McAfee Network Security Platform

Ein umfassender, intelligenter Ansatz für Netzwerksicherheit

Das Eindringungsschutzsystem (IPS) der nächsten Generation McAfee® Network Security Platform (McAfee NSP) erkennt und blockiert hochentwickelte Malware-Bedrohungen im gesamten Netzwerk. Die Lösung nutzt hochentwickelte Erkennungs- und Emulationstechniken, die über einfachen Musterabgleich hinausgehen und äußerst zuverlässigen Schutz vor heimlichen Angriffen bieten. Um die Anforderungen anspruchsvoller Netzwerke zu erfüllen, kann die Plattform mit nur einem Gerät auf mehr als 40 Gbit/s skaliert werden. Das integrierte McAfee-Lösungsportfolio vereinfacht die Sicherheitsverwaltung durch die Kombination von Echtzeit-Feeds von McAfee Global Threat Intelligence mit umfangreichen Kontextdaten zu Benutzern, Geräten und Anwendungen, damit Sie schnell und präzise auf Angriffe über das Netzwerk reagieren können. Dadurch erreichen Sie optimierte Sicherheitsabläufe.

Hauptvorteile

- Schnelle Erkennung und Blockierung von Bedrohungen zum Schutz von Anwendungen und Daten
- Skalierbare Hochleistungslösung für dynamische Umgebungen
- Zentrale Verwaltung für mehr Transparenz und Kontrolle
- Hochentwickelte Erkennungsfunktionen, einschließlich signaturloser Malware-Analysen

Schutz vor aktuellen verborgenen Bedrohungen

Ihr Netzwerk ist hochentwickelten, verborgenen Angriffen ausgesetzt, die herkömmlichen Entdeckungsmethoden entgehen können. Dadurch sind Ihre Anwendungen und Daten von schwerwiegenden Kompromittierungen und Ausfällen bedroht. Leider fehlen den meisten Unternehmen die finanziellen sowie betrieblichen Ressourcen für die Implementierung und Verwaltung der Tools und Technologien, die für die Gewährleistung von ausreichendem Schutz erforderlich sind.

McAfee NSP kombiniert intelligenten Bedrohungsschutz mit intuitiver Sicherheitsverwaltung, um die Erkennungsgenauigkeit zu verbessern und die Sicherheitsabläufe zu optimieren. Keine einzelne Technologie zur Malware-Erkennung ist im Stande, sämtliche Angriffe abzuwehren. Aus diesem Grund vereint McAfee NSP mehrere fortschrittliche Techniken zur Malware-Analyse, um zu verhindern, dass unerwünschte Malware Ihr Netzwerk beschädigt. Die Lösung führt tiefergehende Untersuchungen des Netzwerkverkehrs durch. Dazu setzt sie auf eine Kombination fortschrittlicher Untersuchungstechniken zur Erkennung sowie Abwehr von Malware-Callbacks, Denial-of-Service (DoS)- sowie Zero-Day-Angriffen und anderen Bedrohungen. Diese Techniken umfassen unter anderem vollständige Protokollanalysen, Bedrohungsreputation und Verhaltensanalysen.

NSS LABS RECOMMENDED

Folgen Sie uns

Integrierte Sicherheit

McAfee Network Security Platform integriert die Lösung McAfee Advanced Threat Defense, die gründliche statische und dynamische (Malware-Sandbox-)Analysen sowie Machine Learning kombiniert, um Zero-Day-Bedrohungen sowie solche Bedrohungen zu erkennen, die Umgehungstechniken und Ransomware nutzen. McAfee NSP berücksichtigt zudem die Dateireputation von McAfee Global Threat Intelligence und kann McAfee® ePolicy Orchestrator® sowie McAfee Enterprise Security Manager integrieren, um die Netzwerkereignisse aller relevanten Quellen in Echtzeit korrelieren zu können. Die kombinierte Lösung verarbeitet Gerätedetails, Benutzerinformationen, die Sicherheitslage von Endgeräten, Schwachstellenanalysen sowie weitere umfangreiche Informationen und hilft Unternehmen auf diese Weise, den Schweregrad von Bedrohungen sowie Risikofaktoren für den Geschäftsbetrieb zu erkennen.

Leistung und Verfügbarkeit

Wenn Sie Sicherheit und hohe Leistung wünschen, ist McAfee Network Security Platform die richtige Antwort. Diese Lösung verbindet eine Architektur für in einem Durchlauf erfolgende protokollbasierte Untersuchungen mit speziell entwickelter Hardware auf Netzanbieterniveau. Dadurch erreicht sie einen Nettodurchsatz von mehr als 40 Gbit/s pro Appliance.

Die effiziente Architektur garantiert unabhängig von den Sicherheitseinstellungen gleichbleibend hohe Leistung, während der Durchsatz bei anderen IPS-Lösungen um bis zu 50 Prozent sinkt, wenn innerhalb der Richtlinien Sicherheit statt Leistung im Mittelpunkt steht.

McAfee NSP bietet zudem Active-Active- und Active-Passive-Cluster mit statusbasiertem Failover, sodass Sie Hochverfügbarkeits-SLAs einhalten und gleichzeitig Engpässe durch langsame Appliances oder überlastete eigenständige Lösungen vermeiden können.

