

SandBlast Cloud Securing Office 365 Demo

AMA

Goal of the demo

The Goal of the demo is to show the integration between Microsoft office 365 email system and the Check Point SandBlast advanced threat prevention system.

In this demo we will use 3 systems: Check Point cloud management, office 365 account, External Webmail.

We will send an email with malicious attachment from the external Webmail to the office 365 account and monitor the connection and review the security forensics report via the cloud management system.

Credentials

Office 365 – <https://outlook.office.com>

Username – user1@ama-demo.com

Password – Cpwins1!

External email - US – <https://friends.walla.co.il/#/login>

Username - AMA365demo@walla.com

Password – Cpwins1!

Cloud management

Use your own credentials

If you do not have credentials please contact sagy@checkpoint.com

Preparation

Open office 365 outlook web client <https://outlook.office.com>



Work or school account

user1@americas-demo.com

.....

Keep me signed in

Sign in

[Can't access your account?](#)

Type in the user and password

Username – user1@ama-demo.com

Password – Cpwins1!

This is the screen you will get

Office 365 | Outlook

Search Mail and People + New |

Folders

Inbox

Sent Items
Drafts
More

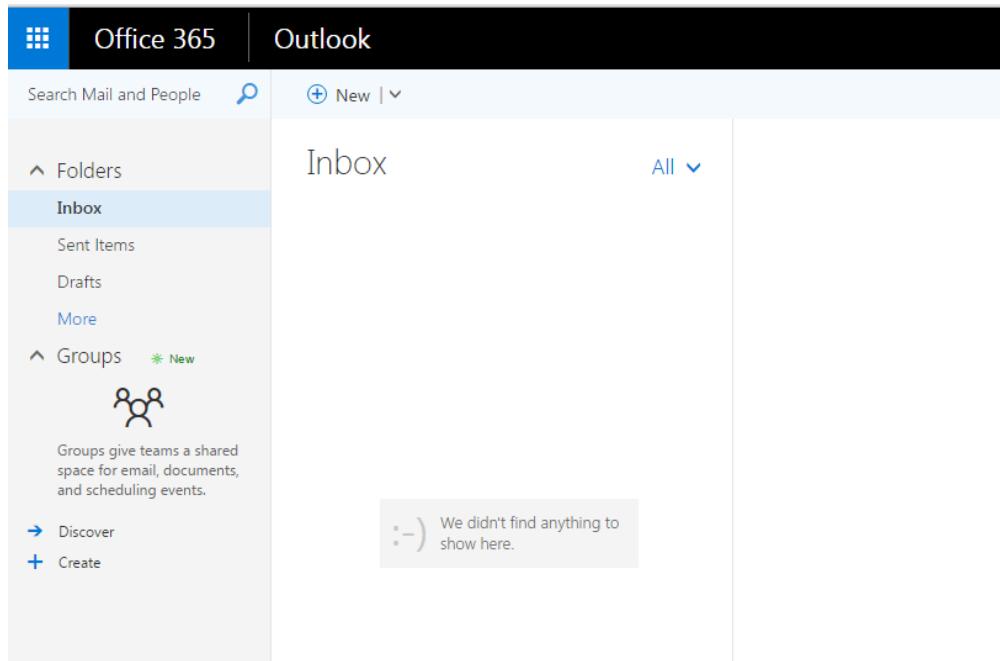
Groups * New

 Groups give teams a shared space for email, documents, and scheduling events.

→ Discover + Create

Inbox All +

We didn't find anything to show here.

