Check Point
SOFTWARE TECHNOLOGIES LTD.

AVANTEC
Competence. Security. Trust.

Die neue Generation der Gefahrenabwehr: erkennt und blockiert zuvor unerkannte Malware

Produktvorteile

- Beste Erkennungsrate bei unbekannter Malware
- Umgehung durch Hacker wird praktisch unmöglich
- Identifiziert und stoppt Angriffe bereits in deren Entwicklungsstadium
- Schnelle Wiederherstellung von Dateien und Bereitstellung sicheren Contents
- Reduziert das Risiko teurer Datenschutzverletzungen oder Ausfälle
- Integrierter Schutz maximiert den betrieblichen Wert und minimiert die TCO

Produktfunktionen

- Malware-Tiefenprüfung auf CPU-Ebene, wo sich Exploits nicht verbergen können
- Schützt eine breite Palette an Dokumenten und gängigen Dateitypen
- Arbeitet mit bestehender Infrastruktur, neues Equipment ist nicht notwendig
- Wandelt wiederhergestellte Dateien in PDFs um, um die Sicherheit zu optimieren, oder liefert das Ursprungsformat
- Integrierte Threat Prevention und Security Management für umfassende Sicherheit und Transparenz über Bedrohungen
- Automatische Aktualisierung von Bedrohungsinformationen mit ThreatCloud™

DIE AKTUELLE LAGE

Der Cyber-Krieg geht weiter. Hacker verändern ihre Strategien und Methoden ständig, um schwer auffindbar zu bleiben und ihre Ziele zu erreichen. Cyber-Kriminelle haben es heute leicht, Exploit-Code, neue Schwachstellen und sogar Wissen mit ihren Verbündeten zu teilen.

Anti-Virus, Next Generation Firewalls und andere zentrale Sicherheitslösungen beschränken sich ausschließlich auf bekannte Bedrohungen – diejenigen mit bekannten Signaturen oder Profilen. In Anbetracht von 106 neuen Malware-Arten, die jede Stunde auftreten, stellt sich die Frage, wie Sie sich vor dem Unbekannten schützen. Traditionelle Sandbox-Lösungen identifizieren „neue“ und unbekannte Malware, brauchen aber Zeit, weshalb sie das Risiko bergen, das Netzwerk zu infizieren, bevor eine Erkennung und Sperrung erfolgt. Leider sind sie zudem anfällig gegenüber Umgehungsversuchen herkömmlicher Sandbox-Erkennungsmethoden.

DIE LÖSUNG

Check Point SandBlast Zero-Day Protection setzt auf Threat Emulation und Threat Extraction, um die Gefahrenabwehr auf das nächste Level zu heben. Dafür kommen eine umgehungssichere Malware-Erkennung und umfassender Schutz vor den gefährlichsten Angriffen zum Einsatz – gleichzeitig wird die schnelle Zustellung der sicheren Inhalte an Ihre Anwender gewährleistet.

Threat Emulation führt eine Tiefenprüfung auf CPU-Ebene aus, was auch die gefährlichsten Angriffe stoppt, bevor Malware die Möglichkeit hat, ihre Tätigkeit aufzunehmen und einer Erkennung zu entgehen. SandBlast Threat Emulation nutzt die Prüfung auf Betriebssystemebene, um eine breite Palette an Dateitypen zu prüfen, einschließlich ausführbarer Dateien und Dokumente. Mit seinen einzigartigen Prüfungsmethoden liefert SandBlast Threat Emulation die bestmögliche Erkennungsrate für Bedrohungen und ist praktisch immun gegen die Umgehungstechniken der Angreifer.

SandBlast Threat Extraction ergänzt diese Lösung durch die sofortige Bereitstellung sicheren Contents oder sauberer und wiederhergestellter Versionen potenziell schadhafter Dateien – so wird der Geschäftsbetrieb nicht unterbrochen.

