Abwehr hochentwickelter Bedrohungen für Netzwerk-Eindringungsschutzsysteme

Umfassender Schutz vor Stealth-Malware

Hauptvorteile

- Automatisches Finden, Stoppen und Beheben von hochentwickelter Malware und Stealth-Angriffen, die sich im Netzwerkverkehr verstecken
- Ergänzung der Netzwerksicherheit um echte statische Code- und zielspezifische Sandbox-Analyse ohne zusätzliche Belastung der Eindringungsschutzsysteme
- Plug-and-Play-Blockierung von Bedrohungen ohne Verzögerungen durch erforderliche Benutzereingriffe

Das netzwerkbasierte Eindringungsschutzsystem (IPS) ist eine Hauptsäule der Sicherheitsarchitekturen von Unternehmen. Dabei werden die IPS-Systeme per In-Band-Bereitstellung und zusammen mit Gateways sowie hostbasierten Sicherheitsmaßnahmen eingesetzt. Sie überwachen den Netzwerkverkehr und das Endgeräteverhalten mithilfe verschiedenster Techniken, um Angriffe zu erkennen und Abwehrmaßnahmen zu ergreifen.

Heute gelingt es allerdings einer wachsenden Zahl unbekannter Zero-Day-Bedrohungen, die herkömmlichen Schutzmaßnahmen erfolgreich zu umgehen. Diese raffinierten, gut getarnten und höchst anpassungsfähigen Stealth-Angriffe mit oftmals genauester Zielorientierung machen zwar einen kleinen, dafür aber unverhältnismäßig gefährlichen und kostspieligen Teil der sich ständig ändernden Bedrohungen aus.

Als Reaktion auf diese Entwicklung ergänzen einige Unternehmen ihre IPS-Infrastruktur um dynamische Analysen in Form von Out-of-Band-Sandbox-Appliances. Die Sandbox startet verdächtige ausführbare Dateien in einer abgesicherten virtuellen Umgebung und überwacht deren Ausführungsverhalten, um böswillige Absichten zu erkennen. Oft geht dieser Vorsprung bei der Erkennungsgenauigkeit jedoch aufgrund mangelhafter Integration und manueller Reaktionsprozesse schnell verloren.

Die meisten Sandbox-Appliances von Drittanbietern können Sicherheitsanalysten bei einem neuen Angriff beispielsweise nur alarmieren. Es ist dann die Aufgabe der Analysten, manuell neue Blockierungsregeln für das Eindringungsschutzsystem sowie die Firewall zu erstellen, alle während der Out-of-Band-Sandbox-Analyse kompromittierten Endgeräte zu ermitteln und die Probleme darauf zu beheben. Zudem müssen die vorhandenen Lösungen häufig mit folgenden Einschränkungen kämpfen:

- Pro IPS-Sensor ist eine Sandbox-Appliance erforderlich, was immense Kosten verursacht.
- Die Kunden vertrauen auf eine generische virtuelle Arbeitsumgebung, in der zielspezifisches Angriffsverhalten übersehen werden kann.
- Die Kunden verlassen sich nur auf dynamische Analysen, wodurch die Sandbox anfällig ist für verschiedene Malware-Strategien zur Erkennung sicherer Umgebungen und Verzögerung des Beginns ihres böswilligen Verhaltens.