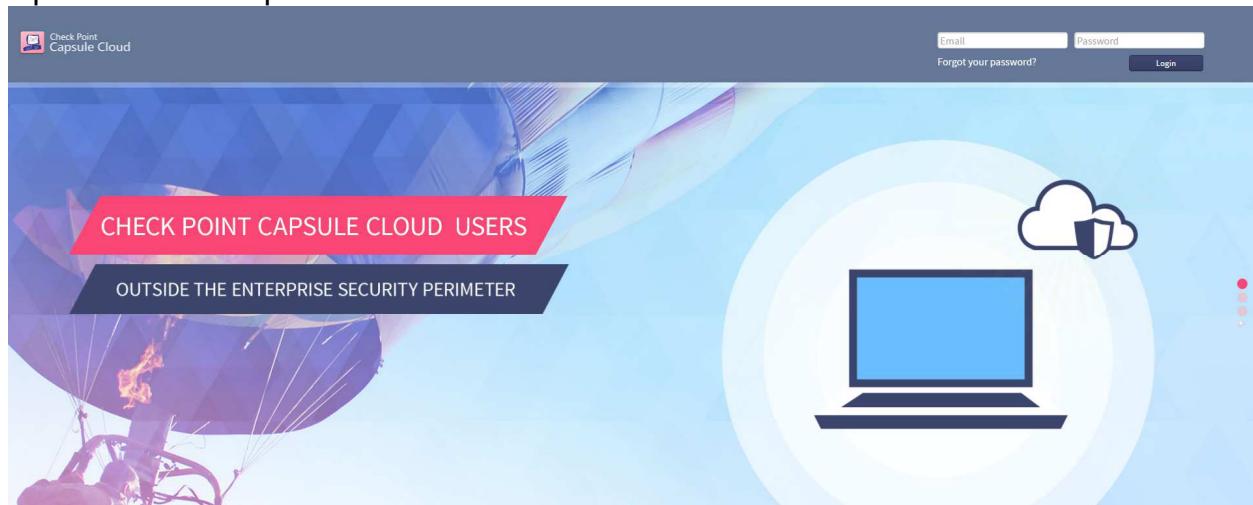


Open cloud.checkpoint.com

Check Point Capsule Cloud

Email Password
[Forgot your password?](#)

CHECK POINT CAPSULE CLOUD USERS
OUTSIDE THE ENTERPRISE SECURITY PERIMETER



Enter your credentials based on the invitation you have received.
If you have not received an invitation please contact sagy@checkpoint.com and ask for credentials (please allow up to 24 hours)

Login to an external email web client
<https://friends.walla.co.il/#/login>

כניסה לחשבון

Username	<input type="text"/>
Password	<input type="password"/>
<input checked="" type="checkbox"/> הישאר מחובר	
Login	
שכחתי את הסיסמה	

Username - ama365demo@walla.com

Password - Cpwins1!

