



McAfee Advanced Threat Defense

Erkennung hochentwickelter gezielter Angriffe

Als Teil der Intel Security®-Produktpalette ermöglicht McAfee® Advanced Threat Defense Unternehmen die Erkennung aktueller hochentwickelter und gezielter Angriffe sowie die Nutzung von Bedrohungsinformationen für sofortige Gegenmaßnahmen. Im Gegensatz zu herkömmlichen Sandbox-Analysefunktionen besitzt diese Lösung zusätzliche Untersuchungs-funktionen, die die Erkennungsmöglichkeiten erweitern und auf diese Weise Stealth-Bedrohungen aufdecken. Die enge Vernetzung der Intel Security-Lösungen, die alle Bereiche vom Netzwerk bis zu den Endgeräten abdecken, ermöglicht den Sofort austausch von Bedrohungsdaten in der gesamten Umgebung, wodurch die Schutz-sowie Untersuchungsmöglichkeiten erweitert werden. Die flexiblen Bereitstellungsoptionen unterstützen jede Netzwerkkonfiguration.

Wichtigste Vorteile von McAfee Advanced Threat Defense

Starke Vernetzung der Intel Security-Lösungen

- Schließung der Schutzlücke zwischen Entdeckung und Eindämmung sowie Schutz für das gesamte Unternehmen
- Optimierung von Arbeitsabläufen für schnellere Reaktionen und Behebungsmaßnahmen

Leistungsstarke Analysefunktionen

- Starke Entpackfunktionen zur besseren und vollständigeren Analyse
- Kombination aus gründlicher Code-Überprüfung und dynamischer Analyse für genauere Erkennung durch einzigartige Analysedaten

Flexible, zentrale Bereitstellung

- Niedrigere Kosten durch zentrale Bereitstellung und Unterstützung mehrerer Protokolle
- Flexible Bereitstellungsoptionen unterstützen jede Netzwerkkonfiguration

Unsere Technologie hat die Vorgehensweise bei der Erkennung grundlegend verändert, indem fortschrittliche Malware-Analysefunktionen mit vorhandenen Abwehrmaßnahmen kombiniert wurden – von der Netzwerkperipherie bis zum Endgerät. Zudem werden Bedrohungsanalysen in der gesamten IT-Umgebung weitergegeben. Durch die gemeinsame Nutzung der Bedrohungsanalysen in Verwaltungs-, Netzwerk- und Endgerätesystemen unterbrechen unsere Lösungen sofort die Befehls- und Steuerungskommunikation, isolieren kompromittierte Systeme und blockieren weitere Instanzen der gleichen oder ähnlicher Bedrohungen. Darüber hinaus wird geprüft, wo der Schaden aufgetreten sein könnte, und es werden entsprechende Gegenmaßnahmen ergriffen.

McAfee Advanced Threat Defense: Erkennung hochentwickelter Bedrohungen

McAfee Advanced Threat Defense erkennt aktuelle Stealth- und Zero-Day-Malware mithilfe eines innovativen, mehrstufigen Ansatzes. Hierfür verbindet sie Schutzmaßnahmen mit geringem Ressourcenverbrauch – Virenschutzsignaturen, Reputationsdaten und Echtzeitemulation – mit gründlicher Code-Überprüfung sowie dynamischer Analyse (Sandbox), um das tatsächliche Verhalten von Malware zu analysieren. Diese Kombination ergibt die stärkste sowie fortschrittlichste verfügbare Technologie zum Schutz vor hochentwickelter Malware und schafft ein Gleichgewicht zwischen der notwendigen Sicherheit und Leistungsfähigkeit.

Integrierte Lösungen

- McAfee Active Response
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
 - McAfee Application Control
 - McAfee Endpoint Protection
 - McAfee Server Security
- McAfee Web Gateway

Während Methoden mit geringerer Analyselast wie Signaturen und Echtzeitemulation Leistungsvorteile bieten, indem sie bekannte Malware erfassen, ermöglichen die gründliche Code- sowie die Sandbox-Analyse Schutz vor stark getarnten sowie schwer aufspürbaren Bedrohungen. Die Lösung stellt detaillierte Informationen zur Malware-Klassifizierung zur Verfügung und ermöglicht die Einschätzung der Ähnlichkeit mit bekannten Malware-Familien, die Code-Bestandteile wiederverwenden. Sandbox-Umgehungstechniken wie verzögerte oder verborgene Ausführungspfade, die in einer dynamischen Umgebung häufig nicht ausgeführt werden, können durch Entpacken und gründliche Code-Analyse ermittelt werden.