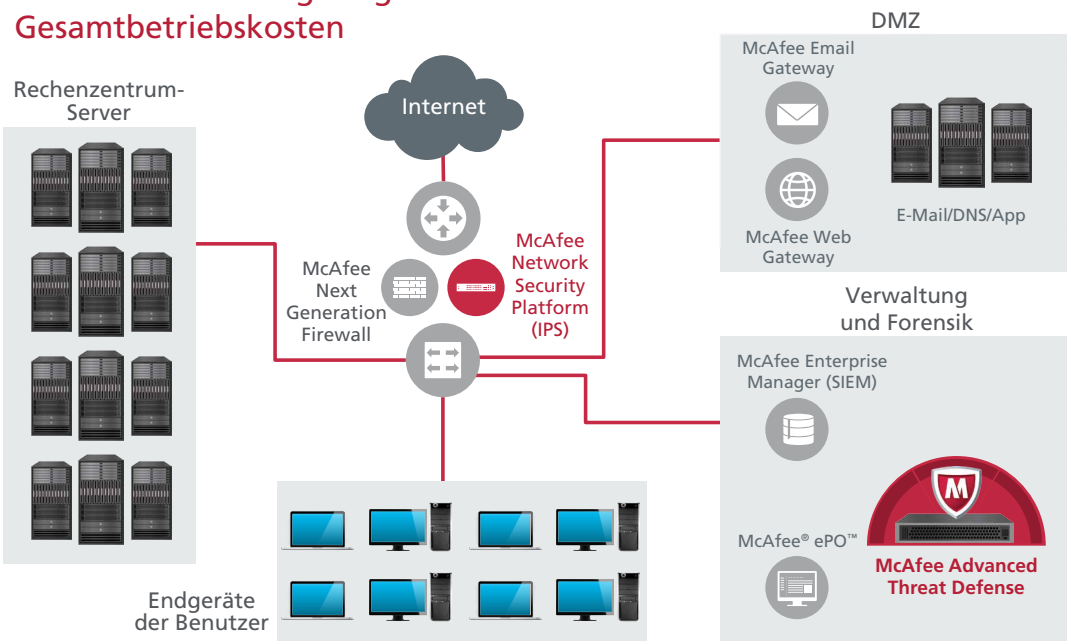
Eine IPS- und Sandbox-Lösung im Rahmen des Security Connected-Ansatzes

McAfee bietet eine Lösung für alle diese Herausforderungen: die nahtlos integrierte Kombination aus McAfee Network Security Platform, einem hochleistungsfähigen modernen IPS-Sensor, und McAfee Advanced Threat Defense, der branchenweit leistungsstärksten und umfassendsten Appliance zur Erkennung hochentwickelter Malware. McAfee Network Security Platform ermöglicht die In-Band-Datenverkehrsuntersuchung und Blockierung von Bedrohungen mit einer Reihe von Technologien zur Malware-Erkennung, die für die Ausführung in Echtzeit optimiert sind. Mit McAfee Advanced Threat Defense erhalten Sie einen umfangreicheren und ressourcenintensiveren Satz an Analysen, der sowohl zielspezifische Sandbox- als auch echte statische Code-Analysen umfasst. Gemeinsam finden und stoppen diese beiden Lösungen alle neuen, unbekannten sowie hochentwickelten Stealth-Bedrohungen. Durch die Ergänzung um Real Time for McAfee ePO™ können Sie alle von hochentwickelter Malware betroffenen Systeme schnell erkennen und die Probleme darauf beheben.

- *Finden:* Die innovativen Analysetechnologien erkennen gemeinsam, schnell und zuverlässig raffinierte Bedrohungen in den verschiedenen Protokollen.
- *Stoppen:* Die eng verzahnten McAfee-Sicherheitsprodukte blockieren Eindringungsversuche sofort und isolieren so infizierte Endgeräte.
- *Beheben:* Die McAfee-Lösung grenzt eine neu entdeckte Infiltration in der Umgebung automatisch ab und startet die Problembehebung auf dem Endgerät.

Zentrale Bereitstellung

Skalierbarkeit und geringere Gesamtbetriebskosten



Da McAfee Advanced Threat Defense für Netzwerk-Eindringungsschutzsysteme im Rahmen des Security Connected-Ansatzes die Integration der Unternehmenssicherheitslösungen ermöglicht, können Sie eine Reihe branchenweit einmaliger operative und Schutzvorteile nutzen. Dazu zählen:

- *Plug-and-Play-Blockierung von Bedrohungen:* Von McAfee Advanced Threat Defense erkannte Angriffe werden durch McAfee Network Security Platform automatisch blockiert, ohne dass auf einen Benutzereingriff gewartet werden muss bzw. ein Benutzereingriff an sich notwendig ist.
- *Bericht- und Workflow-Integration:* Von McAfee Advanced Threat Defense generierte Berichte werden automatisch in die McAfee Network Security Platform-Workflows integriert, sodass Sie während der Untersuchungen nicht mehr zwischen Bildschirmen wechseln müssen.
- *Überblick über Endgeräte:* McAfee Advanced Threat Defense hat Zugang zu allen in McAfee Network Security Platform gespeicherten Endgerätedaten und kann sie nutzen, um Bedrohungen schneller sowie präziser zu erkennen.

