

Check Point Endpoint Security

Effiziente Sicherung der Endpunkte durch die
Vereinigung von wesentlichen Sicherheits-
Komponenten in einem einzigen Agent

Inhalt

Management Summary	3
Die Herausforderungen der Endpoint-Absicherung.....	4
Eine neue Strategie: Einheitlicher Endpoint Security-Ansatz	6
Leistungsvorteile einer einheitlichen Endpoint Security	6
Check Point Endpoint Security	10
Fazit	12

Management Summary

Jeder Security-Verantwortliche, der sich über Informationssicherheit Gedanken macht, wird erkennen, dass Endpoints die Achilles-Ferse der unternehmensweiten Security-Strategie sein können. Endpoints bringen drei wesentliche Risiken mit sich. Als erstes geht es um Angriffe, die zunehmend herkömmliche Perimeter-Security umgehen und den Endpunkt sowie das Unternehmensnetzwerk mit einer Vielzahl von Methoden, wie beispielsweise durch die Interaktionen mit bösartigen Webseiten angreifen. Ein zweites Risiko ist die Tatsache, dass eine große Anzahl der Endpoints mobil sind, sodass sie innerhalb und außerhalb des traditionellen Perimeters eingesetzt werden können. Schließlich stellen Endpoints eine enorme logistische Herausforderung für das IT-Personal dar, das die Durchsetzung von Policies und den Einsatz der Komponenten von verschiedenen Security Agents auf jedem physischen Gerät verwalten muss.

Endpoints benötigen geeignete Security-Lösungen, sonst laufen sie zunehmend Gefahr, Opfer von Exploits zu werden, die Schwachstellen ausnutzen. Überwinden Angriffe erfolgreich Schwachstellen am Endpoint, kann dies zu Datendiebstahl, Unterbrechung von Geschäftsvorgängen und potentiellen Strafen für fehlende Gesetzes- und Vorschriftenkonformität in Bezug auf die Sicherheit führen.

Um sich dieser Herausforderung zu stellen, wenden sich Unternehmen einer neuen Strategie zu, zu der eine große Anzahl von Technologien für Endpoint Sicherheit gehört und die in einem einzigen Agenten vereinigt und zentral verwaltet sind. Das ist die richtige Strategie – aber damit ihr Erfolg auch gesichert ist, wird die Implementierung aller Komponenten benötigt, die die Security-Risiken bis hin zum Endpoint abdecken. Zusätzlich zu der funktionellen Bandbreite, müssen Unternehmen sicherstellen, dass die Kosten für Security-Lösung relativ gering sind, dass die Komponenten für den User nicht sichtbar sind und dass die gesamte Lösung von einem zentralen Standort aus verwaltet werden kann. Dieses White Paper beschreibt die Risiken und stellt eine einheitliche Lösung vor, die Check Point Endpoint Security™ heißt.

Die Herausforderungen der Endpoint-Absicherung

Aus Sicht der IT und eines Security Managers waren Technologie-Infrastrukturen und Daten einfacher zu schützen, als PCs, Netzwerke und das Internet in Unternehmen noch nicht so große Bedeutung hatten. Im Zuge dieser Veränderung, war der Netzwerk-Perimeter der Fokus aller Sicherheits-Bemühungen, da Unternehmen versuchten, Angriffe von außen davon abzuhalten, in das interne System einzudringen. Hacker und Kriminelle haben gelernt, wie Schwachstellen durch neue Angriffe ausgenutzt werden können, was zu einem unübersichtlichen Wirrwarr an neuen Security-Lösungen führte. Die herkömmliche Meinung ist, umfassenden Schutz mit einem abgestuften Ansatz gegenüber dem Netzwerk und der Informationssicherheit zu implementieren, damit potentielle Schwachstellen nicht übersehen werden.

Heutzutage richten Experten ihre Aufmerksamkeit mehr und mehr auf einen Hauptrisikobereich – den Endpoint, der eine eigene Absicherung benötigt. Zu Endpoints zählt praktisch jedes EDV-Gerät, das an ein Netzwerk angeschlossen ist. Dazu gehören PCs, Notebooks, portable oder elektronische Geräte mit Speicher, I/O, und/oder kabellose Connectivity und IP-Netzwerk-Geräte.

