SandBlast Agent FAQ

What is Check Point SandBlast Agent?

Check Point SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including following elements:

1. **Threat Extraction**
   Proactively prevents malicious content from reaching users by quickly delivering safe reconstructed copy, while original files are being inspected for potential threats.
2. **Threat Emulation**
   Detects zero-day and unknown attacks. Files which are copied or downloaded to the endpoint are sent to sandbox for emulation to detect evasive zero-day attacks.
3. **Anti-Ransomware**
   Uses a purpose-built behavioral analysis engine capable of detecting and remediating ransomware infections on both online and offline endpoints. Ransomware infections are automatically and fully quarantined based on SandBlast Agent's forensic analysis. Automatically restores files that were encrypted prior to the attack containment.
4. **Zero Phishing Technology**
   Blocks phishing sites - even those never seen before. Prevents use of corporate credentials on external websites. For details refer to *SandBlast Agent for Browsers FAQ* .
5. **Anti-Bot**
   Monitors the endpoint for Command-and-Control communications, alerting administrators to infected devices, even if the endpoint is behind NAT, and blocks C&C communications.
6. **Forensics and Automated Incident Analysis**
   Provides actionable insights into a breach or infection. Helps businesses avoid expensive manual analysis. Automated remediation of malware – both known and unknown.

I am using SandBlast Network. Do I still need Check Point SandBlast Agent?

Yes. Check Point SandBlast Agent extends your enterprise network's advanced zero-day protection to web browsers and endpoint devices. It also adds anti-ransomware, zero-phishing, forensics and automated incident analysis making malware detections actionable.
SandBlast Agent covers some attack vectors not seen on the network such as when endpoint devices roam outside the network or when files are copied directly to the endpoint via external storage devices. Anti-ransomware protects even in the offline mode by automatically restoring encrypted files.

I do not have a Check Point gateway, should I use SandBlast Agent?

Yes, absolutely.
SandBlast Agent is an independent advanced security solution for endpoint devices. You can deploy SandBlast Agent, while using any security gateway on your enterprise network, and still benefit from the protection of SandBlast Agent on your endpoint systems.

I already have an endpoint security /Antivirus solution; do I still need SandBlast Agent?

Yes. SandBlast Agent will compliment your existing solution in several key ways:

- Adding advanced protections from threats that can bypass traditional AV solutions.
- SandBlast Agent adds Anti-Ransomware capabilities that can detect, prevent and automatically remediate and recover ransomware attacks, even in the offline scenario.
- Adding zero phishing technology to prevent zero-day malware and socially engineered attacks from reaching users via the web
- SandBlast Agent can easily integrate with your AV solution providing automated forensic analysis of detections made by your AV product.
- For customers using other Check Point endpoint security products, SandBlast Agents augments and complements it within the same unified security architecture.

To meet the endpoint protection requirement of an organization, should I recommend SandBlast Agent OR Capsule Cloud?

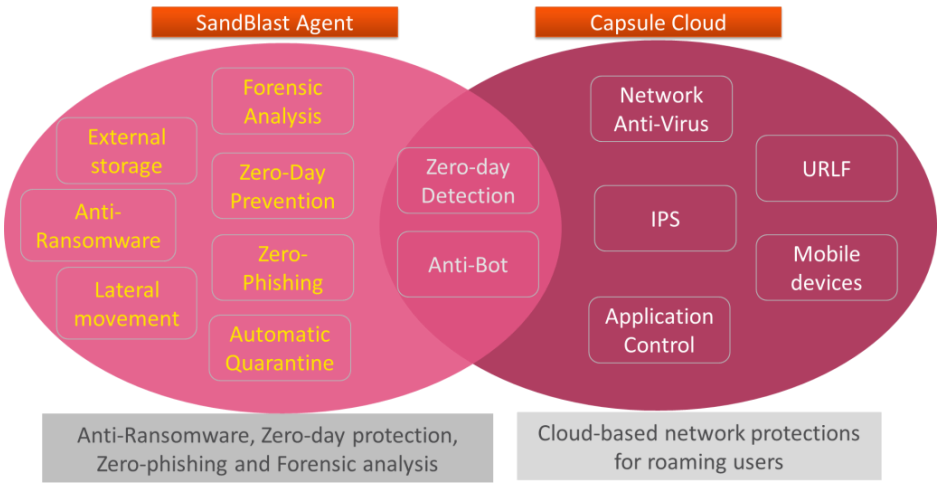
Both SandBlast Agent and Capsule Cloud provide endpoint protection for different requirements:

Recommend SandBlast Agent:

- For organizations looking for **zero-day protection** for infrastructure, especially **endpoints**
- For organizations concern about ransomware or were previously hit by ransomware.
- For customers interested in an Endpoint Detection and Response (**EDR**) solution
- When talking to SOC / **Incident response** teams
- When competing with PAN Traps, FireEye HX/MIR, Cisco AMP, Carbon Black, Tanium, etc

Recommend Capsule Cloud:

- For organizations looking for **network security as a service** in the cloud
    - When competing with Zscaler, Cato Networks, and similar cloud services



Does SandBlast Agent protect itself and its data from malware?