Click on Login

Compose

Inbox

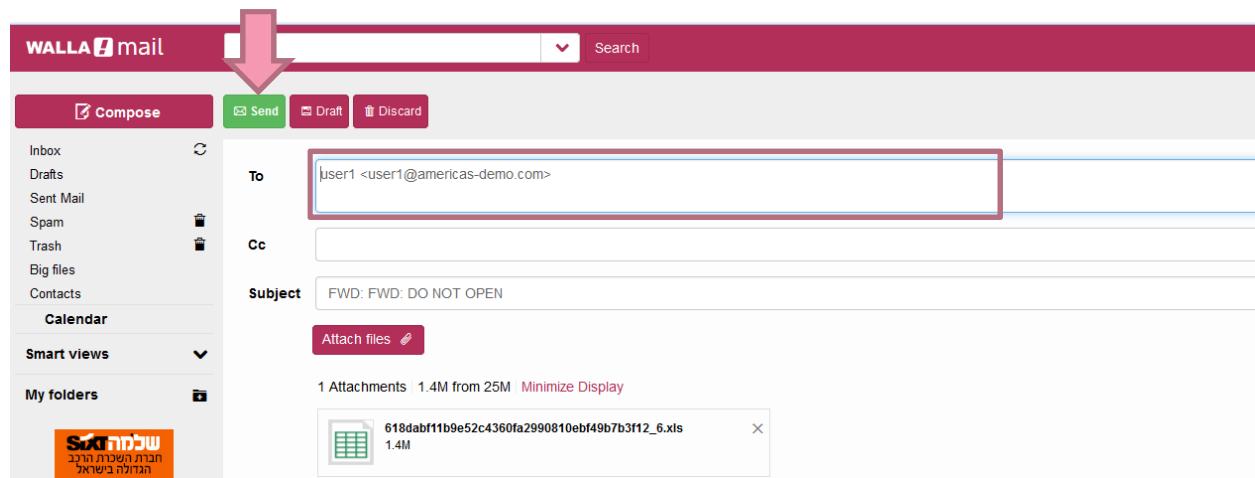
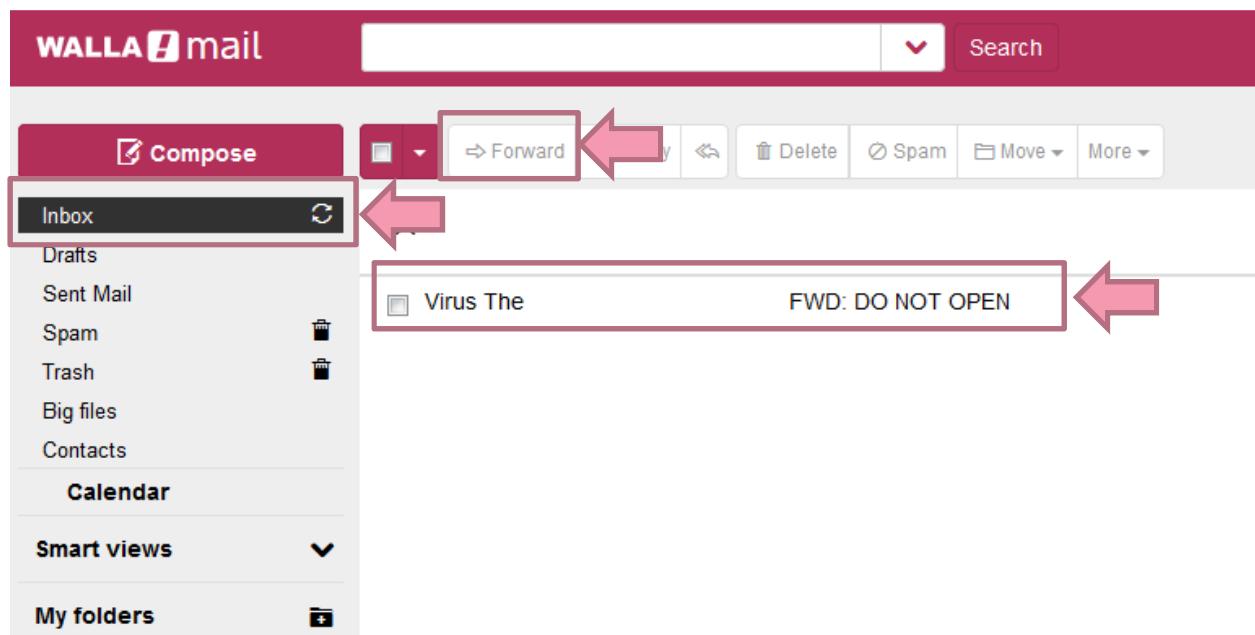
- Drafts
- Sent M
- Spam
- Trash
- Big files
- Contacts

