Check Point
SOFTWARE TECHNOLOGIES LTD.

WE SECURE THE FUTURE

SandBlast Agent for Browsers

With Zero Phishing Technology

FAQ

What is Check Point SandBlast Agent for Browsers?

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.

The security protections included in *Check Point SandBlast Agent for Browsers* are:

A. Real-Time Zero-Day Protection for Web-Downloads

- **Threat Extraction**
  Prevents malicious content within downloaded files from reaching users by quickly delivering a safe reconstructed copy of the file, while the original file is being inspected for potential threats by threat emulation.
- **Threat Emulation**
  Sends files to the *Check Point SandBlast Service* for Threat Emulation. Threat Emulation performs OS and CPU level sandboxing of files to detect and block unknown malware and zero-day threats.

B. Zero Phishing

- **Real-time protection from new and unknown phishing sites**
  Protects users from advanced phishing sites attempting to steal credentials and private information. As soon as users click on an input field, Zero Phishing initiates a mixture of static, heuristic and machine learning-based analysis of the sites attributes - URL, top-level domain, and IP analysis, etc.
- **Protects user credentials and corporate passwords**
  Prevents reuse of corporate credentials on 3rd party sites. An attempt to use a password from an admin-defined protected domain on an external site will create both a security log and display a warning to the user.

How is it different from SandBlast Agent?

SandBlast Agent for Browsers provides real-time protection for the most common threats of malicious web-downloads and phishing emails, delivered with a minimal footprint as a browser extension. *SandBlast Agent for Browsers* is a component of *SandBlast Agent*, which includes zero-day protection for additional threat vectors beyond web- downloads (including USB file transfer, lateral movement, etc.), as well as Anti-Ransomware, Anti-Bot Command & Control detection, Forensics & Automated Incident Analysis.

What are key differentiators of SandBlast Agent for Browsers?

- **Real-time Browser Protection with the Highest Detection Rate** – Blocks unsafe content using Check Point SandBlast™ market-leading technologies, Threat Emulation with CPU-level evasion detection, and Threat Extraction.
- **Zero Phishing** – Protects from phishing attacks using real-time dynamic analysis and advanced heuristics. Prevents re-use of corporate credentials on public websites.
- **Simplicity, with Minimal Footprint** – Implemented as a browser-plugin, *SandBlast Agent for Browsers* takes less than 5 minutes to install. It starts protecting users immediately, with no down time. Cloud-based analysis minimizes system footprint.

The SandBlast Agent browser extension is an innovative solution that provides market-leading threat prevention methods while retaining a simple, intuitive user experience.

When would I select SandBlast Agent for Browsers instead of SandBlast Agent?

SandBlast Agent for Browsers serves as a great method to provide zero-day protection for web browsing. Whether the threats are based on web-downloads or phishing sites, *SandBlast Agent for Browsers* delivers strong real-time protection, including several completely unique methods and engines.

The complete *SandBlast Agent product* provides multiple protection vectors that the browser version doesn't possess, such as detecting malware copied from external storage, Anti-ransomware to detect and quarantine ransomware followed by recovering encrypted or deleted files. It also has built-in Anti-bot capabilities that can identify and block malicious communications if a threat were to reach an endpoint via unprotected channels. In addition, forensics capabilities of the complete *SandBlast Agent* package provide in-depth, automated analysis of the threats themselves.

SandBlast Agent for Browsers is also ideal for customers looking for an alternative to heavy endpoint software implementation. This solution uses a simple web-browser plugin form-factor in order to speed implementation and reduce management overhead, and minimizes the footprint on the user's system by conducting all the analysis in the cloud.

Can SandBlast Agent for Browsers work along with third-party AV software?

