozessen[1]	Schützt Patient Null, indem verhindert wird, dass Greyware böswillige Änderungen an Endgeräten inner- und außerhalb des Netzwerks vornimmt.	• Analyse potenzieller Bedrohungen, ohne Patient Null zu gefährden • Erweiterter Schutz ohne Beeinträchtigung der Benutzer oder vertrauenswürdiger Anwendungen • Kürzere Zeit von der Entdeckung bis zur Eindämmung – mit minimalen Eingriffen • Absicherung von Patient Null ohne Beeinträchtigung der Endgeräteproduktivität, Isolierung des Netzwerks von Infektionen	• Integriert in die Intel Security-Infrastruktur für optimalen Schutz und Effizienz • Funktioniert mit und ohne Internetverbindung und erfordert keine externen Eingaben oder Analysen • Transparent für die Benutzer • Beobachtungsmodus bietet sofortige Bedrohungsübersicht zu potenziellem Exploit-Verhalten innerhalb der Umgebung	√	√
Real Protect	Nutzt Machine-Learning-Verhaltens-klassifizierung zur Blockierung von Zero-Day-Malware vor deren Ausführung und wehrt aktive Bedrohungen ab, die vorherige Erkennungs-funktionen umgehen konnten.	• Einfache Abwehr von mehr Zero-Day-Malware, einschließlich gut verborgener Objekte wie Ransomware • Automatische Demaskierung, Analyse und Beseitigung von Bedrohungen ohne manuelle Eingriffe • Anpassung von Schutzmaßnahmen mithilfe automatisierter Klassifizierung und einer vernetzten Sicherheitsinfrastruktur	• Statische und dynamische Verhaltensanalyse für besseren Schutz als bei einstufigen Ansätzen • Erkennung von Malware, die nur durch dynamische Verhaltensanalysen entdeckt werden kann • Enge Vernetzung, sodass aktualisierte Reputations-informationen in Echtzeit ausgetauscht und die Sicherheitseffizienz aller Sicherheitskomponenten verbessert werden	√	√

Komponente	Vorteil	Kundenvorteile	Differenzierung	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Threat Intelligence Exchange	Vernetzt Sicherheits-komponenten zum Austausch von Kontextdaten und bietet einen unternehmens-weiten Überblick sowie Kontroll-funktionen für adaptiven Bedrohungsschutz.	• Erkennung von Patient-Null-Bedrohungen und sofortige Weitergabe innerhalb des Sicherheits-systems zur Verhinderung der nächsten Infektion • Geringere Gesamt-betriebskosten und höhere Effizienz der Endgerätesicherheit • Vernetzung unabhängiger Sicherheitstechnologien zu einem koordinierten, geschlossenen Schutzkreislauf	• Kombination von McAfee Global Threat Intelligence-Feeds sowie externen und lokalen Bedrohungsdaten • Einstufung der Vertrauens-würdigkeit anhand lokaler oder interner Bedrohungsdaten • Sofortige Weitergabe von Informationen zur Bedrohungs-reputation an Endgeräte-, Web-, Netzwerk- und Cloud-Produkte • Generierung detaillierter umsetzbarer Berichte zu Bedrohungsdaten zur Anpassung der Schutzmaßnahmen	√	√
McAfee Data Exchange Layer	Vernetzt Sicherheits-lösungen zur Integration und Optimierung der Kommunikation mit Intel Security- sowie Drittanbieter-produkten.	• Risikominimierung und kürzere Reaktionszeit • Verringerung von Verwaltungsaufwand und Personalkosten • Optimierung von Prozessen und praktische Empfehlungen	• Weitergabe der Bedrohungsinformationen an alle Sicherheits-produkte • Sofortige Weitergabe von Bedrohungsdaten über Patient Null an alle anderen Endgeräte, um Infektionen zu verhindern und die Schutzmaßnahmen zu aktualisieren	√	√
Verwaltungs-plattform McAfee ePO	Bietet einen zentralen Überblick zur stark skalierbaren, flexiblen sowie automatisierten Verwaltung von Sicherheits-richtlinien, um Sicherheits-probleme zu erkennen und zu beheben.	• Einheitliche und vereinfachte Sicherheitsabläufe für bewährte Effizienz • Zentraler Überblick über alle Systeme, um die Sicherheitslage schnell und den Schutz in Echtzeit zu analysieren • Schnelle Bereitstellung und Verwaltung von Intel Security-Schutzmaßnahmen mit individueller Richtlinienerzwingung • Verkürzung der Zeit vom Erhalt der Information bis zur Reaktion – mit dynamischen automatisierten Abfragen, Dashboards und Reaktionen	• Detaillierte Kontrolle, geringere Kosten und schnellere Verwaltung von Sicherheitsabläufen mit einer einzigen Konsole • Drag & Drop-Dashboards bieten besseren Echtzeit-überblick über das gesamte Ökosystem • Offene Plattform-SDKs (Software Development Kits) ermöglichen schnelle Implementierung zukünftiger Sicherheits-innovationen	√	√