Endpoints sind für eine Reihe von Angriffsarten sehr anfällig, speziell bei Schwachstellen in allgemeinen Netzwerk-Protokollen, die Zugang aufgrund von offenen oder unkontrollierten Ports gewähren. Andere Exploits konzentrieren sich auf Programmierfehler in großen Software Data Buffer, die bei einem Overflow Speicher korrumpieren und die Ausführung von Malicious Code zulassen. Die meisten PCs laufen auf einem der Windows-Betriebssysteme (OSes) von Microsoft. Sie sind gefährdet durch Angriffe von Hackern, deren Attacken auf Hundertmillionen von Geräten abzielen, die diese Plattformen nutzen. Aber neben den Betriebssystemen sind alle Endpoints, die IP nutzen anfällig für Angriffe und viele befürchten, dass deshalb Endpoints die neue Achilles-Ferse des Unternehmensnetzwerks sind.

Die drei Risiken bei Endpoints

Durch Endpoints kommen drei neue, signifikante Risiken auf die IT eines Unternehmens zu. Zum einen umgehen Angriffe zunehmend herkömmliche Perimeter-Security und infiltrieren Unternehmensnetzwerke über die webbasierte Anwendung, auf die sie über die Endpoints Zugriff erhalten haben. Durch einen harmlosen Besuch auf einer bösartigen Webseite, können Schwachstellen im Browser ausgenutzt werden. Die meisten Gefahren, wie beispielsweise Cross-Site Scripting-Angriffe stellen für fast alle Browser ein Risiko dar. Der webbasierte Netzwerkzugang ist auch vor anderen Bedrohungen nicht geschützt, wie beispielweise der Offenlegung von Cookies oder lokalen Dateien, der Ausführung von lokalen Programmen oder Malicious Code oder sogar vor einer kompletten Übernahme eines ungeschützten PCs.

Die zweite große Risikogruppe besteht aus der wachsenden Zahl an mobilen Endpoints, was eine Nutzung in- und außerhalb der herkömmlichen Perimeter Security zur Folge hat. Inzwischen stellen Laptops 50 Prozent aller PC-Lieferungen weltweit¹ dar und ihre Anzahl steigt ständig. Endpoints, auf denen keine lokalen Security-Komponenten installiert sind, laufen bei einer Nutzung außerhalb des Perimeters Gefahr, angegriffen zu werden.

Schlussendlich stellen Endpoints eine enorme logistische Herausforderung an das IT-Personal dar, die den Einsatz von policy-basierten Komponenten auf jedem physischen Gerät verwalten müssen. Der Einsatz der Security Software, das Installieren von Updates und neuen Signatur-Dateien sowie das konstante Einhalten von bestehenden Richtlinien und Konfigurationen sind zeitaufwendige Aufgaben und sehr schwer manuell durchzuführen – speziell bei Unternehmen mit Tausenden von mobilen Endpoints.

¹ Quelle: 451 Group

Eine neue Strategie: Einheitliche Endpoint Security

Umsichtige IT-Security Manager sehen in Endpoints „Risiko-Inseln“, besonders wenn sie als mobile Geräte außerhalb des Unternehmens-Netzwerk-Perimeters eingesetzt werden. Eine Möglichkeit, die Ausnutzung der Schwachstellen an den Endpoints zu verhindern, ist der Einsatz eines umfassenden Endpoint-Security-Schutzes auf jedem PC.

Unternehmen haben meist einige alleinstehenden Endpoint-Lösungen für deren Sicherheit im Einsatz, wie beispielsweise eine Personal Firewall oder Anti-Virus-Software. Dieser Ansatz kann sehr schnell zu einem Albtraum werden, wenn es sich um Firmen mit Hunderten oder Tausenden von PCs handelt. Beispielsweise muss jedes Mal, wenn ein Software Update für individuelle Endpoint-Agenten zur Verfügung steht, die IT Test-Läufe durchführen, um die Version auf die Leistung und Kompatibilität zu prüfen, bevor das Update auch auf den Endpoints aktiviert werden kann. Da es nicht ungewöhnlich ist, dass Unternehmen drei oder mehr Endpoint Security Agents auf jedem Gerät im Einsatz haben, kann eine Implementierung sehr zeitaufwendig und teuer werden.

