NORMAN

NORMAN NetworkProtection v4

Herausforderung

Zweifellos ist es heutzutage eine wichtige Aufgabe von Unternehmen, Ihre Netzwerke, Unternehmens- und Kundendaten effektiv vor Bedrohungen zu schützen. Durch den zunehmenden Austausch von Daten über das Netzwerk mit einer Vielzahl von Quellen, ist auch das Risiko einer Infektion durch Malware gestiegen. Norman bietet wirksamen Schutz für Unternehmen auch mit speziellen Netzwerken, in denen kein lokaler Virenschutz installiert werden kann, z.B. Produktionsnetze oder ECM-Systeme.

Lösung

Norman Network Protection ist eine umfassende Hochleistungs-Sicherheitsanwendung zur Überprüfung des Netzwerkverkehrs auf Malware in Echtzeit. NNP bietet Unternehmen effektiven Schutz ihrer wichtigen IT-Infrastruktur gegen Cyberkriminalität.

Hauptvorteile

Hervorragende und sofort einsatzbereite Antimalware-Lösung: Schutz Ihres Netzwerkes vor Malware in einem Gerät.

Schnelle Einrichtung: Norman Network Protection Appliance kann mit dem Konfigurationsassistenten schnell und einfach eingerichtet werden.

Verbesserte Sicherheit: Nach Malware suchen, wo keine andere Lösung suchen kann! Tausende schädlicher Dateien verwenden Netzwerkprotokolle, um tiefer in Ihr Netzwerk vorzudringen. Mit NNP können Sie zum ersten Mal zusätzlich zu den herkömmlichen Internetprotokollen die Ausbreitung über häufig verwendete Netzwerkprotokolle wie **RPC, CIFS, SMB und Windows Filesharing** verhindern.

Integriertes Sicherheits-Management: Norman Network Protection Appliance ermöglicht mit dem Norman Endpoint Manager eine zentrale Verwaltung mehrerer NNPs von einer einzigen Konsole.

Latenz – kein Problem: Herkömmliche Proxy-Lösungen weisen einige Nachteile auf. Der größte Nachteil besteht in der Latenz beim Datenverkehr, für die der Proxy selbst verantwortlich ist. Ein Proxy hält den gesamten Datei-Stream zurück, während NNP dieses Problem umgeht, indem nur die für die Überprüfung auf Malware erforderlichen Daten zurückgehalten werden.

URL-Blocking: Verhindert den Zugriff auf unerwünschte Websites und schützt den Benutzer vor Bedrohungen und unangemessenen Inhalten.

Full Duplex 10Gb/s Netzwerk-Performance auf Basis von Ubuntu 64-Bit Linux: Sorgt für eine hohe Verfügbarkeit geschäftskritischer Anwendungen mit bis zu 10 GBit/s Ethernet-Durchsatz. Der leistungsstarke Antimalware-Scanner basiert auf Ubuntu 64-Bit Linux.

Hochverfügbarkeitslösung: Norman Network Protection bietet Hochverfügbarkeitsnetzwerken unterschiedlich anspruchsvolle Optionen für die Ausfallsicherung. Mit dem Silicom-Bypass-Server-Netzwerkadapter wird grundlegende Ausfallsicherheit auf Einsteigerniveau bereitgestellt. Für Ausfallsicherheit in Hochverfügbarkeits-Umgebungen bietet NNP eine Hardware-Failover-Lösung mit zwei Knoten.

Virtualisierung Neben der Installation auf einer physikalischen Hardware kann Norman Network Protection auch als virtuelle Appliance auf einem ESXi-Server betrieben werden. Damit kann NNP auch verwendet werden, um virtuelle Systeme gegeneinander abzusichern.

Prävention: Wenn die NNP Appliance eine bösartige Datei im Datenverkehr entdeckt, wird die Dateiübertragung von der Lösung aktiv abgebrochen, und der betreffende Netzwerkpfad blockiert, damit andere Benutzer oder Systeme nicht auf diese Datei zugreifen können.