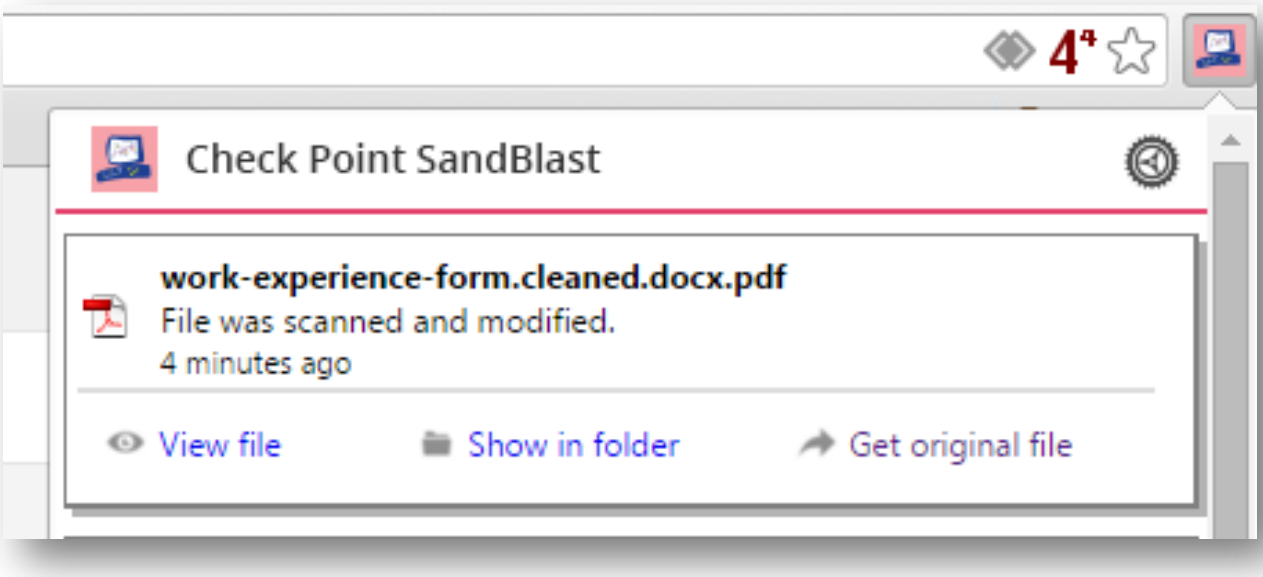
Yes. *SandBlast Agent for Browsers* is a browser-extension. It interacts only with SandBlast service or SandBlast appliance. Therefore it can co-exist with any endpoint security software.

Does Threat Emulation of web-download content add delays, resulting in inferior browser user-experience?

No. *SandBlast Agent for Browsers* features a threat extraction capability that quickly delivers a safe reconstructed copy of the file. At the same time, the original file is being inspected for potential threats by threat emulation. This eliminates any delay in browsing.

How does the user obtain the original version of a file, if the extracted version isn't sufficient?

When common document formats are downloaded from a website, or via a link in an email, an extracted file (safe reconstructed copy) is delivered in seconds. Then, once emulation is complete *SandBlast Agent for Browsers* provides three options – "*View file*", "*Show in folder*", and "*Get original file*".