Besser im Verbund

- Bessere Nutzung vorhandener Sicherheitslösungen
- Weniger Umstrukturierungen der Netzwerkarchitektur
- Erweiterter und automatisierter Schutz
- Weniger Problembehebungen und Untersuchungen dank zuverlässiger Inline-Blockierung
- Workflow-Optimierung dank McAfee Network Security Platform-Schnittstelle

Security Connected

Die Security Connected-Plattform von McAfee bietet ein einheitliches Framework für hunderte Produkte, Services und Partner, damit diese voneinander lernen, kontextspezifische Daten in Echtzeit austauschen sowie als Team agieren, um somit die Sicherheit von Informationen sowie Netzwerken gewährleisten zu können. Dank des innovativen Konzepts, der optimierten Prozesse sowie der praktischen Empfehlungen, durch die sich diese Plattform auszeichnet, kann jedes Unternehmen nicht nur den Zeitaufwand für Erkennung und Reaktion reduzieren, sondern gleichzeitig den Verwaltungsaufwand minimieren und die Betriebskosten senken.

Die IPS-Lösung: McAfee Network Security Platform

McAfee Network Security Platform umfasst eine Reihe integrierter Eindringungsschutz-Appliances, die raffinierte Bedrohungen – einschließlich hochentwickelter Malware, Zero-Day-Bedrohungen, DoS-Angriffe und Botnets – erkennen sowie blockieren. Dank der Kombination aus äußerst effizienter Architektur für tiefgehende Untersuchungen in einem Durchlauf und speziell entwickelter Hardware auf Netzanbieterniveau bietet McAfee Network Security Platform Verbindungsgeschwindigkeiten von 40 Gbit/s mit einem einzelnen Gerät. Darüber hinaus gewährt die Plattform-Lösung unabhängig von den Sicherheitseinstellungen außergewöhnliche Durchsatzraten und Genauigkeit. Integrierte Bedrohungsanalysefunktionen umfassen neben anpassbaren Signaturen und vollständiger Protokollanalyse auch Bedrohungsreputationsdaten, intensive Dateianalysen mit Emulation und JavaScript-Erkennung sowie die Korrelation zwischen Verhalten und Anwendungsnutzung basierend auf Layer-7-Daten zu mehr als 1.500 Anwendungen und Protokollen.

Die wohl größte Stärke von McAfee Network Security Platform ist jedoch die Möglichkeit zur Integration sowie Nutzung der Daten und Fähigkeiten anderer McAfee-Sicherheitslösungen. Besonders wichtig ist dabei die nahtlose Integration folgender Produkte:

- Real Time for McAfee® ePolicy Orchestrator® (McAfee ePO) bietet die Echtzeittransparenz von Endgeräten und den Verwaltungszugang, die für die Isolierung und Behebung erfolgreicher Angriffe notwendig sind.
- McAfee Enterprise Security Manager ist eine revolutionäre SIEM-Lösung (Sicherheitsinformations- und Ereignis-Management), die Echtzeitüberblick über die interne IT-Umgebung liefert und diese Daten mit externen Kontextinformationen kombiniert sowie korreliert. Die hochoptimierte McAfee Enterprise Security Manager-Datenbank erfasst Milliarden Protokollereignisse, die mit anderen relevanten Datenströmen in Beziehung gesetzt werden, sodass Sicherheitsereignisdaten von mehreren Jahren sofort zur Verfügung stehen. Die Lösung berechnet die Basiswerte für alle eingehenden Datenströme, um Anomalien und potenzielle Bedrohungen zu erkennen, bevor sie sich entwickeln. Darüber hinaus wird die Compliance-Verwaltung durch hunderte vorinstallierte Dashboards und auftragsspezifische Berichte vereinfacht.
- McAfee Advanced Threat Defense übernimmt hierbei die Erkennung hochentwickelter Malware.

Die Sandbox-Lösung: McAfee Advanced Threat Defense

McAfee Advanced Threat Defense ist eine mehrstufige Malware-Erkennungslösung, die eine Reihe erweiterbarer Untersuchungsmodule und Analysefunktionen – abgestuft nach Rechenaufwand – hintereinanderschaltet. Dieser einzigartige Ansatz für umfassende und dennoch effiziente Bewertungen ermöglicht sehr hohe Erkennungsgenauigkeit und Zuverlässigkeit bei äußerst hohen Durchsatzraten. Folgende integrierte Analysen werden von McAfee Advanced Threat Defense angewendet:

