Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point SandBlast Cloud

Zero-Day Protection for Office 365™ Email

CHECK POINT SANDBLAST CLOUD

Industry-leading zero-day protection for Microsoft Office 365™ cloud email environments

Product Benefits

- Complete protection from known and unknown threats for cloud-based email environments
- Best catch rate of unknown threats and zero-day malware
- Rapid reconstruction of files for immediate access to safe content
- Ensures email continuity to maintain full user and business productivity
- Consistent and intuitive user experience
- Easy to deploy and manage
- Seamless integration with existing infrastructure

Product Features

- Includes multiple layers of defenses: Antivirus, URL reputation, Threat Emulation, Threat Extraction
- Deep malware inspection at the CPU-level, where exploits cannot hide
- Inspects broad range of documents and common file-types
- Removes active content and other exploitable content from documents
- API-level integration ensures email continuity
- Full visibility and policy customization through cloud-based management portal
- Pure cloud solution – makes it easy to get up and running quickly

INSIGHTS

The increasing adoption of cloud email tools such as Microsoft Office 365™ enables businesses to efficiently communicate and collaborate, without investing resources in managing and maintaining their own dedicated IT infrastructure. However, the shift to cloud-based tools also brings with it an array of security risks, including susceptibility to sophisticated attacks such as ransomware and spear-phishing which use email as a primary entry point.

Traditional security solutions such as Antivirus that protect against known threats are an essential part of a comprehensive security plan, but are no longer enough on their own. With hackers constantly modifying their strategies and techniques to remain elusive and achieve their goals, it's become critical for organizations to stay one step ahead of unknown malware and zero-day attacks, regardless of their environment.

So how can organizations ensure a balance between leveraging the benefits of deploying cloud-based email, while maintaining robust protection against modern malware?

SOLUTION

Check Point SandBlast™ Cloud brings best-in-class proactive protection from known threats, unknown malware and zero-day attacks to Office 365 users. With multiple layers of defenses, transparently applied to all incoming content, SandBlast Cloud keeps malware from ever reaching users. Antivirus and URL Reputation protections within SandBlast Cloud leverage real-time intelligence from the ThreatCloud database to secure against the latest threats from known sources.

Advanced threat protection capabilities, including Threat Emulation and Threat Extraction elevate defenses against zero-day and unknown malware for cloud-based email users. Threat Emulation sandboxing performs deep CPU-level inspection, stopping even the most dangerous attacks before malware has an opportunity to deploy and evade detection. Threat Extraction complements Threat Emulation by ensuring quick delivery of safe content to your users through the elimination of exploitable content and reconstruction of files with only known safe elements.

All content analysis is completed in the cloud, providing a non-intrusive solution that maintains a consistent user experience.

Check Point SandBlast Cloud – a simple, seamless and complete advanced threat protection solution for Office 365 email environments.

May 17, 2016

INDUSTRY-LEADING SECURITY FOR CLOUD-BASED ENVIRONMENTS

SandBlast Cloud provides Check Point's industry-leading security protection to organizations using Microsoft Office 365 cloud-based email. This comprehensive solution blocks known threats using tools like Antivirus and URL Reputation to secure users from the latest malicious files and infested websites. Using Threat Emulation and Threat Extraction, SandBlast Cloud brings the highest catch rate and proactive protection from unknown attacks to cloud-based email.

IDENTIFY AND PREVENT MORE MALWARE

The Threat Emulation sandboxing engine within SandBlast Cloud intercepts and filters inbound files, including any files originating from URLs within emails by running them in a virtual environment. File behavior is inspected simultaneously across multiple operating systems and versions. Files engaging in suspicious activity commonly associated with malware, such as modifying the registry, network connections, and new file creation are flagged and further analyzed. Malicious files are prevented from reaching users.

EVASION RESISTANT DETECTION

Unlike other solutions, the sandboxing technology used within Check Point SandBlast Cloud uses a unique technology that does inspection at the CPU-level to stop attacks before they have a chance to launch.