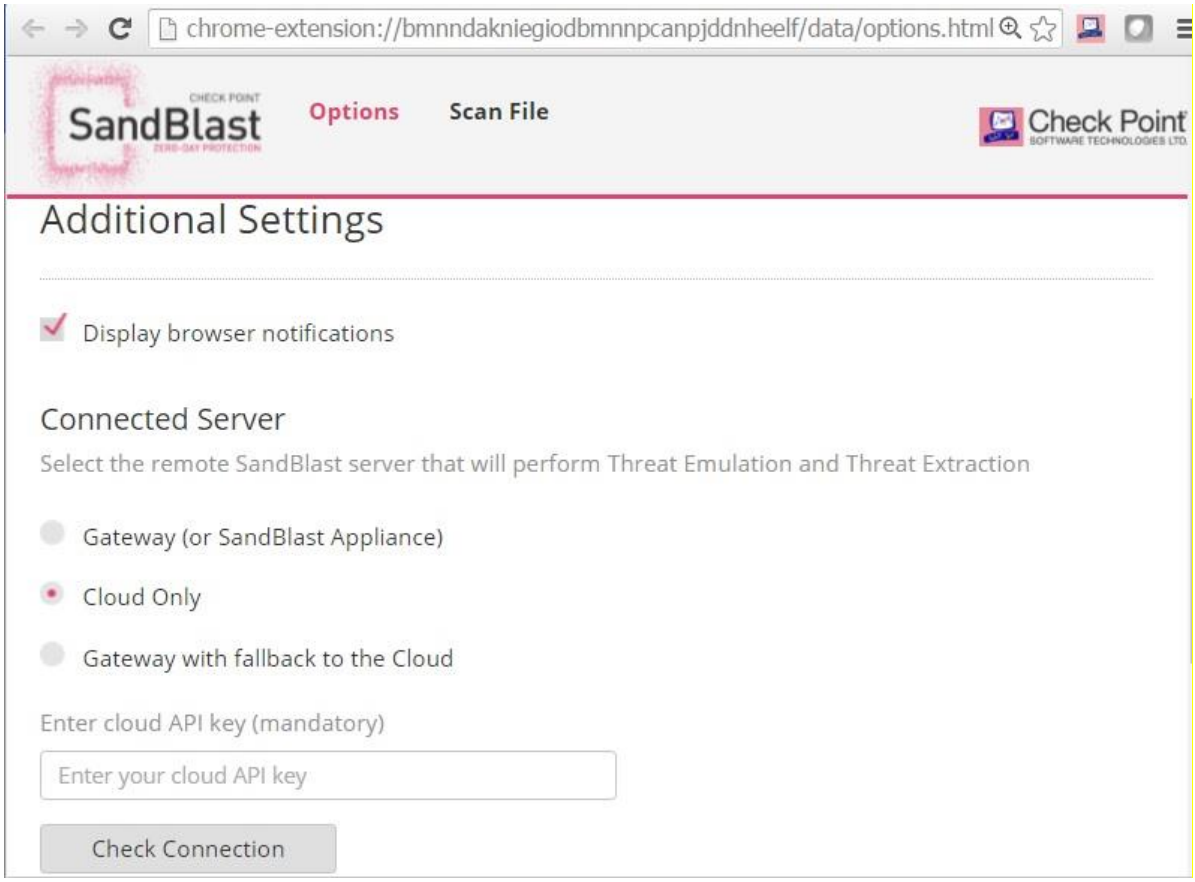


What browsers are supported by the extension?

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.

Is it possible to use an on-premise SandBlast Appliance with SandBlast Agent for Browsers?

Yes. Businesses have the option to use either cloud services or on-premise appliances.



Zero Phishing

How does Zero Phishing protect users from phishing attacks and credential theft?

Zero Phishing is a new innovation in the SandBlast family that protects corporate credentials and prevents users from accessing unknown phishing sites.

