CHECK POINT
ADVANCED ENDPOINT SECURITY

ADVANCED ENDPOINT SECURITY

Benefits

- Protect endpoints from sophisticated attacks and zero-day threats
- Secure data at rest, in use and in transit on endpoint devices
- Reduce security gaps by monitoring, managing, and enforcing user and machine based policies
- Enable deep understanding of security events for faster response

Features

- Advanced threat prevention, data security and forensics for complete endpoint protection
- Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content
- Single console manages endpoint threat prevention, data security, network access, and compliance

"A major value with Check Point is centralized control; it gives us a much higher degree of confidence knowing that our entire endpoint is more secure than it's ever been."

Industry: Government

OVERVIEW

Unprotected endpoints put an entire business at risk from threats, data loss, and unauthorized access. To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Creating and managing new policies for desktops, laptops, Macs, and other devices quickly becomes complicated. In addition, engaging and educating users can take valuable time away from administrators. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well.

SOLUTION

Give your security administrators the power to enforce, manage, report, and educate users under one console. A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization. Manage our full suite of Endpoint Security Software Blades for PCs and Mac under one console. Administrators can easily manage multiple enforcement capabilities for a cohesive multi-layered defense.

ZERO-DAY THREAT PREVENTION

- SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including Threat Emulation, Threat Extraction, Anti-Bot and Zero Phishing.

ACTIONALABLE INCIDENT ANALYSIS

- SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity.

ACCESS CONTROL

- Firewall protects endpoints by controlling inbound and outbound traffic.
- Compliance Check ensures compliance while accessing the corporate network.
- Remote Access VPN secures access to corporate resources when remote.

DATA SECURITY

- Full Disk Encryption secures the entire drive.
- Media Encryption encrypts removable storage media.
- Port control enables management and auditing of all endpoint ports.
- Capsule Docs seamlessly protect documents, ensuring access to authorized users.

CHECK POINT SandBlast™ AGENT

PREVENTS ZERO-DAY MALWARE

SandBlast Agent extends the proven protections of SandBlast Zero-Day Protection to endpoint devices, as well as to web browsers. Threat Extraction reconstructs downloaded files in seconds, eliminating potential threats and promptly delivering a safe version to users. At the same time, Threat Emulation (sandboxing) discovers malicious behavior and prevents infection from new malware and targeted attacks by quickly inspecting files in a virtual sandbox.

SandBlast Agent Complete	
Threat Emulation with CPU-Level Detection	✓
Threat Extraction	✓
Anti-Phishing	✓
Credential Protection	✓
Anti-Ransomware	✓
Anti-Bot	✓
Automated Forensics	✓

PROTECTS AGAINST RANSOMWARE

Ransomware impacts businesses by encrypting data files and demanding ransom for their retrieval. Anti-Ransomware uses a behavioral analysis engine capable of detecting and remediating ransomware infections. The signature-less technology works both online and offline. Ransomware infections are automatically and fully quarantined based on SandBlast Agent's forensic analysis and files that were encrypted prior to the attack containment are restored.

BLOCK ZERO-DAY PHISHING ATTACKS

Our Zero Phishing uses dynamic analysis and advanced heuristics to identify and prevent access to new and unknown phishing sites targeting user credentials through web browsers in real-time. This capability prevents theft of corporate credentials from potential breaches of passwords on third party sites by alerting users when violating the corporate password re-use policies.

IDENTIFY AND CONTAIN INFECTIONS

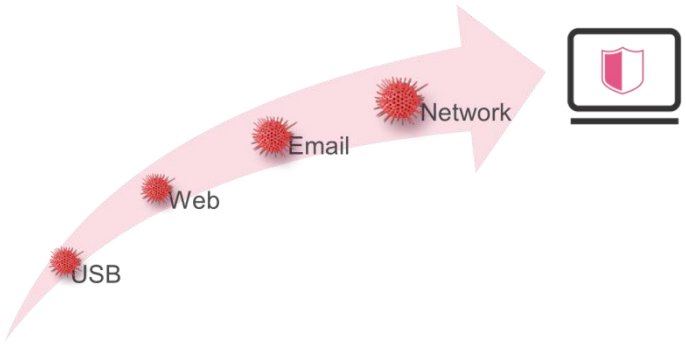
With a local version of Anti-Bot security protection, continuously updated with the latest Threat Intelligence data via ThreatCloud, SandBlast Agent identifies and blocks bot communications with command and control servers to contain and quarantine any infected hosts.