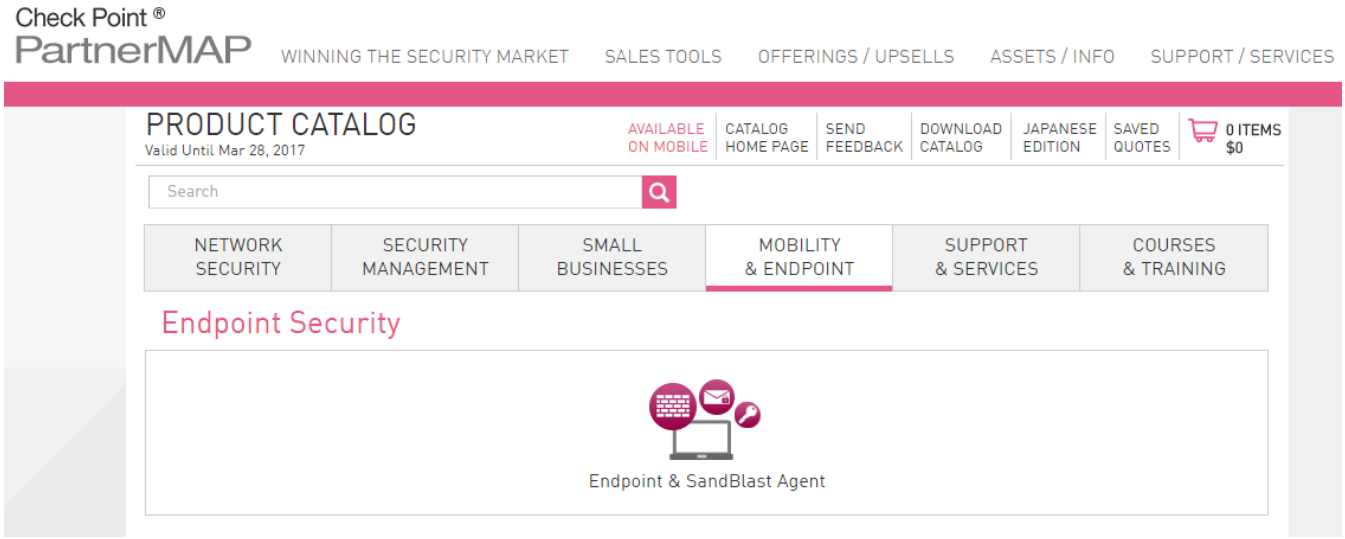
Yes. SandBlast Agent self-protection utilizes state-of-the-art driver-based lockdown and concealing all of its data, executable elements, and anti-ransomware's file snap-shots repository. Thus it prevents, file deletion by ransomware, and any unauthorized access or tampering.

Packaging and Pricing

What is the SKU and pricing for SandBlast Agent?

Check Point SandBlast Agent is sold under an annual subscription model. It is being introduced at a rate of $35 per user account per year, with the SKU *CPEP-SBA-1Y* for a one year subscription. The Annual price includes standard support.

Please note that SKU and pricing information is subject to change at any time in the future. For the latest information on pricing and packaging, please refer to the Check Point product catalog on Check Point PartnerMAP.



Is a separate license required in order to use the SandBlast cloud service?

No separate license needed. The SandBlast Agent license includes the contract for using SandBlast cloud service for Threat Emulation and Threat Extraction.

Can we sell SandBlast Agent to customers who do not have NGTX gateways or SandBlast appliances?

Yes, definitely. Such customers will work with the cloud and TE cloud quota is included in the SandBlast agent price.

Can I combine SandBlast Agent with other Check Point Endpoint blades?

Yes. SandBlast Agent is fully integrated with Check Point Endpoint security, allowing customers to deploy a single agent with comprehensive security coverage and unified management. The two products are sold separately. Endpoint Security requires an *endpoint container license* in addition to the endpoint blades or packages. SandBlast Agent does not require an endpoint container license. Once purchased, the two products will be delivered as a unified agent.

What protection capabilities are featured in the different packages?