Eine neue Strategie ist eine vereinheitlichte Endpoint Security, mit Sicherheits-funktionalitäten auf jedem PC, die zentral eingesetzt und von den IT Security-Spezialisten auf einer einzigen Konsole verwaltet werden. Die Vereinheitlichung der Security-Funktionen ermöglicht vereinfachten Einsatz und Management, was letztendlich die Betriebskosten senkt. Durch den Ansatz, nur einen einheitlichen Agenten zu verwenden, muss die IT auch nur einen Test für einen Agenten laufen lassen und kann sicher gehen, dass jede Funktion innerhalb des Agenten kompatibel ist. Um also eine höchstmögliche Sicherheit der Endpunkte zu erreichen, sollte sich ein Unternehmen Gedanken über die Funktionen einer vereinheitlichten Endpoint Lösung machen. Nur ein umfassendes Set an Security-Instrumentarien kann einem Unternehmen umfassende Endpoint-Sicherheit bieten.

Firmen sollten folgende Schritte beachten, die für eine vereinheitlichte Endpoint Security notwendig sind:

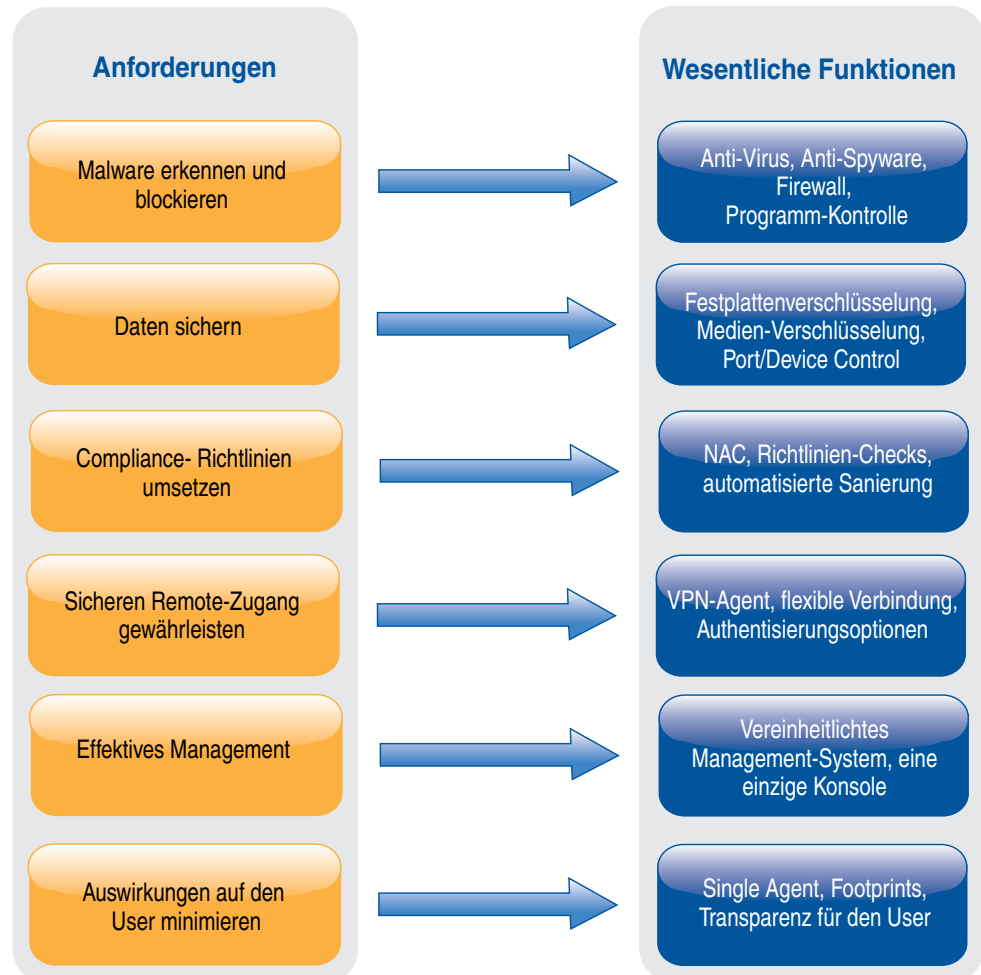
- Malware erkennen und blockieren
- Daten sichern
- Compliance- Richtlinien umsetzen
- Sicheren Remote-Zugang gewährleisten
- Effektives Management
- Auswirkungen auf den User minimieren