HARNESS THE POWER OF THE CLOUD

Unlike other vendor products who do zero-day theat analysis on your endpoints, we offload processing to the cloud (Check Point or on premise), letting your employees work safely no matter where they are without compromising on productivity. OS emulation environments include Microsoft Windows XP, 7 and 8.1. We detect malware in over 40 file types, including: Adobe PDF, Microsoft Word, Excel, and PowerPoint, Executables (EXE, COM, SCR), Shockwave Flash (SWF), Rich Text Format (RTF) and Archives.

DETECT THREATS FROM ANY SOURCE

SandBlast Agent protects from threats delivered via web downloads, content copied from removable storage devices, links or attachments in email messages, lateral movement of data and malware between systems on a network segment and infections delivered via encrypted content.



THIRD-PARTY INTEGRATION

SandBlast Agent works in conjunction with Antivirus and other security solutions from Check Point, as well as from other vendors. It enhances the detection capabilities of existing Antivirus products, enabling protection from advanced threats and providing actionable incident analysis. When triggered by an event or investigation request by another Check Point component or third party solution, endpoint forensics logs are analyzed to generate reports viewable in SmartEvent and SmartLog.

ACTIONABLE INCIDENT ANALYSIS

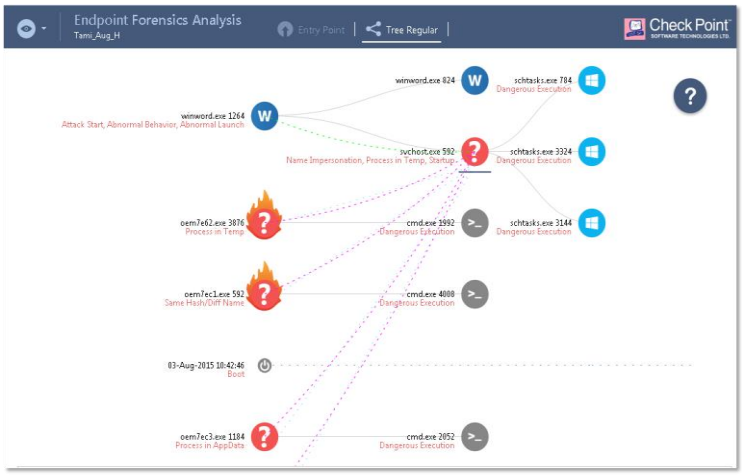
The forensics analysis process automatically starts when a malware event occurs. Using a combination of advanced algorithms and deep analysis of the raw forensic data, it builds a comprehensive incident summary. The summary provides key actionable attack information, including:

Malicious events – What evidence of suspicious behavior was detected throughout the attack lifecycle?

Entry point – How did the attack enter the network? What were the main elements used in the attack? How was the attack initiated?

Damage scope – What did the malware do once activated that may impact the business? What data was compromised and/or copied externally?

Infected hosts – Who else or what else is affected?



Detailed Incident Timeline

This comprehensive attack diagnostics and visibility supports remediation efforts. System administrators and incident response teams can swiftly and efficiently triage and resolve attacks, getting your organization back to business as usual quicker.

> *"SandBlast Agent found multiple threats within the first days we deployed it. Not only was Check Point more effective in identifying sophisticated attacks—it also eliminated them before they could cause damage. It actually does its job better than we expected. It's fantastic."*
>
> Michael Brine
> Infrastructure Manager
> Community Newspaper Group

FULL VISIBILITY OF SECURITY EVENTS

SandBlast Agent can trace and report the steps taken by malware, including zero -day threats. Continuous monitoring ensures that data is available after a completed attack, even those that remove files and other indicators of compromise left on the system.

CONTINUOUS MONITORING
• Files affected
• Processes launched
• System registry changes
• Network activity

AUTOMATIC ANALYSIS

When a security event is detected, SandBlast Agent automatically builds actionable forensics reports with key information.