Malware-Autoren nutzen gern Packtechniken, um die Code-Zusammensetzung zu verändern bzw. Code zu verbergen und auf diese Weise die Erkennung zu erschweren. Die meisten Produkte können den gesamten ursprünglichen ausführbaren (Quell-)Code nicht vollständig zur Analyse entpacken. Aus diesem Grund enthält McAfee Advanced Threat Defense umfassende Entpackfunktionen, die Verschleierungstechniken aufheben und so den ausführbaren Original-Code offenlegen. Die Lösung bietet gründliche Code-Analyse, um nicht nur grundlegende Dateiattribute zu untersuchen, sondern auch Anomalien zu erfassen. Dabei werden alle Attribute und Anweisungen auf das resultierende Verhalten untersucht.

Gemeinsam ermöglichen die gründliche, statische Code-Überprüfung und die dynamische Analyse eine vollständige sowie detaillierte Überprüfung auf verdächtige Malware. Die einzigartige Datenanalyse liefert sowohl Übersichtsberichte, mit deren Hilfe Sie das Ausmaß eines Angriffs überblicken und Ihren Maßnahmen Prioritäten zuweisen können, als auch detaillierte Malware-Daten-Berichte.

Erweiterter Schutz

Das Aufspüren hochentwickelter Malware ist wichtig. Doch wenn eine Lösung lediglich einen Bericht liefern oder eine Warnung ausgeben kann, müssen Administratoren unzählige Aufgaben selbst erledigen, und das Netzwerk bleibt ungeschützt.

Durch die starke Integration von McAfee Advanced Threat Defense in Netzwerksicherheitsgeräte – von der Netzwerkperipherie bis zum Endgerät – können sofort Maßnahmen ergriffen werden, sobald McAfee Advanced Threat Defense eine Datei als gefährlich einstuft. Diese starke und automatisierte Integration von Erkennung und Schutz ist unverzichtbar.

McAfee Advanced Threat Defense bietet zwei Integrationsmöglichkeiten: direkt über verschiedene Sicherheitslösungen oder durch McAfee Threat Intelligence Exchange.

Durch die direkte Integration können Intel Security-Sicherheitslösungen sofort Maßnahmen ergreifen, wenn Dateien von McAfee Advanced Threat Defense als gefährlich eingestuft werden. Sie können unverzüglich Bedrohungsdaten in bestehende Prozesse zur Richtlinienerzwingung integrieren und weitere Instanzen der gleichen oder ähnlicher Dateien daran hindern, in das Netzwerk zu gelangen.

Die Erkennungen von McAfee Advanced Threat Defense werden in den Protokollen und Dashboards der integrierten Produkte angezeigt, als wäre die gesamte Analyse in dem jeweiligen Produkt erfolgt. Dadurch werden Arbeitsabläufe optimiert, und Administratoren erhalten die Möglichkeit, Warnungen effizient zu verwalten, indem sie über eine zentrale Benutzeroberfläche arbeiten.

Durch die Integration von McAfee Threat Intelligence Exchange können andere Schutzlösungen, wie zum Beispiel McAfee Endpoint Protection, auf den Funktionsumfang von McAfee Advanced Threat Defense zugreifen. So wird einem breiten Spektrum an integrierten Sicherheitslösungen Zugang zu Analyseergebnissen und Kompromittierungsindikatoren gewährt. Wenn eine Datei von McAfee Advanced Threat Defense überführt wurde, veröffentlicht McAfee Threat Intelligence Exchange diese Bedrohungsinformationen über ein Reputations-Update an alle integrierten Gegenmaßnahmen im Unternehmen.

Endgeräte mit McAfee Threat Intelligence Exchange können Malware-Erstinstallationen blockieren und präventiven Schutz bereitstellen, wenn die Datei später erneut gefunden wird.

Gateways mit McAfee Threat Intelligence Exchange können verhindern, dass die Datei ins Unternehmen gelangt. Außerdem erhalten Endgeräte mit McAfee Threat Intelligence Exchange auch außerhalb des Netzwerks Aktualisierungen zu Dateierkennungen, sodass keine Lücken durch die Out-of-Band-Übertragung von Malware-Code entstehen.

Erkennung kompromittierter Systeme sowie Problembehebung

Zur Behebung von Angriffen benötigen Unternehmen einen umfassenden Überblick mit priorisierten, umsetzbaren Bedrohungsdaten, damit sie bessere Entscheidungen treffen sowie angemessene Reaktionen umsetzen können. McAfee-Lösungen arbeiten zusammen, damit Unternehmen genau den Schutz erhalten, den sie benötigen.