1. Malware erkennen und blockieren

Die Erkennung von Malware und die Blockierung der Ausführung am Endpoint, wird normalerweise durch den Einsatz von separaten Produkten für Firewall, Anti-Virus und Anti-Spyware durchgeführt. Jede dieser Security-Anwendungen bietet wichtige und einzigartige Funktionen im Bezug auf die gemeinsamen Anforderungen, Malware zu erkennen und zu blockieren.

Eine Firewall mit Programm-Kontrolle ist die wichtigste Security-Komponente, weil sie eingehenden und ausgehenden Verkehr stark verändern kann. Nur eine Firewall kann ungewollten Traffic blockieren, wie beispielsweise Malicious Code. Außerdem kann sie kontrollieren, welchen Anwendungen Netzwerkzugang erlaubt ist und sie „versteckt“

Endpoints, sodass sie für Hacker unsichtbar werden. Einige Endpoint Security Suites sind um die Anti-Virus-Funktion herum entwickelt. Allerdings ist die Firewall aufgrund ihrer Fähigkeit, Traffic zu und vom Endpoint des PCs zu kontrollieren, am besten als erste Verteidigungslinie geeignet.



Wichtige Anforderungen für einheitliche Endpoint Security

Anti-Virus wird dazu genutzt, das Eindringen von Viren zu identifizieren und zu stoppen. Eine qualitativ hochwertige Anti-Virus-Anwendung verwendet eine Kombination aus Erkennungstechniken, wie beispielsweise Matching und Heuristik. Ältere Techniken entdecken Viren durch den Vergleich von Dateien mit einer Datenbank, die Informationen über bereits identifizierten Malicious Code enthält. Die Heuristik identifiziert Viren durch den Vergleich von Datei-Delivery und Code-Verhalten, gegenüber bekannten Bedrohungen.

Anti-Spyware verhindert das Eindringen von Würmern, Trojanern, Adware und Keystroke Loggern. Sie bietet Echtzeit-Schutz gegen Spyware-Installationen auf den Endpoints und die Erkennung und das Entfernen von Spyware, die schon früher installiert wurde.

Bei all diesen Maßnahmen ist es für die Administratoren äußerst wichtig, zentrale Kontrolle über die Endpoints zu haben, um Compliance zu gewährleisten. Das bedeutet beispielsweise die Möglichkeit, Scans in regelmäßigen Intervallen auf PCs einzurichten,

die Anzahl der PCs, auf denen ein kompletter Virenskan durchgeführt wurde und die Anzahl der PCs, die aktuell infiziert sind, einsehen zu können.

2. Daten sichern

Daten am Endpoint zu sichern ist äußerst wichtig, seitdem es so einfach geworden ist, einen Laptop oder andere mobile Geräte zu stehlen oder zu verlieren. Fällt das Device einmal in nichtautorisierte Hände, sind unverschlüsselte Daten am Endpoint sofort zugänglich und können missbraucht werden. Komponenten, die Daten am Endpoint sichern, beinhalten komplette Festplattenverschlüsselung, Medienverschlüsselung und Port/Device Control.

Verschlüsselung macht die Daten für jedermann unlesbar, außer für diejenigen, die über den richtigen Schlüssel verfügen. Für gewöhnlich wird ein Schlüssel für die Entschlüsselung und Wiederlesbarkeit der Daten benötigt. Verschlüsselung kann für eine einzelne Datei, einen Ordner oder eine ganze Festplatte sowie andere Arten von Speicher-Medien relevant sein. Früher war die Verschlüsselung am Endpoint sehr schwerfällig und behinderte die System-Leistung. Aktuellere Verschlüsselungs-Lösungen haben dieses Problem gelöst und werden inzwischen weltweit auf Millionen von Endpoints eingesetzt.

