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 Untersuchungsfunktionen, 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 Sofortaustausch von Bedrohungsdaten in der gesamten Umgebung, wodurch die Schutz- sowie Untersuchungsmöglichkeiten erweitert werden.

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 statischer Code-Überprüfung und dynamischer Analyse für genauere Erkennung durch einmalige Analysedaten

Zentrale Malware-Analyse

- Kostensenkung durch Verringerung der benötigten Geräte im Netzwerk dank gemeinsamer Analysen
- Vereinfachte Bereitstellung

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. Dabei verbindet die Lösung Schutzmaßnahmen mit geringem Ressourcenverbrauch – Virenschutzsignaturen, Reputationsdaten und Echtzeitemulation – mit gründlicher statischer 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.

Während Methoden mit geringerer Analyselast wie Signaturen und Echtzeitemulation Leistungsvorteile bieten, indem sie bekannte Malware erfassen, ermöglichen die vollständige statische Code- sowie die Sandbox-Analyse Schutz vor stark getarnten sowie schwer aufzuspürenden Bedrohungen. Die Lösung stellt detaillierte Informationen zur Malware-Klassifizierung zur Verfügung und ermöglicht die Identifizierung von verwandter Malware, die Code-Bestandteile wiederverwendet. Sandbox-Umgehungstechniken wie verzögerte oder verborgene Ausführungspfade, die in einer

intel Security

Integrierte Lösungen

- **McAfee Email Gateway**
- **McAfee Enterprise Security Manager**
- **McAfee ePolicy Orchestrator**
- **McAfee Network Security Platform**
- **McAfee Next Generation Firewall**
- **McAfee Threat Intelligence Exchange**
- **McAfee Web Gateway**

dynamischen Umgebung häufig nicht ausgeführt werden, können durch Entpacken und vollständige statische 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 statische 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 statische Code-Überprüfung und die dynamische Analyse eine vollständige sowie detaillierte Überprüfung auf verdächtige Malware.

Zielspezifische Sandbox-Analyse verbessert die Erkennungsleistung

Administratoren erhalten die Möglichkeit, Objekte in unterschiedliche benutzerdefinierte virtuelle Maschinen oder Gold-Abbilder hochzuladen und zu analysieren. Dadurch können Unternehmen Bedrohungen unter den Bedingungen des tatsächlichen Host-Profils analysieren, anstatt dazu auf ein generisches Abbild zurückgreifen zu müssen, und zudem eine genauere Risikoanalyse durchführen.

Da ein Unternehmen über unterschiedliche Host-Profile verfügen kann, die im gleichen Netzwerk aktiv sind, kontaktiert McAfee Advanced Threat Defense die Software McAfee ePolicy Orchestrator® (McAfee ePO™), um das Betriebssystem sowie die Liste der Anwendungen abzurufen. Anschließend werden lediglich die verdächtigen Dateien unter den Bedingungen des Ziel-Hosts analysiert.

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 immer noch 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 Installationen mit Malware-Erstinfektionen 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 Lösungen, die einen umfassenden Überblick mit priorisierten, umsetzbaren Bedrohungsdaten bieten und dadurch bessere Entscheidungen sowie angemessene Reaktionen ermöglichen. McAfee Enterprise Security Manager, McAfee Endpoint Protection und McAfee Threat Intelligence Exchange agieren eng verzahnt, um Unternehmen bestmöglich zu unterstützen.

McAfee Enterprise Security Manager erfasst und korreliert detaillierte Datei-Reputationsdaten sowie Ausführungsereignisse von McAfee Advanced Threat Defense und anderen Sicherheitssystemen, um erweiterte Warnfunktionen und Verlaufsansichten bereitzustellen, die erweiterte Sicherheitsdaten, Risikopriorisierung und Echtzeitinformationen zur Sicherheitslage ermöglichen. Die Lösung überwacht Basislinien für Endgeräteereignisse, um bei erheblichen Abweichungen von etablierten Schwellenwerten dynamisch zu agieren und die Risiken für Benutzer und Ressourcen zu minimieren. 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 und McAfee Threat Intelligence Exchange ermöglicht Aktionen wie die Veröffentlichung neuer Konfigurationen, Implementierung neuer Richtlinien, Entfernung von Dateien und Ausbringung von Software-Aktualisierungen, die Risiken präventiv beheben können.

Bereitstellung

McAfee Advanced Threat Defense ist eine zentral bereitgestellte Appliance zur fortschrittlichen Malware-Analyse, die sich nahtlos in Ihre vorhandene McAfee-Sicherheitsumgebung integriert. McAfee Advanced Threat Defense agiert dabei als gemeinsam genutzte Ressource zwischen mehreren Intel Security-Netzwerkgeräten und skaliert dadurch kostengünstig mit der Größe des gesamten Netzwerks. Sicherheits-Kontrollzentren und Malware-Analysten können McAfee Advanced Threat Defense für Untersuchungen mit manuellen Eingabemöglichkeiten nutzen. Umfassende Entpackfunktionen verkürzen die für Untersuchungen benötigte Zeit von Tagen auf Minuten. Und während die Übersichtsberichte von McAfee Advanced Threat Defense das allgemeine Verständnis der Bedrohung sowie die Priorisierung von Maßnahmen erleichtern, bieten detaillierte Zusatzberichte wichtige Informationen für Untersuchungen durch Analysten – beispielsweise zu den Ergebnissen der Disassemblierung, zu eingebetteten oder entfernten Dateiinformationen sowie in grafischen Aufrufdiagrammen.

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

Details zu McAfee Advanced Threat Defense	**ATD-3000**	**ATD-6000**
Formfaktor	1 HE-Rackmontage	2 HE-Rackmontage
Leistung	Bis zu 150.000 Objekte pro Tag	Bis zu 250.000 Objekte pro Tag
Erkennung	**ATD-3000/ATD-6000**	
Unterstützte Datei-/Medientypen	PE-Dateien, Adobe-Dateien, Microsoft Office-Dateien, Archive, Java, Android APK-Dateien	
Analysemethoden	McAfee Anti-Malware Engine, McAfee GTI-Dateireputation, Gateway Anti-Malware (Emulation und Verhaltensanalyse), dynamische Analyse (Sandbox), statische Code-Analyse	
Unterstützte Betriebssysteme	Windows 8 (32-Bit/64-Bit), Windows 7 (32-Bit/64-Bit), Windows XP (32-Bit/64-Bit), Windows Server 2003, Windows Server 2008 (64-Bit), Android	

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