McAfee Enterprise Security Manager erfasst und korreliert detaillierte Datei-Reputationsdaten sowie Ausführungsereignisse von McAfee Advanced Threat Defense und anderen Sicherheitssystemen, um erweiterte Warnfunktionen sowie Verlaufsansichten bereitzustellen, die erweiterte Sicherheitsdaten, Risikopriorisierung und Echtzeitinformationen zur Sicherheitslage ermöglichen. Mit den Kompromittierungsindikator-Daten von McAfee Advanced Threat Defense kann McAfee Enterprise Security Manager bis zu sechs Monate alte Daten durchsuchen, um zu überprüfen, ob Hinweise zu diesen Funden in Netzwerk- oder Systemdaten gefunden werden können. Dabei können Systeme aufgedeckt werden, die zuvor mit neu identifizierten Malware-Quellen kommuniziert haben. McAfee Enterprise Security Manager bietet eine verständliche Darstellung der Risiken, sodass interaktive oder automatisierte Behebungsmaßnahmen sofort umgesetzt werden können. Die enge Verzahnung mit McAfee Endpoint Protection, McAfee Threat Intelligence Exchange und McAfee Active Response optimiert Reaktionen auf Sicherheitsabläufe sowie

den Überblick und ermöglicht Aktionen wie die Veröffentlichung neuer Konfigurationen, Implementierung neuer Richtlinien, Entfernung von Dateien und Ausbringung von Software-Aktualisierungen, die Risiken präventiv beheben können. Da infizierte Endgeräte im Netzwerk automatisch von McAfee Active Response erkannt und in McAfee Advanced Threat Defense-Berichten erfasst werden, können Sie auf einfache Weise fundierte Entscheidungen treffen sowie entsprechende Maßnahmen ergreifen.

Bereitstellung

Die flexiblen Bereitstellungsoptionen von McAfee Advanced Threat Defense unterstützen jede Netzwerkkonfiguration. Die Lösung ist als lokale Hardware-Appliance sowie als virtuelle Appliance verfügbar. In allen Fällen agiert die Lösung als gemeinsam genutzte Ressource zwischen mehreren Intel Security-Lösungen, die durch die kostengünstige Skalierbarkeit die Kosten senkt.

Sicherheitskontrollzentren und Malware-Analysten können McAfee Advanced Threat Defense ebenfalls für Untersuchungen nutzen.

McAfee Advanced Threat Defense bietet zahlreiche hochentwickelte Funktionen, zum Beispiel:

- **Unterstützung benutzerdefinierter Images:** Analysiert Bedrohungen unter den Bedingungen eines bestimmten Host-Profiles.
- **Interaktiver Benutzermodus:** Ermöglicht Analysten die direkte Interaktion mit Malware-Exemplaren.
- **Umfangreiche Entpackfunktionen:** Verkürzen die für Untersuchungen benötigte Zeit von Tagen auf Minuten.
- **Vollständiger Logikpfad:** Ermöglicht tiefgehendere Probenanalysen, da die Ausführung zusätzlicher Logikpfade erzwungen wird, die in typischen Sandbox-Umgebungen ruhend bleiben.

- Einsendung von Exemplaren an mehrere virtuelle Umgebungen: Beschleunigt die Untersuchung, da ermittelt wird, welche Umgebungsvariablen für die Dateiausführung erforderlich sind.
- Detaillierte Berichte zu Disassemblierungsausgaben, Speicherabbildern, Aufrufdiagrammen für Grafikfunktionen, eingebetteten oder gelöschten Dateiinformationen, API-Protokollen der Benutzer und PCAP-Informationen: Bietet wichtige Informationen zur Untersuchung durch Analysten.

Wenn Sie weitere Informationen wünschen oder McAfee Advanced Threat Defense evaluieren möchten, wenden Sie sich bitte an Ihren Vertriebsrepräsentanten, oder besuchen Sie www.mcafee.com/de/products/advanced-threat-defense.aspx.

Details zu McAfee Advanced Threat Defense

Formfaktoren der physischen Appliance	ATD-3000 1 HE-Rackmontage	ATD-6000 2 HE-Rackmontage
Formfaktoren der virtuellen Appliance	v1008, v1016, v3032, v6064 ESXi 6.0	v1008, v1016, v3032, v6064 ESXi 6.0

Erkennung

Unterstützte Dateitypen	PE-Dateien, Adobe-Dateien, Microsoft Office Suite-Dateien, Bilddateien, Archive, Java, Android APK-Dateien, URLs
Analysemethoden	McAfee Anti-Malware Engine, GTI-Dateireputation: Datei/URL/IP-Adresse, Gateway Anti-Malware (Emulation und Verhaltensanalyse), dynamische Analyse (Sandbox), gründliche Code-Analyse, benutzerdefinierte YARA-Regeln
Unterstützte Betriebssysteme	Windows 10 (64-Bit), Windows 8.1 (64-Bit), Windows 8 (32-Bit/64-Bit), Windows 7 (32-Bit/64-Bit), Windows XP (32-Bit/64-Bit), Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Alle Sprachversionen der Windows-Betriebssysteme werden unterstützt.
Ausgabeformate	STIX, OpenIOC, XML, JSON, HTML, PDF, Text
Übertragungsmethoden	Integrierte Produkte, direkt/manuell, per API



McAfee. Part of Intel Security.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

Intel und die Intel- und McAfee-Logos, ePolicy Orchestrator und McAfee ePO sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Copyright © 2016 Intel Corporation. 1765_1016 OKTOBER 2016