There are thousands of vulnerabilities and millions of malware implementations, but there are very few methods that cyber criminals utilize to exploit vulnerabilities. The Threat Emulation engine monitors CPU-based instruction flow for exploits attempting to bypass operating system and hardware security controls.

By detecting exploit attempts during the pre-infection stage, the Threat Emulation engine stops attacks before they have a chance to evade detection by the sandbox.

DETAILED REPORTS

A detailed report is generated for each file emulated and found to be malicious. The easy to understand report includes file details and information about any abnormal activity or malicious attempts originated by running the file. The report provides actual screenshots of the environment while running the file for any operating system on which it was simulated.

THREATCLOUD™ ECOSYSTEM

Newly discovered threats are sent to the ThreatCloud intelligence database. Each newly discovered threat signature is distributed across the ThreatCloud ecosystem to protect other Check Point connected gateways. This enables connected gateways to block the new threat before it has a chance to become widespread. Constant collaboration makes ThreatCloud the most advanced and up-to-date threat Intelligence ecosystem available.

PROMPT DELIVERY OF SAFE CONTENT TO END-USERS

When it comes to threat protection for cloud-based environments, it doesn't have to be a trade-off between speed, coverage and accuracy. Unlike other solutions, Check Point SandBlast Cloud can be deployed in detect and prevent mode, while still delivering emails to end-users promptly.

The Threat Extraction component within SandBlast Cloud immediately eliminates any potential threats transported through files by removing risky content such as macros or embedded scripts and then reconstructs the document using only known safe elements.

Unlike detection technologies that require time to analyze and identify threats before blocking them, Threat Extraction preemptively eliminates risk, ensuring prompt delivery of safe documents to end-users.

TRANSPARENT USER EXPERIENCE

All content is analyzed in the cloud before it is delivered to the user's inbox, ensuring that end-users have a consistent experience without the need for any additional actions or complexity.

In formats that have undergone Threat Extraction, a link provides the user with self-service ability to download the original after emulation is complete.

PROTECTS MOST COMMON FILE TYPES

SandBlast Cloud protects a wide range of the most common document types used in organizations today, from Microsoft Office Word, Excel, Power Point, and Adobe PDFs to Archive files.

May 17, 2016

EASY TO DEPLOY AND MANAGE

As organizations adopt Office 365 cloud-based email, they require a solution that seamlessly integrates with their existing infrastructure. Check Point SandBlast Cloud has an API-level integration with Microsoft Office 365, enabling it to be implemented as a complete cloud solution that won't interfere with your email delivery, or require any on-premise hardware.

The cloud-based management portal within the SandBlast Cloud solution provides full visibility into security events at the endpoint, network and for cloud-email. Security Administrators can also customize policy configurations and monitoring - all using our simple cloud-based management portal.

SANDBLAST CLOUD FOR OFFICE 365™ SPECIFICATIONS

ZERO DAY PROTECTION for MICROSOFT OFFICE 365 MAIL		
	Feature	**Description**
Attachments	**Threat Emulation with CPU-Level Detection**	Dynamic file analysis discovers malicious behavior and prevents infection from new malware and targeted attacks
	Threat Extraction **Coming soon*	Reconstructs incoming files, eliminating potential threats and promptly delivering a safe version to users
	Antivirus	Signature-based malware detection powered by the Check Point ThreatCloud™.
Content	**URL Emulation**	Files directly originating from URLs (….com/test.doc) will be scanned by Threat Emulation
	URL Reputation	Signature-based URL analysis powered by the Check Point ThreatCloud™
THREAT EMULATION		
Supported File Types		Over 40 file types, including: Adobe PDF, Microsoft Office, EXE, files in archives, Flash, Java Applets, and PIF
Supported Emulation Environments		Microsoft Windows XP, 7, 8, 10; Microsoft Office; Adobe Reader
THREAT EXTRACTION		
Supported File Types		Microsoft Office 2003-2013, Adobe PDF
GENERAL		
100% Cloud-based solution, powered by a native Microsoft API		
Dedicated web portal for setup, management and visibility		
Advanced monitoring capabilities provide valuable insight into security events		
Optional integration with on-premises Check Point Management		

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

May 17, 2016