

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

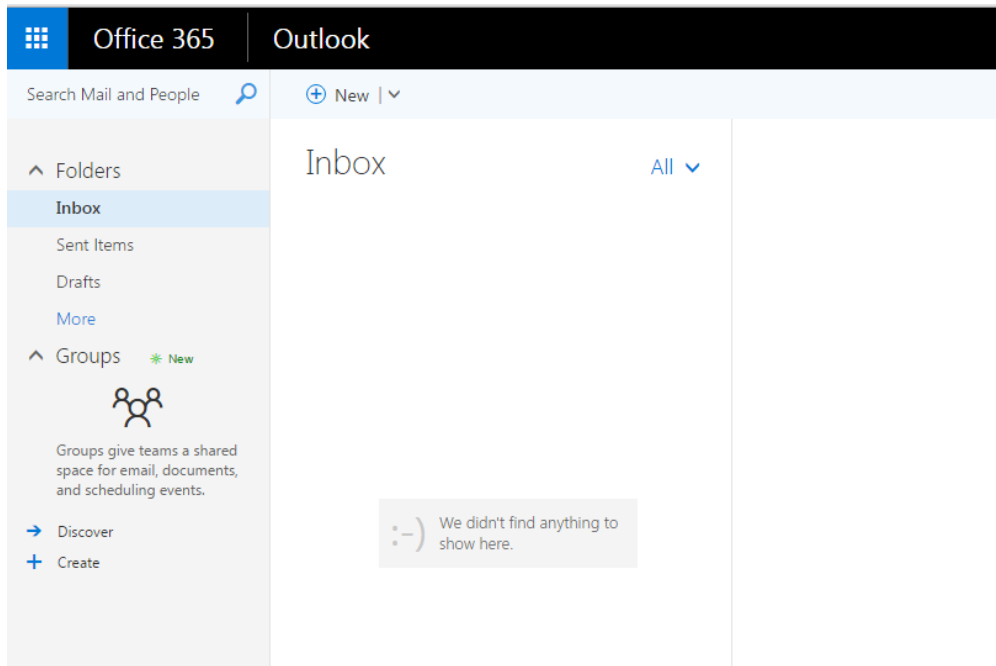
[Can't access your account?](#)

Type in the user and password

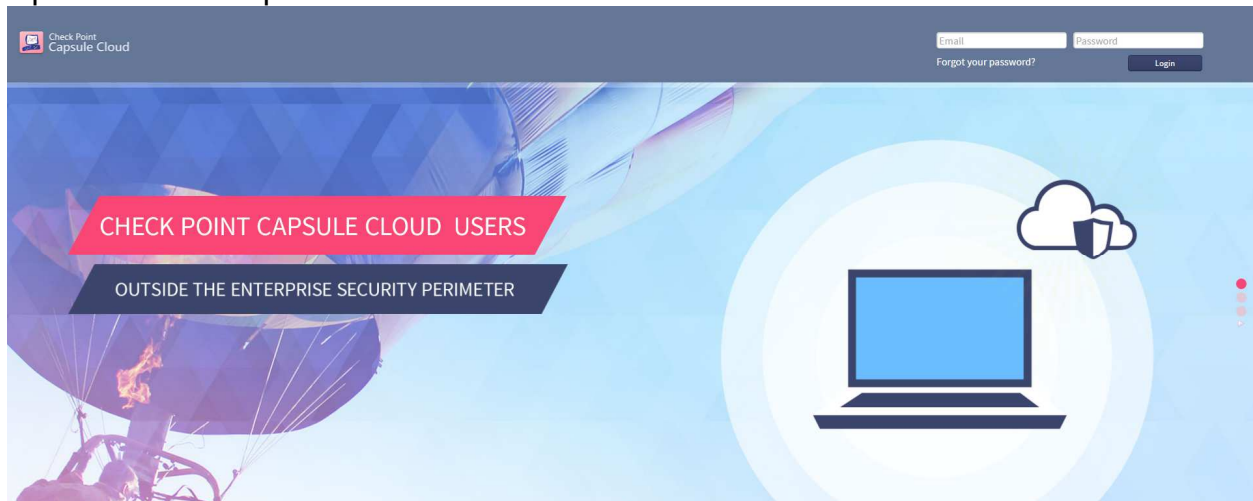
Username – user1@ama-demo.com

Password – Cpwins1!

