Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point SandBlast AGENT

SANDBLAST AGENT: EFFEKTIVER SCHUTZ VON ARBEITSPLÄTZEN

70%

der erfolgreichen Cyber-Angriffe starten vonn PC Arbeitsplätzen aus (IDC)

$1M

minimum Schadensumme pro Angriff auf kleine oder mittlere Unternehmen

63% der Angriffsversuche sind erfolgreich

#1

Ergebnisse des "2019 NSS Labs Breach Prevention Systems Test" zeigten, dass SandBlast Agent die höchste Sicherheitseffizienz bietet

100%

protection

SandBlast Agent Nutzer wurden bisher NICHT von den besonders hochkarätigen und gezielten (insbesondere Ransomware) Angriffen betroffen*

* Stand: Ende Oktober 2019

ZUM SCHUTZ VOR GEZIELTEN ANGRIFFEN REICHEN VIRENSCHUTZ UND VERSCHLÜSSELUNG NICHT AUS

In der dynamischen Welt von heute profitieren Mitarbeiter und Organisationen von den Vorteilen der Produktivitäts-steigerungen, die das mobile Arbeiten bietet. Es ist für die Unternehmen effizient, wenn Mitarbeiter von überall aus arbeiten; unterwegs E-Mails lesen, von zu Hause oder während Dienstreisen auf Dateien und Ressourcen zugreifen können. Um dies sicher zu ermöglichen, ist ein zuverlässiger und moderner Schutz des Arbeitsplatzes vor Cyber-Bedrohungen erforderlich.

Herkömmliche Antivirenprogramme können nur den Teil der Angriffe blockieren, für den bereits Signaturen vorhanden sind. Mit den verfügbaren Mitteln zur schnellen Modifizierung von bekannten Angriffsvarianten können Hacker die traditionelle Verteidigung leicht umgehen. Somit werden in kürzester Reaktionszeit groß angelegte Angriffe mit beträchtlichem Schaden durchgeführt. Die Verhinderung von Angriffen, einschließlich bisher unbekannter (Zero-Day) Angriffe auf Arbeitsplatzebene, wird zu einer wesentlichen Herrausforderung für die Sicherheitsarchitektur von Unternehmen.

> Social Engineering, Phishing, externes Wi-Fi, verschlüsselter Datenverkehr, Flash-Laufwerke und unbemerktes Fortbewegen von Angreifern können nur auf der Arbeitsstation selbst gestoppt werden, wobei fortschrittliche Engines zur Bedrohungsabwehr zum Einsatz kommen.

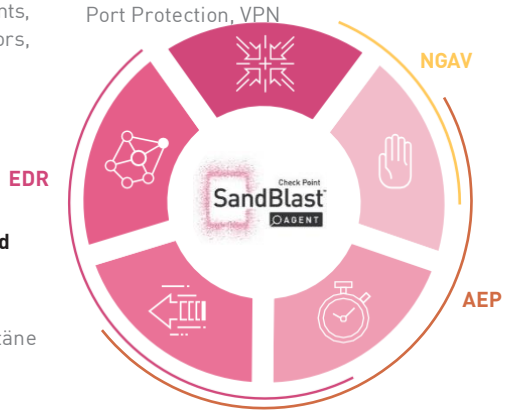
VOLLSTÄNDIGER SCHUTZ DES ARBEITSPLATZES

Untersuchen und Berichten

Attack chronicle; sequence of events, type of attack, entry point, indicators, current status, damage, MITRE ATT&CK

Reduzierung der Angriffsfläche

Firewall, Application Control, Port Protection, VPN



Prävention

Anti-Virus, Threat Extraction, Threat Emulation, Zero Phishing, FW, Anti-Exploit, NGAV

Blockieren Sie die Bedrohung und mildern Sie die Auswirkungen

Anti-Bot, FW, Anti-Ransomware, forensische Maßnahmen, Quarantäne

Verdächtiges Verhalten erkennen

Behavioral Guard, Anti-Ramsomware, Anti-Evasion, Threat Hunting, Anti-Fileless, Anti-Bot, Machine Learning