Port/Device Control ist eine relativ neue Technologie, mit der Unternehmen die Nutzung einzelner Ports auf einem Endpoint überwachen können. Ein praktischer Vorteil ist der Schutz vor nichtautorisiertem Transfer geschützter Daten, von einem Endpoint auf ein persönliches Speichergerät, wie beispielsweise einen USB-Stick. Port Control verhindert auch den Transfer von Malware von externen Speichergeräten auf den Endpoint – und weiter ins Netzwerk des Unternehmens.

3. Compliance-Richtlinien umsetzen

Die Durchsetzung von Compliance-Richtlinien lässt einen Endpoint mit den Security-Richtlinien konform gehen, bevor Zugang zum Netzwerk gewährt wird. Auf einem Basislevel, wird aufgrund dieser Anforderungen ein Richtlinien-Check auf jedem Endpoint durchgeführt, der sich auf Security-Richtlinien bezieht, die von Administratoren erstellt wurden. Beispielsweise fordern Compliance-Vorschriften auf jedem Endpoint die aktuellste Version der Antiviren-Software, wichtige Patches sowie die aktuellsten Anwendungen oder auch die Zusicherung, dass auf dem Endpoint keine verbotenen Programme laufen. Weist ein Check Fehler an einem Endpoint auf, wird der Netzwerkzugang blockiert.

Heterogene Unternehmensnetzwerke erfordern Compliance Policy, um mit Gateways und Authentisierungs-Systemen von verschiedenen Anbietern kompatibel zu sein. Compliance in einem vereinheitlichten Endpoint Security-System sollte dem Industriestandard 802.1x für Authentifizierung entsprechen, damit Network Access Control (NAC) in Umgebungen mit mehreren Anbietern ermöglicht werden kann. Eine weitere Anforderung ist Compliance On Demand. Hier werden Security-Richtlinien bei Bedarf, auf nicht verwalteten Endpoints aktiviert, ohne dass die IT Agent-Software installieren muss. Für jede Sitzung wird Vertraulichkeit für das Gerät zugesichert und Spyware wird erkannt und deaktiviert. Geht ein Mitarbeiter beispielsweise über ein SSL VPN Gateway von einem PC, der sich in einem Internet Café oder einem Flughafen-Kiosk befindet in das Firmennetzwerk, muss die IT gewährleisten, dass dies ein sicherer Zugang auf das Netzwerk ist. Außerdem muss die IT Vertraulichkeit für diese Sitzung zusichern, d.h. es darf auf dem genutzten Gerät nichts zurückbleiben, nachdem ein Mitarbeiter eine Remote-Access-Sitzung beendet hat.

4. Sicheren Remote-Zugang gewährleisten

Durch die zunehmende Verbreitung von mobile Computing, wird sicherer Remote-Zugang zu einer Schlüsselanforderung an die Endpoint-Sicherheit. Die Technologien verfügen über einen Remote-Access-Agent, flexible Verbindung und Authentisierungsoptionen.

Die Virtual Private Network (VPN)-Technologie ist das am häufigsten verwendete Mittel, um sicheren Remote-Zugang an einem Unternehmens-Netzwerk-Gateway zu aktivieren. Die Remote-Zugangsverbindung schützt die Kommunikation, indem ein sicherer, verschlüsselter Zugangstunnel zur Verfügung steht, durch den heimliches Belauschen und Datenmanipulation verhindert werden.

Eine flexible Connectivity sollte dynamische und fixe IP-Adressen für die Einwahl, Kabel-Modem oder digitale Anschlussleitungen beinhalten. Sie sollte ebenfalls mit potentiellen Routing-Problemen umgehen können, die zwischen dem Agent und dem Remote-Access-Gateway auftreten können, wobei die IP-Pakete unter der Original-Remote User IP-Adresse zusammengefasst werden. Dadurch erscheinen Nutzer so, als wenn sie „im Büro“ sind, obwohl sie sich über eine Remote-Verbindung eingeloggt haben.

Authentisierungsoptionen sollten Support für SecurID Token, Username und Passwort beinhalten sowie RADIUS, TACACS, und Biometrics.