- Signaturbasierte Erkennung von Viren, Würmern, Spyware, Bots, Trojanern, Buffer Overflows sowie komplexen Angriffen mithilfe einer umfassenden, von McAfee Labs erstellten und verwalteten KnowledgeBase mit derzeit fast 150 Millionen Signaturen.
- Reputationsbasierte Erkennung mithilfe des McAfee Global Threat Intelligence-Netzwerks zur Erkennung neuer Bedrohungen.
- Statische Echtzeitanalyse und Emulation zur schnellen Erkennung von Malware und Zero-Day-Bedrohungen, die von signatur- oder reputationsbasierten Verfahren nicht erkannt werden.
- Vollständige statische Code-Analyse, die ein Reverse Engineering des Datei-Codes durchführt, um alle Attribute und Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen. Umfassende Entpackungsfunktionen öffnen alle Arten gepackter und komprimierter Dateien für eine vollständige Analyse und Malware-Klassifizierung, damit Unternehmen die spezielle Malware, mit der sie es zu tun haben und die Auswirkungen auf das Unternehmen besser verstehen. Dank vollständiger statischer Code-Analyse erhalten Sie wichtige Einblicke in Eingabe-abhängiges Verhalten und verzögerte oder verborgene Ausführungspfade, die während dynamischer Analysen oft nicht ausgeführt und von weniger umfassenden Sandbox-Lösungen übersehen werden.
- Dynamische Sandbox-Analyse, die den Datei-Code in einer virtuellen Ausführungsumgebung ausführt und sein Verhalten beobachtet. Als einzige der aktuellen Sandbox-Lösungen konfiguriert McAfee Advanced Threat Defense virtuelle Ausführungsumgebungen so, dass sie den Ziel-Host gemäß Abfragen der McAfee ePO-Software abbilden. Dank der Dateiverhaltensanalyse unter den genau gleichen Bedingungen wie auf dem anvisierten Host erhalten Sie schnell und effizient zuverlässige Ergebnisse, die böswilliges Verhalten aufdecken, das in einer generischen Umgebung möglicherweise nicht ausgelöst werden würde. Da viele hochentwickelte Angriffe dafür ausgelegt sind, der Erkennung während der Sandbox-Analyse zu entgehen, umfasst McAfee Advanced Threat Defense innovative Techniken, um die Code-Ausführung während der dynamischen Analyse sicherzustellen.

Die Techniken arbeiten koordiniert zusammen, um viele bekannte und unbekannte Malware-Arten effizient zu erkennen. Die Kombination aus vollständiger statischer und dynamischer Analyse erkennt verschleierte, hochentwickelte Malware, die durch einfache Analysen nicht sicher bestimmt werden kann.

McAfee Advanced Threat Defense-Appliances lassen sich problemlos so konfigurieren, dass nur die nicht auf Upstream-IPS-Sensoren durchgeführten Analysen angewendet und damit redundante Überprüfungen vermieden werden. Die Durchsatzkapazitäten der Appliances können auf bis zu 250.000 Objekte pro Tag skaliert werden, wodurch Sie ein fortschrittliches Malware-System zur Unterstützung mehrerer McAfee Network Security Platform-Sensoren erhalten. Zusammen mit McAfee Network Security Platform werden die McAfee Advanced Threat Defense-Appliances zentral über die von McAfee Network Security Manager bereitgestellte webbasierte Schnittstelle verwaltet.

Effiziente, geschlossene Lösung zum Schutz vor hochentwickelten Bedrohungen

Dank der Kombination von McAfee Network Security Platform und McAfee Advanced Threat Defense erhalten Sie äußert effizienten Netzwerk-Eindringungsschutz sowie besonders effektive Erkennung und Reaktion auf hochentwickelte Malware. Diese automatisierte und geschlossene Lösung findet raffinierte Angriffe, blockiert sie umgehend und behebt die Probleme der betroffenen Host-Systeme ohne manuellen Eingriff durch überarbeitete Netzwerkverantwortliche oder Sicherheitsanalysten.

Weitere Informationen dazu, wie McAfee-Lösungen Ihr Netzwerk vor hochentwickelten Stealth-Bedrohungen schützen können, erhalten Sie von Ihrem McAfee-Vertriebsrepräsentanten oder unter www.mcafee.com/de/products/advanced-threat-defense.aspx.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

61051brf_atd-network-ips_0514_fnl_ETMG