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT
SandBlast
ZERO-DAY PROTECTION

Check Point SandBlast Zero-Day Protection bietet umfassende Erkennung, Prüfung und Schutz gegen die gefährlichsten Zero-Day- und gezielte Angriffe.

SOFORTIGE ERKENNUNG

Im Gegensatz zu anderen Lösungen nutzt Check Point SandBlast Zero-Day Protection eine einzigartige Technologie, die eine Prüfung auf CPU-Ebene durchführt, um Angriffe abzuwehren, bevor diese starten können. Es gibt tausende Schwachstellen und Millionen verschiedener Malware-Implementierungen, doch gibt es nur sehr wenige Wege, auf denen Cyber-Kriminelle Schwachstellen ausnutzen. Die Check Point SandBlast Threat Emulation Engine prüft den CPU-basierten Befehls-Fluss auf Exploits, die Sicherheitsmaßnahmen auf Hardware- und Betriebssystemebene umgehen sollen.

Durch die Erkennung von Exploit-Versuchen bereits vor einer Infektion wehrt Sandboxing mit Check Point Angriffe ab, bevor diese die Möglichkeit haben, einer Erkennung in der Sandbox zu entgehen.

MEHR MALWARE IDENTIFIZIEREN

Check Point SandBlast Zero-Day Protection führt weitere Untersuchungen mit Threat Emulation auf Betriebssystemebene durch, indem eingehende Dateien abgefangen, gefiltert und in einer virtuellen Umgebung ausgeführt werden. Das Verhalten der Dateien wird gleichzeitig für mehrere Betriebssysteme und Versionen geprüft. Dateien, die verdächtige Aktivitäten zeigen, welche üblicherweise mit Malware in Verbindung stehen, wie Änderungen an der Registry, an Netzwerkverbindungen und die Erstellung neuer Dateien, werden markiert und weiter analysiert. Bösartige Dateien werden vom Eindringen in Ihr Netzwerk abgehalten.

FLEXIBEL UND EINFACH EINZUSETZEN

Check Point SandBlast Threat Emulation unterstützt mehrere Einsatzmöglichkeiten und stellt damit kosteneffiziente Lösungen für Unternehmen jeder Größe bereit. Dateien können von bestehenden Gateways entweder an einen Cloud Service oder an eine Appliance vor Ort gesendet werden.

Installiert als zusätzliches Software Blade auf dem Gateway kann Check Point SandBlast Threat Extraction für die ganze Organisation eingesetzt oder nur für bestimmte Personen, Domains oder Abteilungen implementiert werden. Die Administratoren können mitgelieferte Benutzer und Gruppen ganz nach ihren Bedürfnissen konfigurieren, was einen schrittweisen Einsatz im Unternehmen erleichtert.

PROAKTIVER SCHUTZ MIT SOFORTIGER BEREITSTELLUNG SICHEREN CONTENTS

Mit Threat Protection müssen Sie keine Kompromisse zwischen Geschwindigkeit, Abdeckung und Genauigkeit eingehen. Im Gegensatz zu anderen Lösungen kann Check Point SandBlast Zero-Day Protection im Erkennungs- wie im Abwehrmodus eingesetzt werden, ohne den Geschäftsbetrieb zu unterbrechen.

Unsere Threat Extraction-Komponente in Check Point SandBlast eliminiert Bedrohungen, indem risikobehaftete Inhalte, wie Makros oder eingebettete Links, entfernt werden und das Dokument ausschließlich mit sicheren Elementen wiederhergestellt wird.

Im Gegensatz zu Erkennungs-Technologien, die eine gewisse Zeit für die Suche und Identifikation von Bedrohungen benötigen, bevor sie diese sperren können, eliminiert Threat Extraction die Risiken präventiv und gewährleistet die sofortige Zustellung sicherer Dokumente.

AVANTEC
Competence. Security. Trust.

AVANTEC AG ▪ Badenerstrasse 281
CH-8003 Zürich ▪ www.avantec.ch