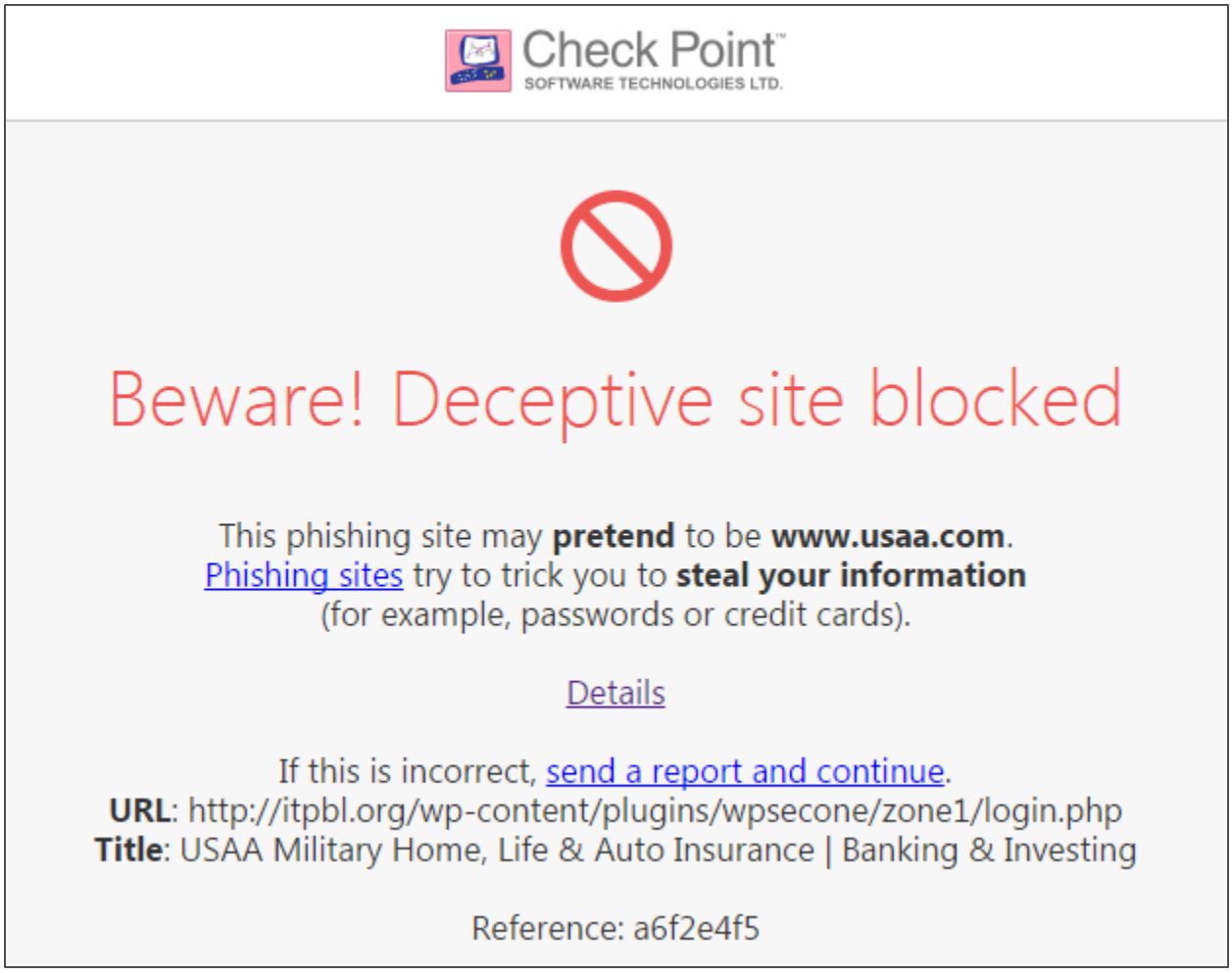
- **Protection from Unknown Phishing Sites:** Zero Phishing uses several heuristic and machine learning methods to detect phishing sites based on their characteristics and the way they behave, not simply based on reputation.
- **Prevention of Corporate Credential Reuse:** By defining “protected” domains, an Admin can prevent users from reusing the corporate credentials for those domains on external websites.