AUTOMATIC TRIGGERS
• Anti-Bot detection on the network or on the endpoint
• Threat Emulation detection on the network
• Check Point Antivirus detection on the endpoint
• Third-party Antivirus detection on the endpoint
• Manual Indicators of Compromise (IoCs)
DAMAGE DETECTION
• Automatically identify: Data exfiltration, data manipulation or encryption, key logging
ROOT CAUSE ANALYSIS
• Trace and identify root cause across multiple system restarts in real-time
MALWARE FLOW ANALYSIS
• Automatically generates interactive graphic model of the attack flow
MALICOUS BEHAVIOR DETECTION
• Over 40 malicious behavior categories
• Hundreds of malicious indicators

DETAILED INCIDENT REPORTS

The forensics capability within SandBlast Agent allows you to view event reports, triggered from the gateway or endpoint itself, from a central location using SmartEvent. Security Administrators can also generate reports for known malicious events, providing a detailed cyber kill chain analysis. These reports provide actionable incident analysis, accelerating the process of understanding the complete attack lifecycle, damage and attack vectors.

ENDPOINT DATA SECURITY SOLUTION

Most corporate laptops and PCs store proprietary data on their drives, and many users regularly work outside of a secure corporate environment. A data breach from a lost, stolen or compromised laptop can result in costly fines, lawsuits and lost revenue. **Full Disk Encryption** secures the entire drive. **Media Encryption and Port Protection** secure removable media. **Remote Access VPN** provides secure access to corporate resources when traveling or working remotely.

DOCUMENT SECURITY

Document sharing is a frequent source of business data loss, especially when mobile users are involved. Check Point **Capsule Docs** is a secure mobile document management system that follows your documents wherever they go, making sure you have complete control over who is accessing sensitive data and what they can do with it.

FULL DISK ENCRYPTION

Check Point Full Disk Encryption (FDE) provides transparent security for all information on all endpoint drives, including user data, operating system files and temporary and erased files. For maximum data protection, multi-factor pre-boot authentication ensures user identity before the operating systems loads, while encryption prevents data loss from theft.

MEDIA ENCRYPTION, PORT PROTECTION

Check Point Media Encryption and Port Protection provides centrally enforceable encryption of removable storage media such as USB flash drives, backup hard drives, CDs and DVDs, for maximum data protection. Educating users on when to share and not share corporate data via UserCheck™ prevents future data sharing mistakes. Port control enables management of all endpoint ports, plus centralized logging of port activity for auditing and compliance.

REMOTE ACCESS VPN

Check Point Remote Access VPN provides users with secure, seamless access to corporate networks and resources when traveling or working remotely. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint system compliance scanning and encryption of all transmitted data.

COMPREHENSIVE ENDPOINT SECURITY

DATA SECURITY	
Full Disk Encryption	✓
Media Encryption	✓
Port Protection	✓
Capsule Docs	✓
ACCESS CONTROL	
Firewall	✓
Application Control	✓
Compliance	✓
Remote Access VPN	✓
THREAT PREVENTION	
Antivirus	✓
SandBlast Agent Threat Emulation	✓
SandBlast Agent Threat Extraction	✓
SandBlast Agent Anti-Bot	✓
SandBlast Agent Anti-Ransomware	✓
SandBlast Agent Zero Phishing	✓
SandBlast Agent Forensics	✓

ORDERING ENDPOINT SECURITY

PACKAGE	SKU
Access Control	CPEP-ACCESS-1Y
	CPEP-ACCESS-RENEWAL-1Y
	CPEP-ACCESS-P
Data Security[1]	CPEP-DATA-1Y
	CPEP-DATA-RENEWAL-1Y
	CPEP-DATA-P
Capsule Docs	CP-CPSL-WORK-1Y
Antivirus	CPEP-AV-1Y
	CPEP-AV-RENEWAL-1Y
Anti-Ransomware	CPEP-AR-1Y
SandBlast Agent	CPEP-SBA-1Y
	CPEP-SBA-RENEWAL-1Y
SandBlast NGAV	CPEP-SBA-NGAV-1Y
	CPEP-SBA-NGAV-RENEWAL-1Y
Complete Security[1]	CPEP-COMPLETE-1Y
	CPEP-COMPLETE-RENEWAL-1Y

[1] Capsule Docs sold separately