See table below for feature composition in three distinct packages on SandBlast:

Features	Endpoint Complete Protection Suite	SandBlast Agent	SandBlast Anti-Ransomware	SandBlast Agent for Browsers (COMING SOON)
Deployment	Endpoint Agent	Endpoint Agent	Endpoint Agent	Browser Extension
Management	SmartCenter	SmartCenter	SmartCenter	Cloud
Anti-Ransomware	✓	✓	✓	
Incident analysis & quarantine	✓	✓	✓	
Forensics report	✓	✓		
Browser extension	✓	✓		✓
Emulation & Extraction	✓	✓		✓
Zero Phishing	✓	✓		✓
Anti-Bot	✓	✓		
Anti Virus	✓			
Full Disk Encryption & Media Encryption	✓			
Firewall & VPN	✓			

NOTE:

- SandBlast Agent for Browsers is currently available as a part of SandBlast Agent managed through SmartCenter.
- SandBlast Agent for Browsers is planned to be available as an independent cloud managed product in Q2 2017.

Deployment

Which operating systems are supported by SandBlast Agent?

SandBlast Agent is available for Windows 7, 8 and 10; and for Windows Server 2008 R2 , 2012, and 2012 R2.

Can SandBlast Agent be deployed alongside my existing endpoint/AV product?

Yes. In fact, SandBlast Agent enhances the power of existing endpoint/AV product by adding CPU- level zero-day protection which can detect threats that evade AV detection, and by triggering automated incident analysis for events detected by the AV product.

How is SandBlast Agent managed?

SandBlast Agent is managed by Check Point Endpoint Management. Security monitoring is done via SmartEvent & SmartLog. Just like monitoring security events from any other Check Point product. This enables the security admin to monitor all security events using a single security console.

Before I deploy the complete SandBlast Agent package, I like to try SandBlast Agent for Browsers. How is it being deployed and managed?

SandBlast Agent for Browser is an ideal fit for organizations looking for rapid deployment with minimal footprint. It is deployed using standard endpoint management tools, such as GPO (Group Policy Object) to push policy to user endpoint devices.

Threat Emulation & Threat Extraction

How are incoming files selected to be emulated and/or extracted?

All files downloaded over web, copied to the local drive (e.g. via USB drive), and files created with active elements (such as by a compiler) are sent for Threat Emulation. Only the files downloaded over web are sent for Threat Extraction also.

Before sending files, SandBlast Agent validates the file hash signature with the SandBlast Cloud service – if it is a known good or bad file, then the verdict is provided immediately and the file is not uploaded for emulation. Specifically, files previously sent to emulation by a security gateway will not be sent for emulation by the SandBlast Agent.

Where are files emulated?

Based on customer configuration, files are sent either to SandBlast service or to the on-premises SandBlast Appliances.

Since SandBlast Agent uses SandBlast service, what will happen when files are copied or created on local drive while endpoint is not connected to Internet?

SandBlast Agent lets files through – avoiding any impact on user experience. SandBlast Agent will check the files with Threat Emulation cloud as soon as endpoint connects to the Internet. If a file is found to be infected, it will be quarantined, and forensic analysis will be triggered.

NOTE: *Offline infection is a rare condition because:*

1. *Now-a-days most PCs are online all the time*
2. *Most infections come through web downloads, not from USB storage*

Therefore in real life, offline infection is not a major infection vector.

Where can I see the Threat Emulation reports?

Threat Emulation reports can be viewed in SmartEvent.

Anti-Ransomware

Our AV has successfully stopped ransomware, why do I need Anti-Ransomware?

Traditional AV can be effective in detecting attacks by known ransomware. However, ransomware is constantly evolving, mutating and incorporating new evasion tricks. Many ransomware attacks are capable of evading AV detection, as evident by the numerous infections suffered by businesses around the world – virtually all of which are utilizing AV. Moreover, signature-less and behavioral-analysis based Anti-Ransomware automatically recovering encrypted files in case ransomware infects endpoint, even in the offline scenario.

If I use Anti-Ransomware feature, do I still need my endpoint AV?

We recommend using endpoint AV on all endpoints – it is still an important part of an effective multi-layered approach to security, and it is still an effective means for preventing basic malware attacks that are still quite prevalent.

SandBlast Agent can be deployed alongside any third party AV or as a single unified product with Check Point Anti-Malware or with Check Point's full endpoint suite for an integrated solution with a single agent and management.

Can Anti-Ransomware detect and block Ransomware attacking Master Boot Record (MBR)?

Yes. Check Point Anti-Ransomware protect against ransomware, such as Petya, GoldenEye, etc.

How Check Point Anti-Ransomware works? What are the steps involve?

Check Point Anti-Ransomware works in four distinct architectural layers:

1. Real-time behavioral analysis to identify ransomware before any damage
2. Identify illegitimate data encryption by ransomware that evades behavioral analysis
3. Automated forensic analysis and quarantine of malware and trace back the attack activities
4. Restores the data immediately if encryption started before malware quarantined

How does Anti-Ransomware distinguish between legitimate and illegitimate encryption to avoid false-positives?