FEATURES

ALLGEMEIN:
- Überall im Netzwerk einsetzbar
- Transparent für alle Netzwerkeinheiten
- Für kleine und große Netzwerke geeignet
- Einfache Installation und Wartung
- Hochgradig skalierbare Hardwareplattform
- Unterstützung von 10-Gbit/s-Netzwerken
- Unterstützt beliebig viele VLANs
- Hochverfügbarkeit
- Redundanz-/Failover-Lösung auf Software- und Hardware-Ebene

MALWARE SCAN:
- Überprüfung des Netzwerkverkehr auf Malware in Echtzeit
- Scan des Datenverkehrs aus VPN-Netzwerken möglich
- Automatischer Schutz vor Outbreaks und Schadensbegrenzung
- Erkennung & Isolierung der Malwarequelle
- Proaktiver Schutz mit Norman SandBox®, DNA-Matching und Exploit Detection
- Automatische Updates von Scanengine und Signaturen
- Scan folgender Protokolle möglich: FTP, HTTP, SMTP, POP3, RPC, TFTP, IRC und CIFS/SMB (Windows Filesharing)

WEITERE VORTEILE:
- Installation auf ESXi-Server möglich
- Optionales Blocken von MSN und BitTorrent
- Anpassbares Blockieren von URLs
- Blockieren und Sperren des Netzwerkverkehrs auf mehreren Schichten nach den Kriterien IP-Adresse, MAC-Adresse oder VLAN-ID
- Unterstützung für SNMP-basierte Verwaltungssysteme
- Multithreading fähige Anwendung ermöglicht die gleichzeitige Ausführung auf mehreren CPUs
- Betriebssystem basiert auf einem Ubuntu 64-Bit Linux
- Als hard- und softwarebasierte Lösung erhältlich

Arla

”Besonders interessant für Arla Foods war die Tatsache, dass die Lösung ohne größere Umstellungen am vorhandenen System implementiert werden konnte.”

Jens Roed Andersen,
Chief Information Security Officer bei Arla

Transparenz: NNP arbeitet auf Layer 2 des Netzwerks und ist für den IP-Verkehr transparent. Es wird lediglich für den Administrationsport eine IP-Adresse benötigt, und schon wird das Netzwerk durch NNP geschützt.

Zentrale Verwaltung:
Norman Endpoint Manager (NEM), eine leistungsstarke webbasierte Sicherheitszentrale mit grafischer Oberfläche, ist für die zentrale Verwaltung von NNP zuständig. Norman Endpoint Manager verwaltet mehrere NNPs über eine zentrale Konsole und hält die gewünschte Konfiguration und das Sicherheitsniveau über Richtlinien ein. So können IT-Administratoren den Sicherheitsstatus mehrerer NNPs ganz einfach remote verwalten; dabei verwenden sie vollständig konfigurierbare Richtlinienvorlagen, um die Kontrolle über die Sicherheitslage im Netzwerk zu behalten. Zudem erhalten sie von jedem Punkt in der Infrastruktur Benachrichtigungen bei Malware-Angriffen.

NEM stellt in Echtzeit Statistiken und Berichte zur Verfügung, in denen erkannte und blockierte Malware sowie System- und Netzwerkstatistiken aufgeführt werden. Im Vorfallsprotokoll werden aktuell blockierte URLs aufgeführt, unter denen Malware entdeckt wurde.

NEM unterstützt IT-Administratoren bei der Bereitstellung der Norman Network Protection- und Endpoint Protection-Clients* sowie bei deren Verwaltung mit Hilfe von Sicherheitsrichtlinien. Mit dem integrierten Richtlinientool können Administratoren den Sicherheitsstatus im gesamten Netzwerk überwachen. Proaktives Verhalten ist der einzige Weg zu Sicherheit. Mit der Technologie von Norman SandBox® werden zielgerichtete Angriffe und bisher unbekannte Malware erkannt. Die Norman SandBox®-Technologie bietet eine virtuelle Umgebung, in der Programme in einem sicheren Rahmen ausgeführt werden können, ohne dabei die echten Prozesse zu beeinträchtigen.