How is the confidentiality of personal data, such as corporate passwords, ensured?

Check Point does not store any personal data or corporate passwords in cloud. All data is encrypted and stored locally. Once the admin has defined the protected domain, the one-way hash of corporate credential is created on the first login. From that point onwards, when inputting passwords, they will be compared to that locally stored hash. Since this is a one-way algorithm, the actual passwords cannot be reconstructed from the hash.

What happens when a user attempts to access an unknown phishing website?

Zero Phishing initiates analysis as soon as a user tries to fill-in a web-form. Analysis is conducted based upon site attributes – URL, top-level domain, and IP analysis, etc. – as well as heuristic methods that compare the site to previously seen phishing techniques. The site is blocked based on the results of the analysis, and details are shared with the user as shown below.

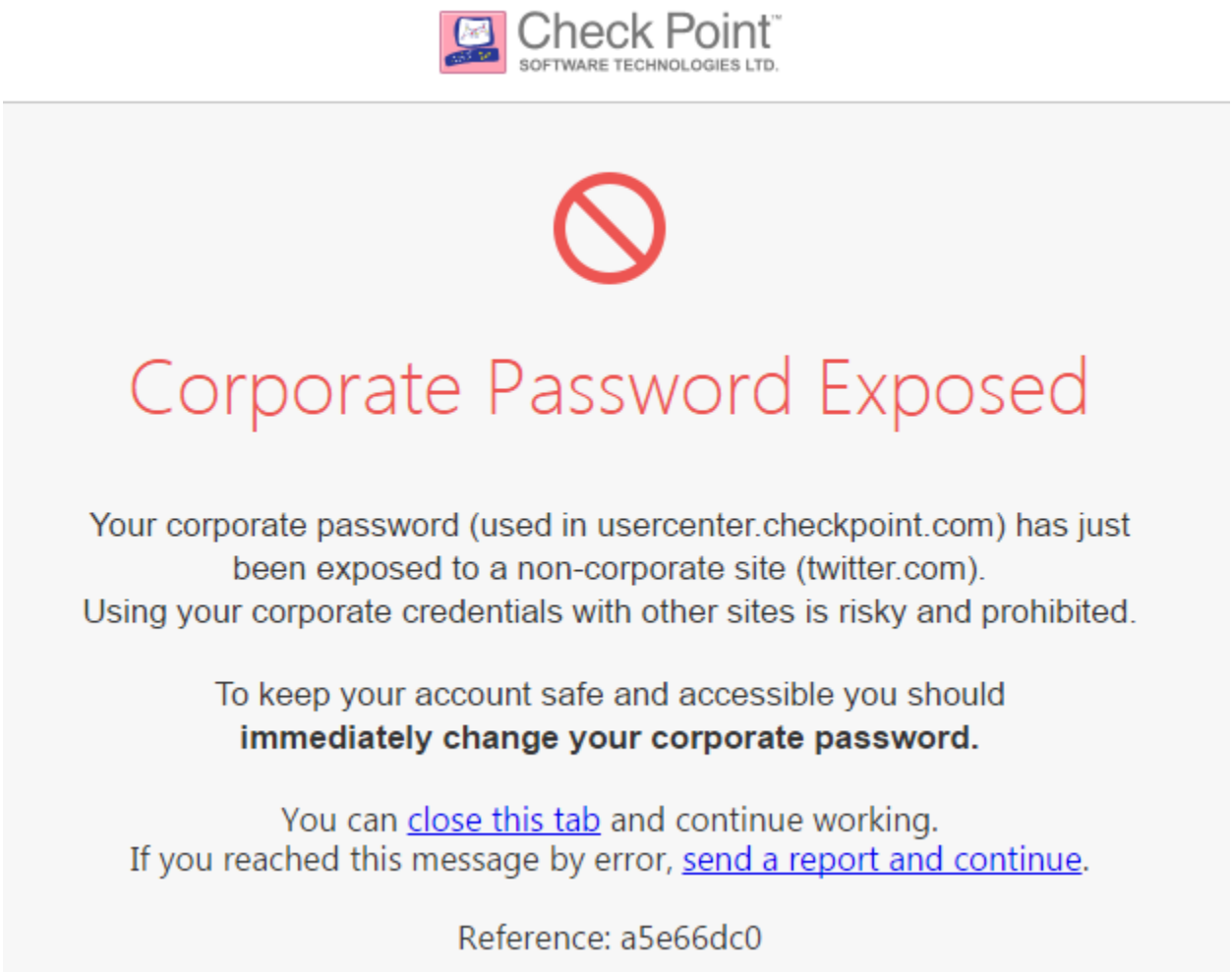


What can a user do if access to a legitimate site is blocked by Zero Phishing?

In this case, as shown above in the warning window, zero phishing provides an option to continue to the site by clicking the link "*send a report and continue*". But this action will be audited.

What is the user experience when a user tries to re-use corporate passwords on an external website?

Whenever the user tries to re-use their corporate credentials on a third-party website (i.e. one that has not been defined by the admin as a protected domain), they will receive a warning and more importantly, a log will be created, allowing the admin to pursue the required actions or provide the user with education on why this is not permitted.



Deployment

How is SandBlast Agent for Browsers deployed?

Check Point SandBlast Agent for Browsers is a browser extension, and depending on how it is being deployed the process varies:

1. Stand-alone - *SandBlast Agent for Browser* can be installed alone on the user's laptop or desktop. In such deployment, it directly communicates with SandBlast Service, and is centrally managed by a dedicated web-based portal. Deployment is managed through typical tools for installing / configuring applications, for example using GPO (Group Policy Object) in Microsoft environments.
2. Integrated with SandBlast Agent - As a component in SandBlast Agent, which includes zero-day protection for all types of file-downloads (including USB file transfer), Anti-Ransomware, Anti-Bot, and Forensics & automated incident analysis, the browser protection and Zero Phishing capabilities are installed as part of the client package.
3. Integrated with Full Endpoint Protection - When deployed along with additional Endpoint protection, SandBlast Agent for Browsers is installed and policies are set through Endpoint Management.

I already have NGTX and /or SandBlast Appliance, why do I also need SandBlast Agent for Browsers?

While the scenario above means that the user has the option to implement Threat Emulation for their web-downloads, it cannot operate in real-time without significant delays impacting the user, since the file must be evaluated before it is released. Access to the Threat Extraction and Zero Phishing capabilities are additional protections that require a presence at the endpoint, either through the full SandBlast Agent or the browser extension.

Packaging and Pricing

What is the SKU and pricing for Check Point SandBlast Agent for Browsers?

Check Point SandBlast Agent for Browsers is sold under an annual subscription model. It is being introduced at a rate of $15 per user account per year, with the SKU *CPEP-SBA-BROWSER-1Y* for a one year subscription. The Annual price includes standard support.

NOTE: The functionality of *SandBlast Agent for Browsers* is already included in *SandBlast Agent* and *Full Endpoint Agent*

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.

How are seats going to be counted?

Every User-id is equal to one seat.

What protection capabilities are featured in the different packages that include SandBlast Agent for Browsers?

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

Features	SandBlast Agent for Browsers (COMING SOON)	SandBlast Agent	Endpoint Complete Protection Suite
Deployment	Browser Extension	Endpoint Agent	Endpoint Agent
Management	Cloud	SmartCenter	SmartCenter
Browser extension included	✓	✓	✓
Emulation & Extraction for web downloads	✓	✓	✓
Credential Protection and Zero Phishing	✓	✓	✓
Anti-Ransomware		✓	✓
File System monitor with Threat Emulation		✓	✓
Infection detection with Anti-Bot		✓	✓
Automated forensics and infection quarantine		✓	✓
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.

For the latest information, always refer to the Check Point product catalog on Check Point PartnerMAP.