Transparenz und Kontrolle

Treffen Sie fundierte Entscheidungen zu den Anwendungen und Protokollen in Ihrem Netzwerk. Die McAfee Network Security Platform ist die erste und einzige IPS-Lösung, die erweiterten Bedrohungsschutz und Anwendungserkennung in einem einzigen Modul für Sicherheitsentscheidungen kombiniert. Die Platform korreliert Bedrohungsaktivitäten mit der Anwendungsnutzung (basierend auf Layer-7-Daten zu mehr als 1.500 Anwendungen und Protokollen). Dadurch können Sie fundiertere Entscheidungen dazu treffen, welche Anwendungen Sie in Ihrem Netzwerk zulassen.

Mit McAfee NSP erhalten Sie nicht nur einen Überblick über die eingesetzten Anwendungen, sondern auch über die Benutzer und Geräte. Dabei werden risikoreiche Hosts sowie Benutzer priorisiert und dank der Erkennung von anormalem Netzwerkverhalten auch aktive Botnets erfasst.

Hauptvorteile (Fortsetzung)

- Entschlüsselung ein- und ausgehender SSL-Verbindungen zur Untersuchung des Netzwerkverkehrs
- Hochverfügbarkeit und Datenwiederherstellung
- Virtuelle Appliance-Modelle verfügbar
- Integration in McAfee-Lösungsportfolio für Gerät-zu-Cloud-Sicherheit

Intelligente, skalierbare Sicherheitsverwaltung

Die intelligente Netzwerk-Sicherheitsverwaltung ermöglicht die optimale Nutzung Ihrer Sicherheitsinvestition. Der webbasierte McAfee Network Security Manager ist skalierbar und kann eine beliebige Anzahl von Sicherheits-Appliances verwalten. Er bietet intuitive Arbeitsprozesse für rückwirkende Entdeckungen, die Administratoren auf relevante Ereignisse hinweisen, sowie benutzerfreundliche Sicherheits-Dashboards, die Ereignisse anhand des Schweregrads und der Relevanz automatisch priorisieren.

Zusätzliche Funktionen

Schutz vor hochentwickelten Bedrohungen

- Entschlüsselung von eingehendem SSL-Datenverkehr (Secure Sockets Layer) unterstützt Diffie-Hellman (DH)- und Elliptic-Curve Diffie–Hellman (ECDH)-Verschlüsselungen durch eine agentenbasierte, freigegebene Schlüssellösung, die die Sensorleistung nicht beeinträchtigt (zum Patent angemeldet, für NS-Serie)
- Entschlüsselung ausgehender SSL-Verbindungen (NS-Serie)
- Emulationsmodul McAfee Gateway Anti-Malware Engine
- Modul zur Emulation von JavaScript in PDF-Dateien
- Modul zur Adobe Flash-Verhaltensanalyse
- Erweiterter Umgehungsschutz
- Analyse der Reputation von Mobilgerätebedrohungen und Cloud-Anwendungen

Schutz vor Botnets und Malware-Callbacks

- Erkennung von DNS/DGA Fast Flux-Callbacks
- DNS-Server-Sinkholes
- Heuristische Bot-Erkennung
- Korrelation unterschiedlicher Angriffe
- Zentrale Steuerungsdatenbank

Erweiterter Eindringungsschutz

- IP-Defragmentierung und Neuordnung des TCP-Datenstroms
- Unterstützung von McAfee-Signaturen, benutzerdefinierten Signaturen sowie Open-Source-Signaturen
- Native Unterstützung von Snort-Signaturen (NS-Serie)
- Whitelist/Blacklist-Verbesserungen bei der Unterstützung von STIX (Structured Threat Information eXpression) (NS-Serie)
- Host-Quarantäne und Bandbreitenbeschränkung
- Überprüfung virtueller Umgebungen
- Integration von McAfee Advanced Threat Defense
- Dekomprimierung von HTTP-Antworten

Abwehr von DoS- und DDoS-Angriffen

- Grenzwert- und heuristikbasierte Erkennung
- Host-basierte Verbindungsbegrenzung
- Selbstlernende, profilbasierte Erkennung

McAfee Global Threat Intelligence

- Datei- und IP-Reputation
- Anwendungs- und Protokollreputation
- Standorterkennung
- Whitelists basieren auf McAfee Global Threat Intelligence-Kategorien

Hochverfügbarkeit

- Active-Active- und Active-Passive-Cluster mit statusbasiertem Failover
- Externes Fail-Open (aktiv)
- Integriertes Fail-Open

Unterstützung für Protokolltunnelung

- IPv6
- V4-in-V4-, V4-in-V6-, V6-in-V4- und V6-in-V6-Tunnel
- MPLS
- GRE
- Q-in-Q Double-VLAN

McAfee Network Security Manager

- Mehrstufige Verwaltungsarchitektur mit bis zu 1.000 Sensoren
- Benutzerauthentifizierung (Radius und LDAP)
- Automatisiertes Fail-Over und Fail-Back
- Notfallwiederherstellung wichtiger Konfigurationsdaten
- Zentrale, hierarchische Richtlinienverwaltung
- Arbeitsspeicher-Dashboard schlüsselt die Speichernutzung nach Gerät auf

Weitere Informationen

Weitere Details sowie Informationen zu den verfügbaren physischen Appliances finden Sie im **Spezifikationsblatt zu McAfee Network Security Platform**.

McAfee
Together is power.

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