5. Effektives Management

Das große Ziel einer vereinheitlichten Endpoint Security ist es, alles von einer Konsole aus zu verwalten. Zentrale Konfiguration, Policy-Administration, Reporting und Analysen der gesamten Endpoint Security sollten gewährleistet sein, was auch in den oben beschriebenen Security-Komponenten enthalten ist, die auf jedem Unternehmens-Endpoint laufen. Unternehmen sollten davon ausgehen, dass effektives Management folgende Punkte beinhaltet:

- Zentralisierte und mächtige Management-Optionen
- Zentrales Monitoring und Reporting einer jeden Endpoint Security-Komponente
- Schnelle Erkennung, Überwachung und Forensische-Analyse von Sicherheitsvorfällen
- Umfassendes Reporting und Support für Audits und Compliance
- Einfacher und schneller Einsatz von Software auf den Agents, ohne dass manuelle Eingriffe durch die IT oder den Usern Vor-Ort notwendig sind
- Vereinigung der Endpoint Security mit dem Netzwerk Security Event Management

6. Auswirkungen auf den User minimieren

Es ist wichtig, dass die vereinheitlichte Endpoint Security dem Endnutzer während seiner Arbeit nicht im Weg steht. Idealerweise sollten alle Security-Komponenten in einem einzigen Small-Footprint-Agent am Endpoint zur Verfügung stehen. Die meisten Endpoint Security Suites müssen allerdings drei, vier, fünf oder sogar mehr Agent-Software-Module auf jeden PC laden. Das Ergebnis ist, dass die Security-Anwendungen den Speicher überlasten, CPU-Leistung aufbrauchen und so die Performance der Business-Anwendungen sinkt. Der Ärger bei den Usern wächst, wenn von ihnen erwartet wird, dass Updates der Security Software, Patches und andere System-Wartung händisch eingegeben werden müssen. Weniger Agents bewirken eine einfachere Verwaltung, bessere Leistung, weniger Nutzer-Interventionen und stärkere Endpoint Security.

Mehr Performance durch vereinheitlichte Endpoint Security

Die Vereinheitlichung von umfassenden Endpoint Security Funktionen hat einen Small-Agent Footprint und leistungsfähigere Endpoint-Systeme zu Folge. Mit weniger Agent-Modulen wird der Einsatz und die Verwaltung eines derartigen Systems vereinfacht.

Check Point Endpoint Security

Eine optimale Verbindung von umfassendem Schutz, Kontrolle und Leistung stellt Check Point Endpoint Security sowohl für bestehende Kunden als auch für andere Unternehmen dar. Die Software verbindet die wichtigsten Security-Komponenten, die für effektiven Schutz der Endpoints benötigt werden. Der Agent ist zentral verwaltet und benötigt keine Aktivität von Seiten des Nutzers.

