Check Point SandBlast™ Cloud FAQ

What is Check Point SandBlast Cloud?

Check Point SandBlast Cloud is a Security-as-a-Service (SaaS) solution that protects Microsoft Office 365™ cloud-based email environments using Check Point SandBlast Zero-Day Protection capabilities.

The security elements included in *Check Point SandBlast Cloud* are:

1. **Antivirus**
   Proactively leverages antivirus signatures to secure against known malware in attached files.
2. **URL Reputation**
   Detects and blocks malicious URLs within email body.
3. **Threat Emulation**
   Inbound file attachments, including any files originating from URLs within emails, are sent to the sandbox for emulation to detect and block unknown malware and zero-day threats.
4. **Threat Extraction**
   Proactively prevents malicious content within attached files from reaching users by quickly delivering safe reconstructed copies of documents, while original files are being inspected for potential threats.

My cloud-based email solution already provides basic security against known threats. Do I still need SandBlast Cloud?

Yes. SandBlast Cloud enables you to bring the same strong security from your enterprise network to prevent advanced malware as you move email services outside your perimeter. SandBlast Cloud provides advanced protection from unknown threats that can bypass traditional AV solutions.

Do I need any Check Point Appliances, Endpoint Security Agent, SandBlast Appliance or SandBlast Agent in order to use Check Point SandBlast Cloud?

Check Point SandBlast Cloud is a pure SaaS solution. Like any other cloud solution, you can buy and deploy it within minutes. No additional Check Point hardware or software is required.

Where are files emulated, and how long does it take?

Files are emulated in **SandBlast Cloud** in one of the three global sites – USA, Europa and Israel. Full emulation typically takes 60-90 seconds in the cloud. Total time varies depending on file size, network traffic and the number of files in queue.

What information is shared with ThreatCloud?

An anonymous sharing mode will share the following information with ThreatCloud: file MD5, file SHA1 and a report that includes the operations performed by this file (launch processes, create files, change the registry or open network connections).

What is the user experience when a malware is detected?

The user will receive an edited version of the original email, without the malicious attachments and/or the malicious URL. We plan to provide alerts that will be added both to the subject and the body of the email. This will be both customizable and localized.

Which other cloud business apps are supported?

Check Point has prioritized Office 365 cloud email, as it is the most widely used cloud enterprise application. Please contact product management for information regarding future roadmap deliverables.

Is Anti-Spam supported by SandBlast Cloud?

SandBlast Cloud uses Microsoft Application Program Interface **(MS API**), a non-intrusive method for integration with Office 365 cloud-based email; therefore users can continue to use the anti-spam capabilities in Microsoft Office 365.

How do you employ MS API for threat prevention using SandBlast Cloud?

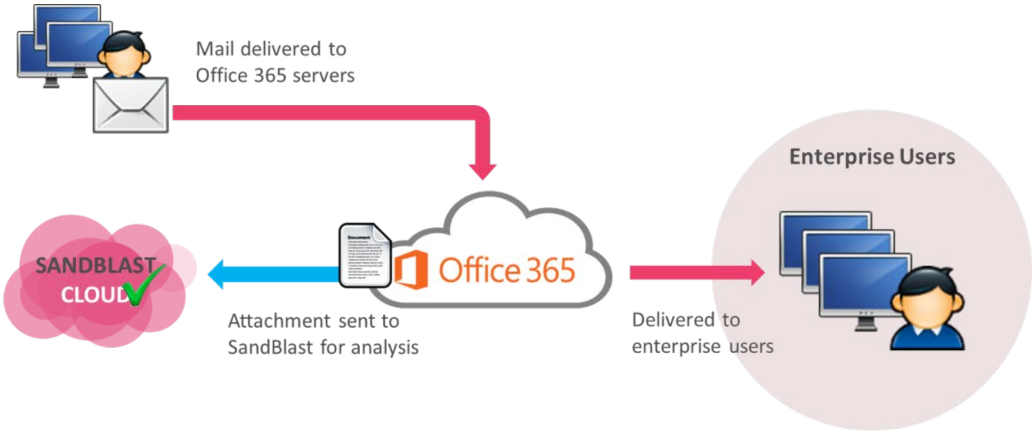
For Office 365 cloud-based email, we use the **MS API** to create a **quarantine folder** within Office 365. This folder is not accessible by user, and is used to hold emails until the extracted version and/or a verdict is delivered from SandBlast Cloud.