Komponente	Vorteil	Kundenvorteile	Differenzierung	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Active Response	Bietet proaktive Bedrohungs-übersicht, Zeitpläne, aktuelle und ältere Suchergebnisse sowie Erkennung mit der Möglichkeit, sofort Maßnahmen zu treffen und den Schutz anzupassen.	• Schnelle Suche in aktuellen und älteren Bedrohungsdaten, um den vollständigen Umfang eines Angriffs zu ermitteln, die Untersuchungen zu beschleunigen sowie die Reaktionszeit zu verkürzen • Automatisierte Bedrohungs-reaktionen und stets aktueller Sicherheitsschutz ohne manuelle Eingriffe • Zuweisung einer höheren Priorität zu schwerwiegenden Bedrohungen • Nutzung kontinuierlicher Überwachung und anpassbarer Erfassung zur Tiefensuche nach Angriffsindikatoren, die nicht nur ausgeführt werden oder ruhen, sondern sogar schon gelöscht wurden	• Sofortiger Überblick über alle unbekannten Exploit-Versuche sowie riskanten Verhaltensweisen, die in der Umgebung ausgeführt werden und nicht von Schutztechnologien entdeckt wurden • Untersuchung der Zeitpläne von Ereignissen auf jedem Endgerät mit integrierter Live-Suche auf allen Endgeräten zum Aufspüren von Bedrohungen • Mit einem einzigen Mausklick gestartete Aktionen zum Schützen, Korrigieren sowie Anpassen, sodass statt mehrerer Tools und Schritte eine einzige Operation nötig ist		✓

Spezifikationen

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Unterstützte Plattformen: • Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary • Mac OS X, Version 10.5 oder höher • Linux: RHEL, SUSE, CentOS, OEL, Amazon Linux und neueste Ubuntu-Versionen **Server:** • Windows Server (2003 SP2 oder höher, 2008 SP2 oder höher, 2012), Windows Server 2016 • Windows Embedded (Standard 2009, Point of Service 1.1 SP3 oder höher) • CitrixXen • Citrix XenApp 5.0 oder höher	**Unterstützte Plattformen:** • Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary • RedHat 6.5 • CentOS 6.5 • Windows Server 2008, 2012, 2016

1. McAfee Endpoint Threat Defense and Response nutzt in den USA gehostete Rechenzentren, in denen die Kundenauthentifizierung durchgeführt, die Dateireputation überprüft und Daten gespeichert werden, die für die Erkennung sowie Beseitigung verdächtiger Dateien relevant sind. Die Cloud-Anbindung ist für die Funktion zur dynamischen Eindämmung von Anwendungsprozessen zwar nicht zwingend erforderlich, zur optimalen Nutzung jedoch unerlässlich. Für den vollständigen Funktionsumfang der dynamischen Eindämmung von Anwendungsprozessen sowie von McAfee Active Response und Real Protect sind Cloud-Zugang und aktiver Support notwendig. Zudem gelten die Cloud-Service-Geschäftsbedingungen.

Weitere Informationen

Weitere Informationen zu den Vorteilen von McAfee Endpoint Threat Defense finden Sie unter **www.mcafee.com/de/products/endpoint-threat-defense.aspx**.

Weitere Informationen zu den Vorteilen von McAfee Endpoint Threat Defense and Response finden Sie unter **www.mcafee.com/de/products/endpoint-threat-defense-response.aspx**.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com