	NNP-R210-100	NNP-R210-250	NNP-R610-500
Anzahl geschützter Clients	100	250	500
Prozessor	Intel Xeon X3450 Prozessor (2,66GHz, 8M Cache, Turbo, HT) 1 S	Intel Xeon X3450 Prozessor (2,66GHz, 8M Cache, Turbo, HT) 1 S	Intel Xeon X5550 Prozessor (2,66GHz, 8M Cache, 6,40 GT/s QPI, Turbo, HT), 1.333MHz max. Speicher
RAM	4GB Speicher (2x2GB Dual Rank UDIMMs) 1.333MHz 1 S	4GB Speicher (2x2GB Dual Rank UDIMMs) 1.333MHz 1 S	6GB Speicher für 1 CPU (3x2GB Dual Rank UDIMMs) 1.333MHz
Festplatte	250GB SATA	250GB SATA	2x73GB SAS 10k 2,5" HD Hot Plug. Raid 1
Netzwerkkarte	4x10/100/1000Mb/s Ethernet	4x10/100/1000Mb/s Ethernet	4x10/100/1000Mb/s Ethernet
OPTIONEN			
Prozessor			Intel Xeon X5550 Prozessor (2,66GHz, 8M Cache, 6,40 GT/s QPI, Turbo, HT), 1.333MHz max. Speicher
RAM			12GB RAM, 24GB RAM
Netzwerkkarte	Gigabit Ethernet Bypass Server Adapter für Fail-over-Option (Kupfer und Glasfaser)	Gigabit Ethernet Bypass Server Adapter für Fail-over-Option (Kupfer und Glasfaser)	Gigabit Ethernet Bypass Server Adapter für Fail-over-Option (Kupfer und Glasfaser) 10Gb NIC Kupfer und Glasfaser
Stromversorgung			Redundante Stromversorgung

NORMAN SANDBOX®
ist eine revolutionäre Lösung zur proaktiven Erkennung neuer und unbekannter Malware.

NORMAN DNA MATCHING
ist eine proaktive Technologie zur Identifizierung des Virenprofils aller Arten von schädlichen Programmen.

NORMAN EXPLOIT DETECTION
ist eine Technologie zur Erkennung von Malware, die Sicherheitslücken in häufig verwendeten Dokumenttypen ausnutzt.

virus BULLETIN

„Seine einfachen und unproblematischen Malware-Schutzfunktionen sowie sein ausgezeichnetes und gleichermaßen unkompliziertes Kontrollsystem machen diese Lösung zu einer absolut anwenderfreundlichen und wirksamen Waffe im Kampf gegen Malware-Angriffe auf Unternehmensnetzwerke. Wir freuen uns schon darauf, noch weitere Sicherheitsgeräte kennen zu lernen, um zu sehen, ob sich diese mit der beeindruckenden Leistung von Norman messen können."

NETWORKcomputing

"NNP verfügt über eine ganze Reihe klarer Vorteile gegenüber herkömmlichen Gateway-Sicherheitsgeräten, da sie über einen breiteren Bereich von Netzwerkszenarien eingesetzt werden kann.

Die Installation ist einzigartig einfach, die Lösung ermöglicht transparenten Betrieb und die Technologie von Norman SandBox® bietet eine starke Sicherheitsbarriere."

TÜV Geprüfter Virenschutz · vb 100 VIRUS virusbtn.com · ICSA labs CERTIFIED ANTI-VIRUS · NSS Labs TESTED

Norman zählt zu den führenden Unternehmen und Pionieren für die Entwicklung proaktiver Lösungen zur Absicherung von Unternehmensdaten und für die Entwicklung von Forensik-Tools zur Malware-Erkennung. Die Produkte von Norman schützen Endanwender und Netzwerke in Unternehmen jeder Größenordnung vor Malware und ermöglichen die Analyse von Schadcode. Norman wurde im Jahr 1984 in Oslo gegründet und vertreibt die Produkte weltweit über eigene Niederlassungen und ein ausgedehntes Partnernetz.

NORMAN®

INTRUSION GUARD · ANTI-SPAM · PERSONAL FIREWALL · PARENTAL CONTROL · PRIVACY CONTROL · MAIL-SCAN · STATISTICS · UPDATE · NETWORK PROTECTION · QUARANTINE · DNA MATCHING · SANDBOX · EXPLOIT PROTECTION

info@norman.de • www.norman.de