Deployment

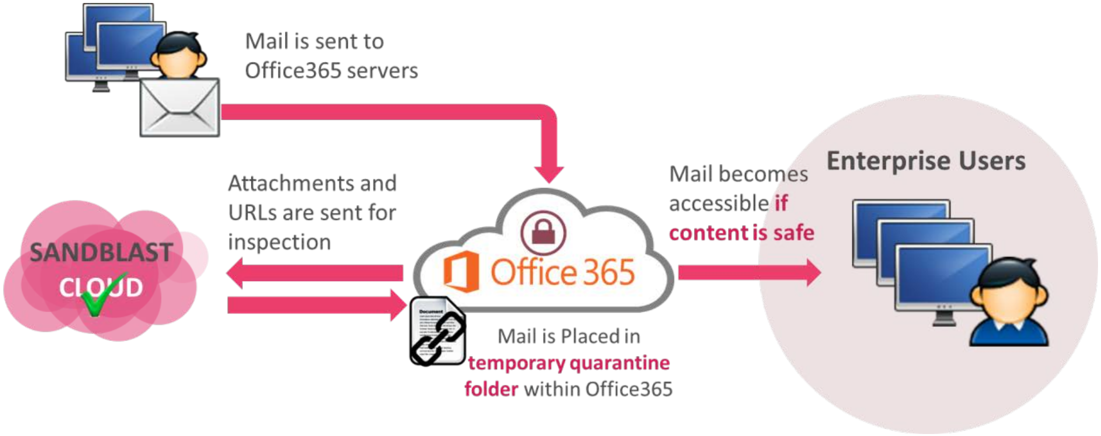
What are the deployment options for Check Point SandBlast Cloud?

Check Point SandBlast Cloud offers both detect and prevent modes. Both are based on a native Microsoft API enabling Check Point to analyze and isolate incoming malicious emails from within the user's inbox.

- **Detect Mode**: Incoming emails are analyzed by Check Point SandBlast but all emails go through to the inbox.

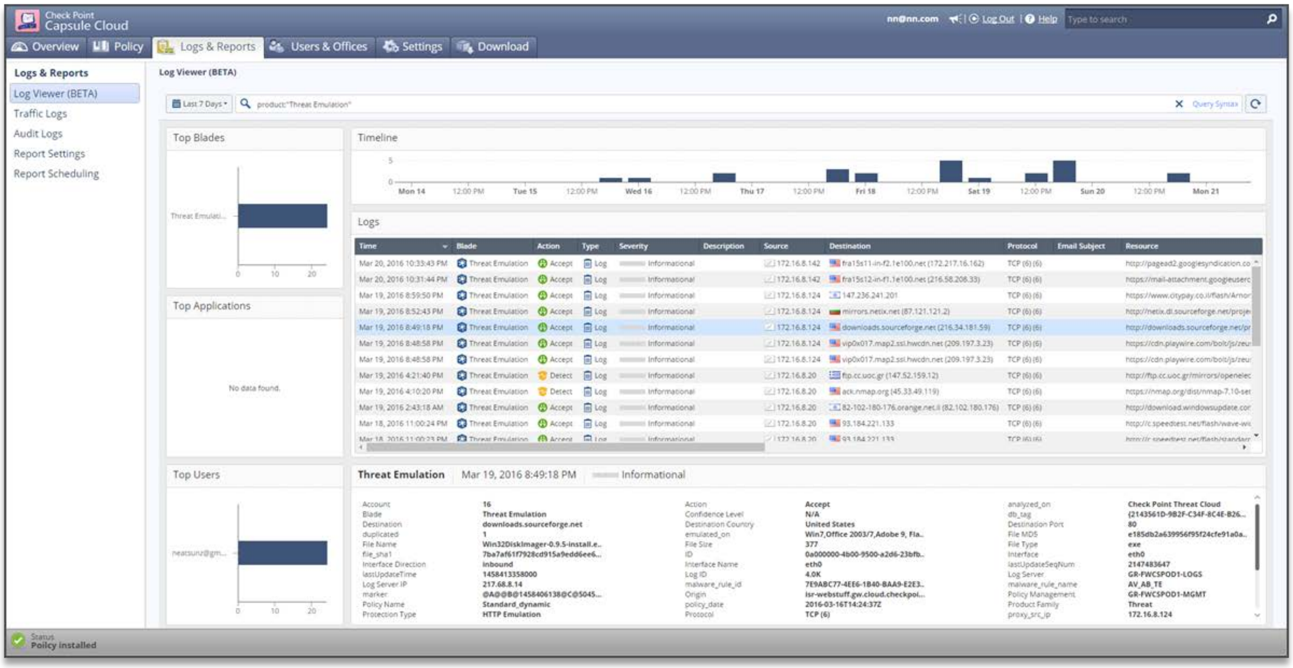


- **Prevent Mode**: Incoming emails are first directed to a preliminary quarantine folder – thus analyzing and isolating incoming malicious emails from within the actual inbox.



How is SandBlast Cloud managed?

A simple web-based management portal controls all configuration and logs. Reports are accessible via an intuitive web-based dashboard.