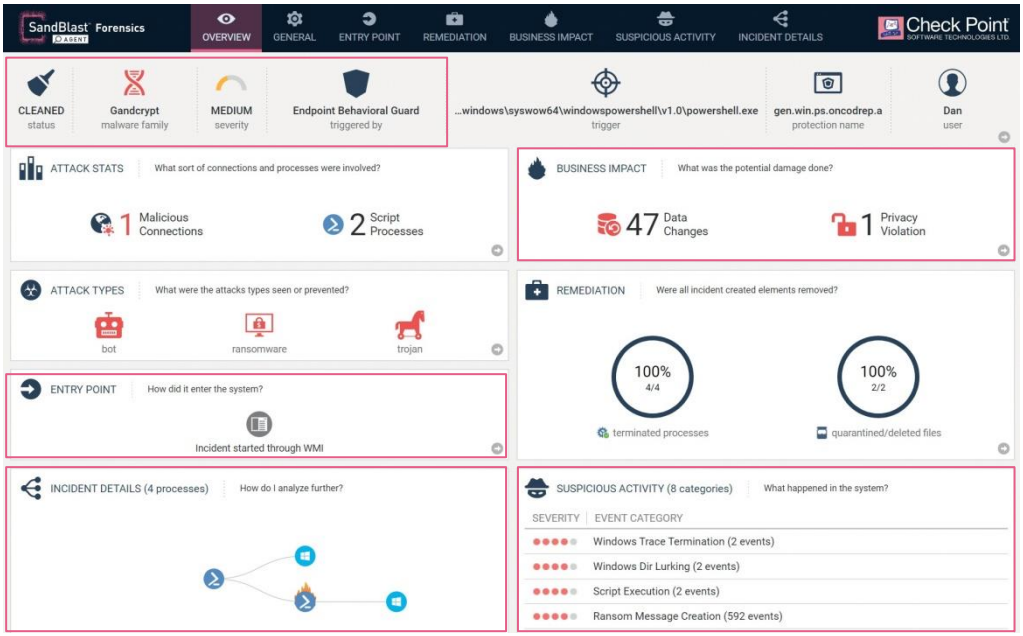
SANDBLAST AGENT – EINZIGARTIGE UND EFFEKTIVE KONTROLLEN

Vollständiger Schutz über SandBlast Agent wird durch den Einsatz einer Reihe einzigartiger Abwehrtechnologien ermöglicht, die in den verschiedenen Phasen des Angriffs aktiv werden. Datenverschlüsselung, VPN, lokale Firewall und Anwendungskontrolle ermöglichen es, einen Angriff zu verhindern.

Im Falle eines Angriffs schränken Zero-Phishing und URL-Filterung den Zugriff auf bösartige Websites ein, der Virenschutz schützt vor bekannten Bedrohungen. Die Threat Extraktion (sofortige Konvertierung von Dateien in eine sichere Form) und die Threat Emulation (dynamische Analyse) blockieren unbekannte Malware. Eine Reihe von Verhaltensanalyse-Technologien wie Anti-Evasion, Anti-Exploit, Anti-Bot, Anti-Ransomware und weitere, verfolgen und blockieren gefährliche Aktivitäten.

SBA analysiert ständig das Systemverhalten (Operationen mit Dateien und Prozessen, Registrierungsänderungen und Netzwerkverbindungen) und speichert Ereignisinformationen lokal auf der Festplatte. Im Falle eines Vorfalls ermöglichen diese Informationen nicht nur, das gesamte Angriffsschema zu verstehen und bis zum Anfang zu verfolgen, sondern auch, das System in seinen ursprünglichen Zustand zurückzuversetzen, einschließlich der Wiederherstellung beschädigter Dateien.

FORENSISCHE ANALYSE UND AUTOMATISIERTE REAKTION AUF VORFÄLLE



Triage: Sofortige Maßnahmen erforderlich?

Was waren die Auswirkungen?

Einstiegspunkt: Was wurde zuerst kompromittiert

Vollständige Angriffs-Ereigniskarte.

War es ein echter Angriff?

VERFÜGBARE PAKETE

Funktionen/SBA Pakete	Basic	Advanced	Complete
Centralized deployment and management *	✓	✓	✓
Access Control, Port Protection, VPN	✓	✓	✓
Next-Generation Anti-Virus (NGAV)**	✓	✓	✓
Firewall, Application Control, Port Protection, VPN	✓	✓	✓
Zero-Phishing, URL Filtering	✓	✓	✓
Endpoint Detect and Response (Forensic Analysis)	✓	✓	✓
Threat Emulation and Extraction		✓	✓
Data Protection (Full Disk Encryption and Media Encryption)			✓

* Alle Pakete werden über die lokal oder in der Cloud bereitgestellte SmartEndpoint Management-Plattform verwaltet.

**Alle SBA-Pakete können sowohl in die bestehende Anti-Virus-Lösung integriert werden als auch diese dank der integrierten Anti-Virus-Engine vollständig ersetzen.

KONTAKT

Thomas Tschan
Threat Prevention Sales Manager
ttschan@checkpoint.com