Calendar

Smart views

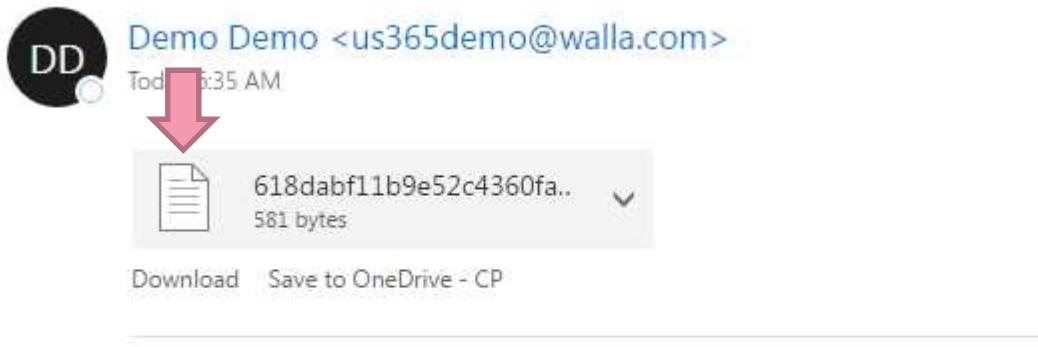
My folders

After login go to “**Inbox**” and forward the malicious email with subject “**Do Not Open**” send it to the office365 email address user1@ama-demo.com And click “SEND”



After clicking "SEND" go to the office 365 console and look for the email.
If you are in prevent mode the email will appear with a text file attachment stating that the malicious XLS file was removed

FWD: DO NOT OPEN



Demo Demo <us365demo@walla.com>
Today 5:35 AM

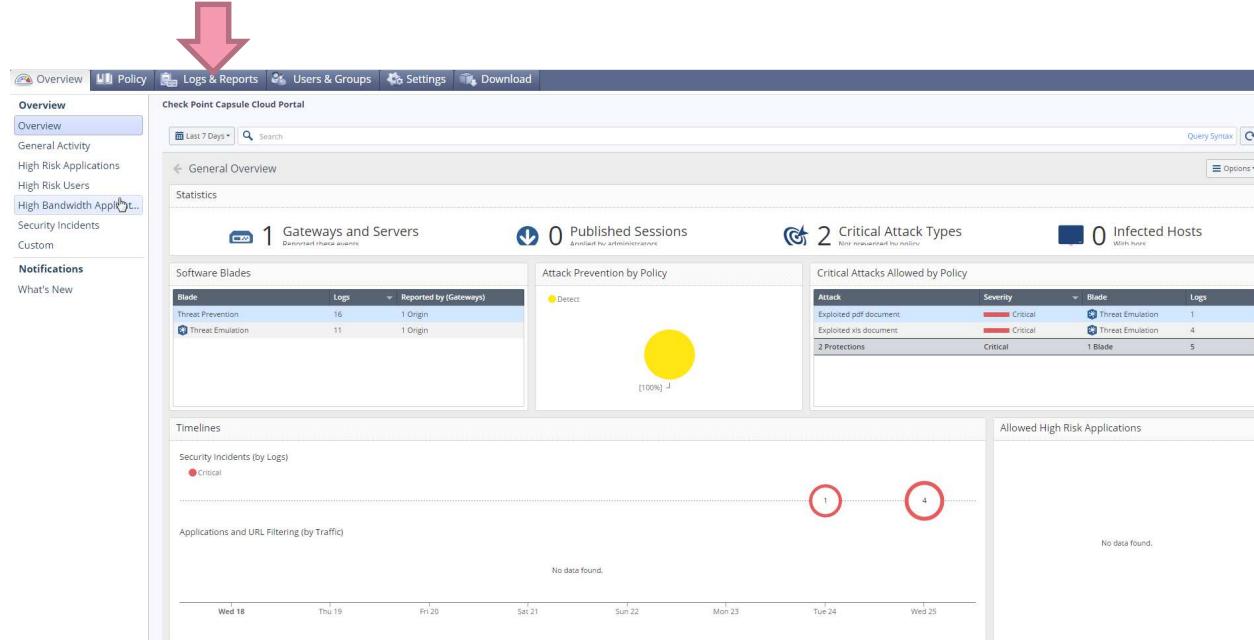
618dabf11b9e52c4360fa.. 581 bytes

Download Save to OneDrive - CP

----- Forwarded message -----
From: Virus The <happyvirus1@walla.com>
To: <user1@americas-demo.com>
Cc: US365demo <US365demo@walla.com>
Date: May 25, 2016 13:18
Subject: FWD: DO NOT OPEN

If you are working in detect mode the email with malicious attachment will arrive as is.

