CHECK POINTS LÖSUNGEN FÜR THREAT PREVENTION

MEHRSTUFIGER SCHUTZ VOR KOMPLEXEN BEDROHUNGEN

Die Vorteile

- Verhinderung von Bedrohungen mit einem umfassenden Paket an integrierten Schutzfunktionen
- ThreatCloud™ bietet Sicherheit in Echtzeit
- Vollständiger Schutz vor fortschrittlichen Zero-Day-Bedrohungen mit Threat Emulation und Threat Extraction
- Erkennung und Abwehr von schadhaften Dateien, die von Websites heruntergeladen werden
- Abwehr nachträglicher Infizierungen und Entschärfung von Bot-Angriffen
- Maximaler Schutz durch Unified-Management, -Monitoring und -Reporting

Die Funktionen

- Die Konsolidierung verschiedener Sicherheitsfunktionen in einer einzigen, integrierten Lösung mit Unified-Policy-Management und Bedrohungsüberwachung reduziert die Komplexität und steigert die betriebliche Effizienz
- Echtzeit-Updates für neue Bedrohungen sorgen für optimalen Schutz an den Gateways und sichern die Unternehmensdaten und die Unternehmensressourcen ab
- Überprüfung der Dateien in einer virtuellen „Sandbox" für den Schutz vor unbekannter Malware
- Rekonstruktion der Dateien mit ausschließlich sicheren Elementen, um infizierte Dateien zu eliminieren bevor sie in das Netzwerk gelangen
- Einblicke in den Sicherheitsstatus mit einer einzigen, zentralen Konsole, die es ermöglicht, den Internet-Datenverkehr und die Internetaktivitäten zu überwachen, zu analysieren und Reports zu erstellen, um die Unternehmensdaten und Unternehmensressourcen vor Schäden zu bewahren

Angreifer werden immer kreativer, wenn es darum geht, auf Unternehmensressourcen zuzugreifen und Firmen Sicherheitsbedrohungen auszusetzen. Unternehmen müssen heute nicht nur Netzwerkangriffe fürchten, sondern auch Angriffe auf die Computer der Endanwender wie beispielsweise durch Viren, Bots oder Drive-by-Downloads. Gehen Unternehmen dem nicht nach, kann jede dieser Bedrohungen ein Risiko für die Daten eines Unternehmens oder auch das Unternehmen selbst darstellen.

Moderne Malware entwickelt sich extrem schnell weiter. Tatsächlich wird nahezu jede Sekunde neue Malware erzeugt. Aufgrund dieser dynamischen Bedrohungslandschaft und der stark wachsenden Zahl an Malware-Varianten, verlieren traditionelle Antiviren-Lösungen an Wirksamkeit und können diese unbekannte Malware weder erkennen noch blockieren bevor diese in das Unternehmen gelangt und das Netzwerk und die Systeme kompromittiert. Heute sind weiter greifende Lösungen erforderlich.

Aufgrund dieser steigenden Zahl an Risiken benötigen Unternehmen umfassende Lösungen, die sie zum einen vor bekannter Malware schützen, und die zum anderen Malware abwehren, die zuvor noch niemals erkannt wurde. Zudem sollten diese Lösungen sie vor Ausfällen, Datenverlust, Produktivitätsbeeinträchtigungen und möglichen Imageschäden schützen. Es mag entmutigend klingen, diese kontinuierlich neu entstehenden Bedrohungen bekämpfen, gleichzeitig die Komplexität reduzieren und die betriebliche Effizienz steigern zu müssen. Doch es gibt bereits eine umfassende, vollständig integrierte und innovative Lösung für die Bedrohungsabwehr, um diese Herausforderungen zu bewältigen.

ÜBERBLICK

Check Points Threat Prevention-Lösungen bieten unmittelbaren Schutz und sichern die Unternehmensressourcen ab, da sie die leistungsstärksten Sicherheitsfunktionen kombinieren. Hierzu zählen:

- ThreatCloud™ für Sicherheit in Echtzeit und übergreifende Zusammenarbeit
- Umfassender Schutz vor Zero-Day-Bedrohungen mit Threat Emulation und Threat Extraction
- IPS (empfohlen von den NSS Labs) für die Abwehr von Eindringlingen
- Antivirus für die Erkennung und Abwehr von Malware
- Anti-Bot erkennt Bots und schützt vor Bot-Schäden
- Anti-Spam schützt die Messaging-Infrastruktur im Unternehmen
- Application Control verhindert die Nutzung risikoreicher Anwendungen
- URL Filtering verhindert den Zugriff auf Websites mit Malware
- Identity Awareness definiert Richtlinien für Anwender und Gruppen
- Unified Policy deckt alle Websites, Anwendungen, Nutzer und Rechner ab
- Logging and Status für die aktive Datenanalyse

Check Points integrierte Lösungen für Threat Prevention schützen Unternehmen mit einem einzigen Security-Gateway vor der wachsenden Zahl an Internetangriffen. Eine Reihe an Optionen – von All-in-one-Appliances bis hin zu Add-on-Funktionen – ermöglicht es, die Komplexität zu reduzieren und die effektivsten Maßnahmen für die Bedrohungsabwehr in Ihrer Netzwerkinfrastruktur zu wählen.

FUNKTIONEN FÜR DIE BEDROHUNGSABWEHR

Powered by ThreatCloud™
Die ThreatCloud™ liefert den Software-Blades des Security-Gateways Sicherheitsinformationen in Echtzeit, die in dem ersten, gemeinsam genutzten Netzwerk für die Bekämpfung von Cyber-Kriminalität gesammelt werden, um Bedrohungen zu erkennen und Angriffe zu verhindern.