Vereinheitliche Funktionalitäten der Check Point Endpoint Security

Funktion	Beschreibung
Firewall	Mit 15 Jahren Marktführerschaft im Bereich Enterprise-Firewalls und durch die Vorteile der weitverbreiteten ZoneAlarm® Personal Firewall-Technologie, bietet Check Point Endpoint Security proaktiven Schutz für eingehenden und ausgehenden Datenverkehr. Die Ausbreitung von Malicious Code auf Endpoint-PCs wird verhindert, ungewollter Traffic blockiert und es wird eine „schlaue Methode“ verwendet, die Endpoints für Hacker unsichtbar macht, die auf der Suche nach anfälligen Systemen sind.
Programm-Kontrolle	Kontrolliert das Verhalten von Anwendungen mit herkömmlichen Firewall-Regeln. Es wird automatisch ein Verzeichnis aller PC-Anwendung erstellt, die Netzwerkzugang anstreben. Dadurch wird eine schnelle und effiziente Identifikation sowie die Absicherung von potentiellen Netzwerkschwachstellen aktiviert. Außerdem wird sichergestellt, dass bereits freigeschaltete Programme nicht kompromittiert, verändert oder übernommen werden können.
Programm-Advisor	Bietet Administratoren die Möglichkeit, einen Großteil der Entscheidungen bezüglich Richtlinien, die auf Echtzeitdaten beruhen und die von Millionen PCs weltweit zusammengetragen werden, zu automatisieren. Der positive Effekt der Check Point-Wissensdatenbank wird durch vertrauensvolle und sofortige Anwendung von Best-Practice-Richtlinien im Fall von Malware gesteigert, wobei die Kommunikation entweder blockiert oder erlaubt wird. Zudem wird die Ausführung von jedem böswärtigen Programm, das identifiziert wird, automatisch eliminiert.
Network Access Control (NAC)	Administratoren erhalten die Möglichkeit, den Zugang zu ihrem Netzwerk zu kontrollieren und Endpoint-Richtlinien für VPN-basierten Zugang und internen Netzwerkzugang zu implementieren. NAC-Funktionen können mit den Check Point Gateways und mit Infrastruktur-Geräten von führenden Netzwerk-Herstellern in Verbindung stehen. Support des Industrie-Standard 802.1x Authentifizierung ermöglicht NAC in Multi-vendor Umgebungen – mit oder ohne Check Point Infrastruktur.
Anti-Virus	Vereinheitlichte, hochleistungsfähige Anti-Virus-Technologie erkennt und eliminiert Viren und andere damit verbundene Malware vom Endpoint. Die Erkennung von Viren basiert auf einer Kombination von Signaturen, Verhaltens-Block und heuristischen Analysen, die gemeinsam die Netzwerkumgebung so aktivieren, dass eine der höchsten Erkennungsraten innerhalb der Branche erreicht wird.
Anti-Spyware	Schützt Unternehmen vor finanziellem Schaden, der durch Spyware entsteht, die sensible Daten stiehlt oder offen legt, interne Netzwerke überschwemmt und Helpdesk-Ausgaben durch verlangsamte PC-Leistung erhöht. Anti-Spyware bietet zentral konfigurierte und durchsetzbare Signatur-Updates, um zu gewährleisten, dass Endpoints jederzeit über den aktuellsten Spyware-Schutz verfügen.
Datensicherheit *	Check Point Endpoint Security setzt Pointsecs® markführende Datensicherheits-Technologie ein, um den Schutz vertraulicher Daten mit einer effizienten Auswahl an Preboot-Authentifizierung mit Festplattenverschlüsselung, Medien-Verschlüsselung und Port-Management zu gewährleisten. Die komplette Festplattenverschlüsselung bietet eine benutzerfreundliche Kombination aus Verschlüsselung mit Zugangskontrolle, die die gesamten Festplatten-Daten schützt, während der User weiterhin Transparenz über alle Vorgänge behält. Medien-Verschlüsselung gewährleistet effektive Verschlüsselung für alle Medien wie z.B. USB Flash Drives. Port-Schutz beinhaltet umfassende Inhaltskontrolle von eingehenden und ausgehenden Inhalten, aufgrund von Datenüberprüfung, zentralisiertem Auditing und Port-Management, die ein gemeinsames Ziel verfolgen - Datenlecks zu verhindern.
Remote-Zugang	Check Point Endpoint Security ist die einzige Endpoint-Lösung, die in sich einen hochentwickelten IPSec VPN-Agent vereinigt, der auf dem prämierten VPN-1® SecureClient™ basiert und somit sicheren Remote-Zugang als integralen Bestandteil der Endpoint-Sicherheit bietet. Diese IPSec VPN-Funktion ist komplett mit dem Single Endpoint Security Agent verbunden. Sie nutzen das gleiche User-Interface und das gleiche System-Ablage-Symbol, wie die anderen Endpoint Security-Funktionen.
Vereinheitlichtes Management	Gibt Administratoren starke Tools an die Hand, um die Endpoint Security-Policies zu verbessern und an die speziellen Anforderungen ihrer Unternehmen anzupassen. Sie können damit eindeutige Richtlinien definieren, die sich automatisch an den Endpoints ausrichten, wenn sie sich zwischen den Netzwerken, Standorten und Gateways hin- und herbewegen. Check Point Endpoint Security verringert Zeit und Aufwand, der notwendig ist, um die Anwendung und die Security-Policies zu verwalten, damit das Geschäft ohne Komplikationen weiterlaufen kann und dabei sicher und effizient ist.
Integration mit Check Point Unified Security Architecture	Aufgrund der Check Point Unified Security Architecture können Administratoren Endpoint Security und NAC mit dem gleichen SmartCenter™ und Provider-1® Management System verwalten, die verwendet werden, um andere Check Point-Produkte zu verwalten. Vereinheitlichung schließt die Notwendigkeit aus, separate Management-Logins und Server zu betreiben, reduziert IT-Zeit, Kosten und Komplexität – während die gesamte Sicherheit des Unternehmens verbessert wird.