Time	Blade	Action	Type	Severity	Description	Source	Destination	Protocol	Email Subject	Resource
Mar 20, 2016 10:33:43 PM	Threat Emulation	Accept	Log	Informational		172.16.8.142	fra15s11-in-f2.1e100.net (172.217.16.162)	TCP (6) (6)		http://pagead2.googlesyndication.co
Mar 20, 2016 10:31:44 PM	Threat Emulation	Accept	Log	Informational		172.16.8.142	fra15s12-in-f1.1e100.net (216.58.208.33)	TCP (6) (6)		https://mail-attachment.googleuserc
Mar 19, 2016 8:59:50 PM	Threat Emulation	Accept	Log	Informational		172.16.8.124	147.236.241.201	TCP (6) (6)		https://www.citypay.co.il/flash/Amor
Mar 19, 2016 8:52:43 PM	Threat Emulation	Accept	Log	Informational		172.16.8.124	mirrors.netix.net (87.121.121.2)	TCP (6) (6)		http://netix.dl.sourceforge.net/proje
Mar 19, 2016 8:49:18 PM	Threat Emulation	Accept	Log	Informational		172.16.8.124	downloads.sourceforge.net (216.34.181.59)	TCP (6) (6)		http://downloads.sourceforge.net/pr
Mar 19, 2016 8:48:58 PM	Threat Emulation	Accept	Log	Informational		172.16.8.124	vip0x017.map2.ssl.hwcdn.net (209.197.3.23)	TCP (6) (6)		https://cdn.playwire.com/bolt/js/zeu
Mar 19, 2016 8:48:58 PM	Threat Emulation	Accept	Log	Informational		172.16.8.124	vip0x017.map2.ssl.hwcdn.net (209.197.3.23)	TCP (6) (6)		https://cdn.playwire.com/bolt/js/zeu
Mar 19, 2016 4:21:40 PM	Threat Emulation	Detect	Log	Informational		172.16.8.20	ftp.cc.uoc.gr (147.52.159.12)	TCP (6) (6)		http://ftp.cc.uoc.gr/mirrors/openelec
Mar 19, 2016 4:10:20 PM	Threat Emulation	Detect	Log	Informational		172.16.8.20	ack.nmap.org (45.33.49.119)	TCP (6) (6)		https://nmap.org/dist/nmap-7.10-set
Mar 19, 2016 2:43:18 AM	Threat Emulation	Accept	Log	Informational		172.16.8.20	82-102-180-176.orange.net.il (82.102.180.176)	TCP (6) (6)		http://download.windowsupdate.cor
Mar 18, 2016 11:00:24 PM	Threat Emulation	Accept	Log	Informational		172.16.8.20	93.184.221.133	TCP (6) (6)		http://c.speedtest.net/flash/wave-wi
Mar 18, 2016 11:00:23 PM	Threat Emulation	Accept	Log	Informational		172.16.8.20	93.184.221.133	TCP (6) (6)		http://c.speedtest.net/flash/standar

Threat Emulation | Mar 19, 2016 8:49:18 PM | Informational

Account	16	Action	Accept	analyzed_on	Check Point Threat Cloud		
Blade	Threat Emulation	Confidence Level	N/A	db_tag	{2143561D-9B2F-C34F-8C4E-B26...		
Destination	downloads.sourceforge.net	Destination Country	United States	Destination Port	80		
duplicated	1	emulated_on	Win7,Office 2003/7,Adobe 9, Fla...	File MD5	e185db2a639956f95f24cfe91a0a...		
File Name	Win32DiskImager-0.9.5-install.e...	File Size	377	File Type	exe		
file_sha1	7ba7af61f7928cd915a9edd6ee6...	ID	0a000000-4b00-9500-a2d6-23bfb...	Interface	eth0		
Interface Direction	inbound	Interface Name	eth0	lastUpdateSeqNum	2147483647		
lastUpdateTime	1458413358000	Log ID	4.0K	Log Server	GR-FWCSPOD1-LOGS		
Log Server IP	217.68.8.14	malware_rule_id	7E9ABC77-4EE6-1B40-BAA9-E2E3...	malware_rule_name	AV_AB_TE		
marker	@A@@B@1458406138@C@5045...	Origin	isr-webstuff.gw.cloud.checkpoi...	Policy Management	GR-FWCSPOD1-MGMT		
Policy Name	Standard_dynamic	policy_date	2016-03-16T14:24:37Z	Product Family	Threat		
Protection Type	HTTP Emulation	Protocol	TCP (6)	proxy_src_ip	172.16.8.124		

Future releases will support integration with on-premise Check Point management servers.

What is the process of adding an additional email address to the service?

New mailboxes will be added automatically every hour.

Packaging and Pricing

What is the SKU and pricing for Check Point SandBlast Cloud?

Check Point SandBlast Cloud is a pure Security as a Service, sold under an annual subscription model. It is being introduced at a rate of $15 per user account (i.e per mailbox) per year, with the SKU *CP-CLOUD-CMP-O365-1Y* 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 Partner MAP.