ThreatCloud™ Emulation Service
Check Point ThreatCloud™ Emulation Service verhindert Infizierungen durch bisher unerkannte Zero-Day-Exploits und zielgerichtete Angriffe. Diese innovative Lösung überprüft Dateien sehr schnell und führt diese in einer virtuellen „Sandbox“ aus, um schadhaftes Verhalten zu erkennen. Die erkannte Malware kann somit nicht mehr in das Unternehmensnetzwerk eindringen.

Threat Extraction
Check Point Threat Extraction bietet Schutz vor infizierten Dokumenten, indem die Dateien mit ausschließlich sicheren Elementen rekonstruiert werden. Ausführbare Inhalte – und dies umfasst aktive Inhalte und verschiedene Formen von eingebetteten Objekten – werden aus den rekonstruierten Dateien eliminiert, um so mögliche Bedrohungen abzuwehren und Malware-freie Dokumente ohne jegliche Zeitverzögerung zuzustellen.

IPS
Das IPS-Software-Blade bietet vollständige und aktive Intrusion Prevention – mit allen Bereitstellungs- und Management-Vorteilen einer intergierten und gleichzeitig erweiterbaren Next-Generation Firewall. Das IPS-Software-Blade vervollständigt Check Points Firewall-Schutz und sichert das Netzwerk durch die Überprüfung aller Datenpakete am Gateway zusätzlich ab. Das Intrusion Prevention System ist sehr funktionsreich und bietet beispielsweise auch Geo-Schutzfunktionen. Es wird kontinuierlich mit neuen Schutzmechanismen aktualisiert.

Antivirus
Stoppen Sie eingehende, schadhafte Dateien am Gateway mit Echtzeit-Virensignaturen und Schutzmechanismen vor Anomalien mit der ThreatCloud™ – noch bevor die Nutzer infiziert werden können. Identifizieren Sie mehr als 12 Millionen Malwaresignaturen und über eine Million schädliche Websites mit einem kontinuierlich aktualisierten Netzwerk aus Sensoren, das verlässliche Informationen zu Malware liefert.

Anti-Bot
Anti-Bot erkennt mit Bots infizierte Rechner und schützt vor Schäden durch Bots, indem die „Command and Control“-Kommunikation, die Cyber-Kriminelle hierfür nutzen, blockiert wird. Anti-Bot erhält regelmäßige Aktualisierungen aus der ThreatCloud™.

Firewall
Sichern Sie Ihr Netzwerk mit einer Next-Generation Firewall (empfohlen von den NSS Labs) ab.

Anti-Spam & Email Security
Das Check Point Software-Blade für Anti-Spam & Email Security liefert einen mehrdimensionalen Ansatz, um die Messaging-Infrastruktur zu schützen: Es bietet eine Spam-Erkennung in sehr hoher Genauigkeit und schützt Unternehmen vor einer Vielzahl von Viren und Malware-Bedrohungen, die per E-Mail übermittelt werden.

Application Control
Check Point Application Control bietet die branchenweit stärkste Anwendungssicherheit und Identitätskontrolle für Unternehmen jeder Größenordnung. Die Lösung ermöglicht es IT-Abteilungen, sehr granulare Richtlinien für einzelne Anwender oder Gruppen zu erstellen, um die Nutzung von über 5.000 Web 2.0-Anwendungen und 200.000 Widgets (Elemente auf Websites) zu identifizieren, zu beschränken oder zu blockieren.

URL Filtering
URL Filtering überwacht den Zugriff auf Millionen von Websites – basierend auf Kategorien, Anwender, Anwendergruppen oder Rechner. Hierbei kommen cloudbasierende Technologien zum Einsatz, die kontinuierlich um neue Websites ergänzt werden, um so die Produktivität der Mitarbeiter zu steigern und die Sicherheitsstrategie des Unternehmens zu unterstützen. URL Filtering blockiert den Zugriff auf komplette Websites oder einzelne Seiten einer Website, wobei auch Zeitbeschränkungen oder Bandbreitenbegrenzungen durchgesetzt werden können.

Identity Awareness
Identity Awareness liefert genaue Einblicke in die Aktivitäten der Nutzer, der Nutzergruppen und der Rechner und ermöglicht dank der genauen, identitätsbasierenden Richtlinien eine unvergleichliche Anwendungs- und Zugriffskontrolle.

Logging and Status
Logging and Status verwandelt Daten mithilfe von SmartLog in nützliche Sicherheitsinformationen. SmartLog ist ein hochentwickelter Logdaten-Analyzer, der binnen Sekundenbruchteilen Suchergebnisse liefert und Transparenz in Milliarden von Logdaten-Aufzeichnungen für verschiedene Zeiträume und Domänen in Echtzeit schafft.

Integriertes Sicherheitsmanagement
Unified-Security-Management vereinfacht die umfangreiche Aufgabe, die steigende Zahl an Bedrohungen abzuwehren und alle User und Geräte zu verwalten. Check Points umfassendes und zentrales System für das Sicherheitsmanagement überwacht alle Check Point-Gateways und Software-Blades mit einem Smart-Dashboard, einer intuitiven und grafischen Benutzeroberfläche. Fügen Sie die SIEM-Lösung SmartEvent hinzu, können Sie sicherheitskritische Ereignisse sehr schnell erkennen, Bedrohungen direkt am Event-Screen stoppen und Schutzfunktionen hinzufügen, um Angriffe zu beheben.

Ergänzen Sie genau die Funktionen, die Sie benötigen
Setzen Unternehmen die Threat Prevention Appliance ein, können Sie diese um zusätzliche Software-Funktionalitäten ergänzen, wenn ihr Sicherheitsbedürfnis steigt. Um sich beispielsweise vor Datenverlust zu schützen, können sie das Software-Blade für Data Loss Prevention hinzufügen.