Check Point Anti-Ransomware detection is based on behavioral analysis, which is based on Check Point's own fundamental and extensive research and wide experience. False-positive rate for this technology is extremely low.

Do you take snapshots of files on RW access network share?

Not currently. It is on roadmap by end of 2017.

Where in the endpoint it saves the files snapshots?

File snapshots are stored in the directory “SandBlastBackup” on every volume in endpoint machine.

Doesn’t Anti-ransomware engine use Machine learning technology?

Machine learning is one form of behavioral analysis, which is used by our Anti-ransomware engine. It used broader aspects that would identify a process or a series of events as belonging to ransomware. Check Point’s forensic based algorithms offer the best behavioral analysis specific to ransomware.

Does backup and restore rely on shadow copy?

No. We implement our own secure storage for backup using local storage. This is not a traditional backup, but snapshot (a short term backup), that focuses on most recent version of file. We keep deleting (purging) older versions.

How much storage is required for Anti-Ransomware’s file snapshots?

We recommend allocating 1GB of storage for file snapshots. The storage capacity can be configured by the customer. This allocation grows or shrinks dynamically based on Anti-ransomware engine’s suspicion whether file change activity is legitimate or not.

Do I still need my conventional backups if I use the Anti-Ransomware feature?

Yes. Anti-Ransomware focuses only on recovering data encrypted by ransomware, not on general purpose backup. In order to ensure data recovery in other cases such as disk failure, a conventional backup is always and highly recommended.

How are file snapshots protected?

File snapshots are protected by the SandBlast Agent self-protection kernel driver, which prevents any attempt to access the data by processes that are not part of SandBlast Agent and signed by Check Point.

What does IT organization require to do when Anti-Ransomware detects an event?

Nothing. Anti-ransomware can automatically recover files affected by ransomware. It keeps user notified at all steps. It is self-catered and highly interactive, and provides user with options to review and restore files at different location.

SandBlast Agent for Browsers

What is Check Point SandBlast Agent for Browsers?

An integral part of SandBlast Agent package, *Check Point SandBlast Agent for Browsers* is an extension or plugin for browsers that proactively prevents zero-day malware and socially engineered attacks from reaching users via the web. It uses Threat Emulation and Threat Extraction technology delivered via SandBlast Service in Check Point cloud.

In addition, the browser extension includes the zero phishing technology for real-time protection from new and unknown phishing web-sites, and prevents re-use of corporate credentials. The browser extension can also be used as separate product that can provide real-time zero-day protection only for web-downloads.

How is the Browser Extension deployed and managed?

The extension is automatically installed alongside the SandBlast Agent. As it receives the same security profile as the Agent, there is no need for any individual configuration process.

What browsers are supported by the extension?

Google Chrome is currently supported by the SandBlast browser extension. Support for additional browsers - Internet Explorer and Firefox, is planned to be available in Q2 2017.

NOTE: For details on how to use the *Check Point SandBlast Agent for Browsers* as independent product, refer to product SandBlast Agent for Browsers FAQ

Anti-Bot

How does Check Point Anti-Bot receive its intelligence?

Anti-Bot in SandBlast Agent uses the same logic and same signatures used by network-based anti-bot. It communicates with Check Point ThreatCloud for real-time intelligence on bot hideouts and communication patterns.

Forensics

What forensic information is collected?

SandBlast Agent collects ongoing activity information from the Operating System. The collected information includes process activity, network communications, registry changes, file-system access and many more indicators that are probed by the agent's sensors.

Where is the forensic data stored?

The forensic data collected by SandBlast Agent is stored locally on the endpoint itself. The stored data is protected from unauthorized access or tampering in SandBlast Agent's secure log structure.

How much disk space does the forensic data occupy?

Forensic analysis typically requires approximately 1GB of hard-disk storage for one month of data. The amount of collected data may vary based on usage patterns of the PC. When the allocated storage is consumed, new records will replace old ones. The amount of disk space allocated to the storage of the forensics data is configurable.

Where can I see the forensic reports?

Forensics reports can be viewed on either SmartEvent or SmartLog. SmartEvent is highly recommended as it provides advanced event correlation, filtering and searching of logs allowing for a more productive workflow for security event monitoring and response. For instance, using SmartEvent, forensic analysis reports are grouped alongside the network based events which triggered the analysis.

Can 3rd party AV detections trigger a forensic analysis?

Yes. Most endpoint products provide a simple way to trigger a command-line instruction on AV detections and this mechanism can be easily used for triggering a forensic analysis. SKs describing where to enable this setting on the 3rd party AV management are available for common AV vendors.