Open the cloud management system to look at the logs and activities



Check Point Capsule Cloud Portal

General Overview

Statistics

1 Gateways and Servers

Blade	Logs	Reported by (Gateways)
Threat Prevention	16	1 Origin
Threat Emulation	11	1 Origin

0 Published Sessions

2 Critical Attack Types

Attack	Severity	Blade	Logs
Exploded pdf document	Critical	Threat Emulation	1
Exploded vbs document	Critical	Threat Emulation	4
2 Protections	Critical	1 Blade	5

0 Infected Hosts

Timelines

Security Incidents (by Logs)

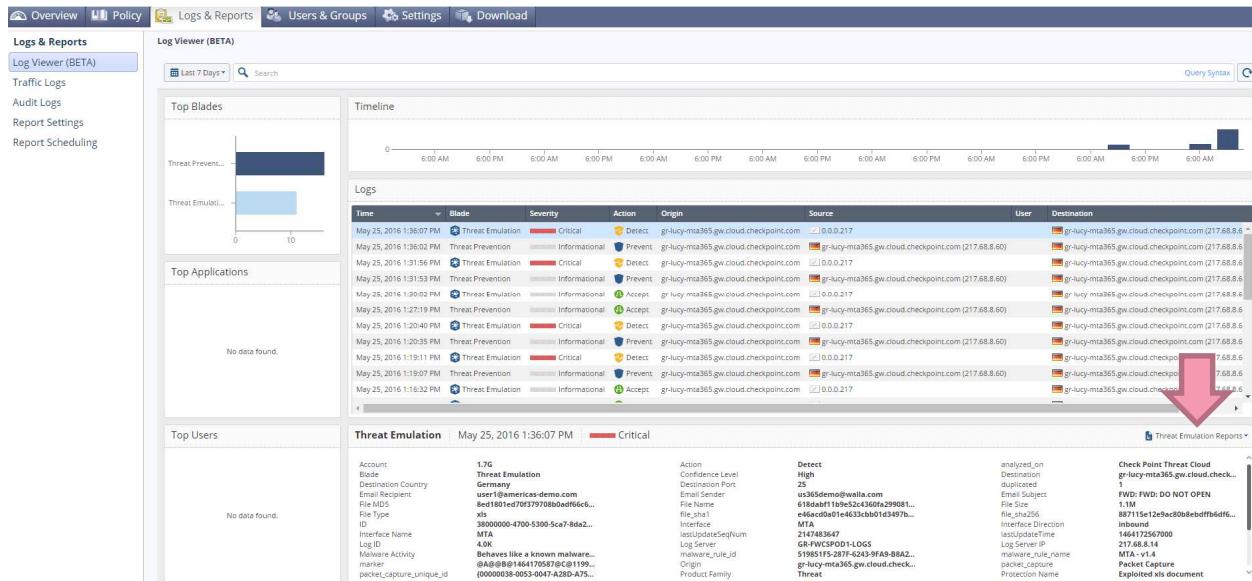
No data found.

Applications and URL Filtering (by Traffic)

No data found.

Wed 18 Thu 19 Fri 20 Sat 21 Sun 22 Mon 23 Tue 24 Wed 25

In order to follow the logs please click on logs and reports



Under logs and reports you will be able to see the prevent or detect logs according to the policy.

In order to see the SandBlast report please click on threat emulation reports and chose the relevant operating system.

After showing and explaining the report conclude the demo stating that the implementation of this technology is seamless and is a two-step configuration, there is nothing that the customer/admin needs to do in terms of his MX record or infrastructure.