*Single Agent inklusive Data Security verfügbar ab Q3 2008

Fazit

Ohne vereinheitlichte Endpoint Security sind Endpunkte die Achilles-Ferse der Netzwerk- und Informationssicherheit. Durch den Einsatz der umfassendsten Security-Lösung innerhalb der Branche - Check Point Endpoint Security – können Unternehmen Anwendungen mit vereinheitlichtem Security-Komponenten an jedem Endpoint gewährleisten, während die Verwaltung der Endpoint Security im gesamten Unternehmen vereinfacht wird. Check Point Endpoint Security vereint die am höchsten bewertete Firewall, Netzwerkzugangskontrolle (NAC), Programm-Kontrolle, Anti-Virus, Anti-Spyware, Datensicherheit und Remote-Access in einem einzigen, zentral verwalteten Agent. Dadurch besteht nicht mehr die Notwendigkeit, verschiedene Endpoint Security Agents zu verwalten, was die Zeit und den Aufwand für das Management dramatisch reduziert.

Nehmen Sie mit Check Point, dem weltweiten Marktführer für Netzwerksicherheit, Datensicherheit und Security Management, Kontakt auf, um mehr Informationen zur Check Point Endpoint Security zu erhalten.

Produktinformation

http://www.checkpoint.com/products/endpoint_security

Über Check Point Software Technologies Ltd.

Check Point Software Technologies ist ein führender Anbieter von intelligenten Sicherheitslösungen. Das Unternehmen gilt sowohl im weltweiten Enterprise Firewall-Markt, als auch im Personal Firewall-, Datensicherheits- und VPN-Segment als unbestrittener Marktführer.

Mit seinem Konzept der „Total Security“ fokussiert das Unternehmen ausschließlich IT-Sicherheit und verfügt über ein umfassendes Portfolio an Lösungen für Netzwerksicherheit, Datensicherheit und Security Management. Auf Basis seiner NGX-Plattform bietet Check Point eine so genannte Unified Security Architecture, also eine vereinheitlichte Sicherheitsarchitektur, die eine Vielzahl von Perimeter-, Internal-, Web- und Endpoint Security-Lösungen umfasst.

Weltweit setzen tausende Organisationen aller Branchen und Größen – darunter 100 Prozent der Fortune 100-Unternehmen – auf die Lösungen von Check Point

CHECK POINT NIEDERLASSUNGEN

Weltweiter Firmensitz

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel.: 972-3-753 4555
Fax: 972-3-575 9256
E-Mail: info@checkpoint.com

Deutsche Niederlassung

Fraunhofer Straße 7
85737 Ismaning
Tel.: 49-89-999819-0
Fax: 49-89-999819-499
www.checkpoint.com

©2003–2008 Check Point Software Technologies Ltd. Alle Rechte vorbehalten. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, das Check Point Logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, das puresecurity Logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartViewMonitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Anti-Virus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, und das Zone Labs Logo sind Handelsmarken oder registrierte Handelsmarken von Check Point Software Technologies Ltd. oder angegliederten Unternehmen. ZoneAlarm ist ein Check Point Software Technologies, Inc. Unternehmen. Alle anderen Produktnamen, die hier erwähnt werden, sind Handelsmarken oder registrierte Handelsmarken des jeweiligen Eigentümers. Die Produkte, die in diesem Dokument beschrieben werden, sind durch folgende U.S. Patente geschützt: Nr. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, und 7,165,076 und können wiederum durch andere U.S. Patente, ausländische Patente oder Patentanmeldungen geschützt sein.