This is the screen you will get



Open cloud.checkpoint.com




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 

Password 

הישאר מחובר ☒

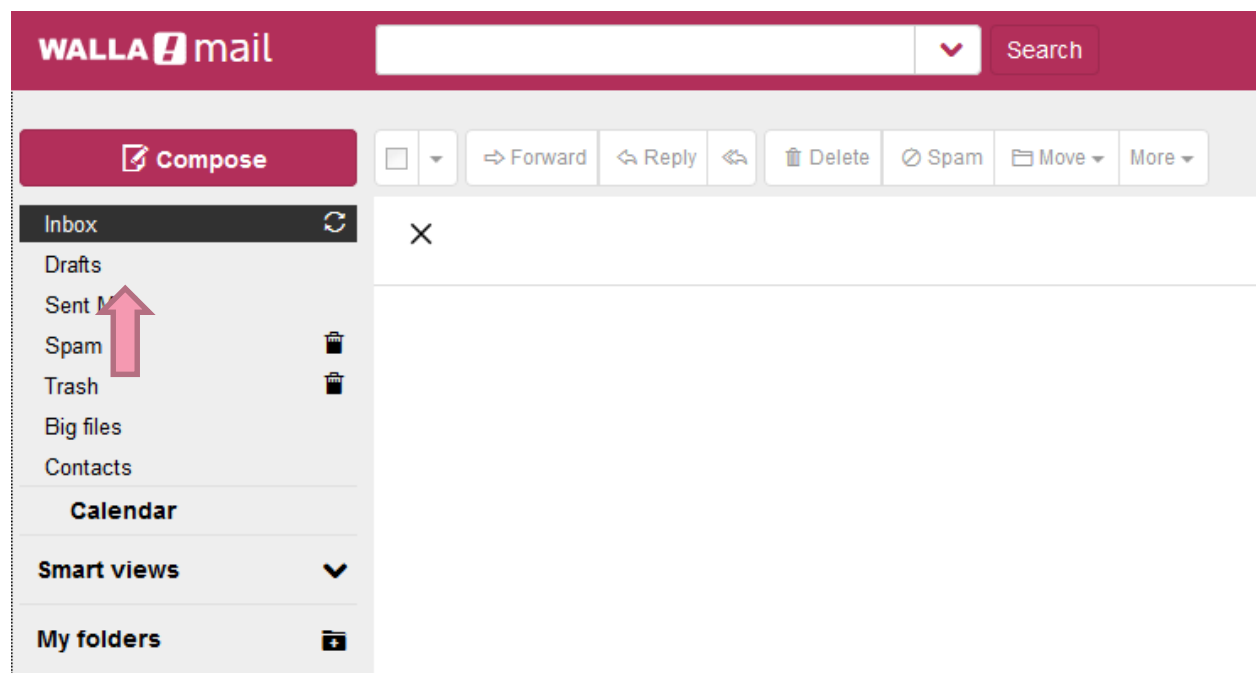
Login

[שכחתי את הסיסמה](#)

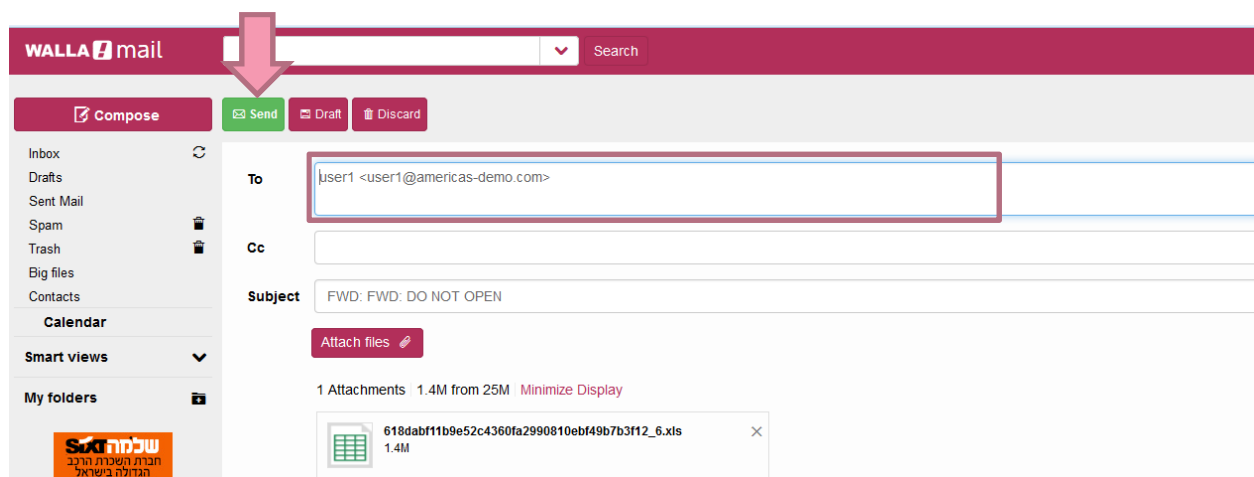
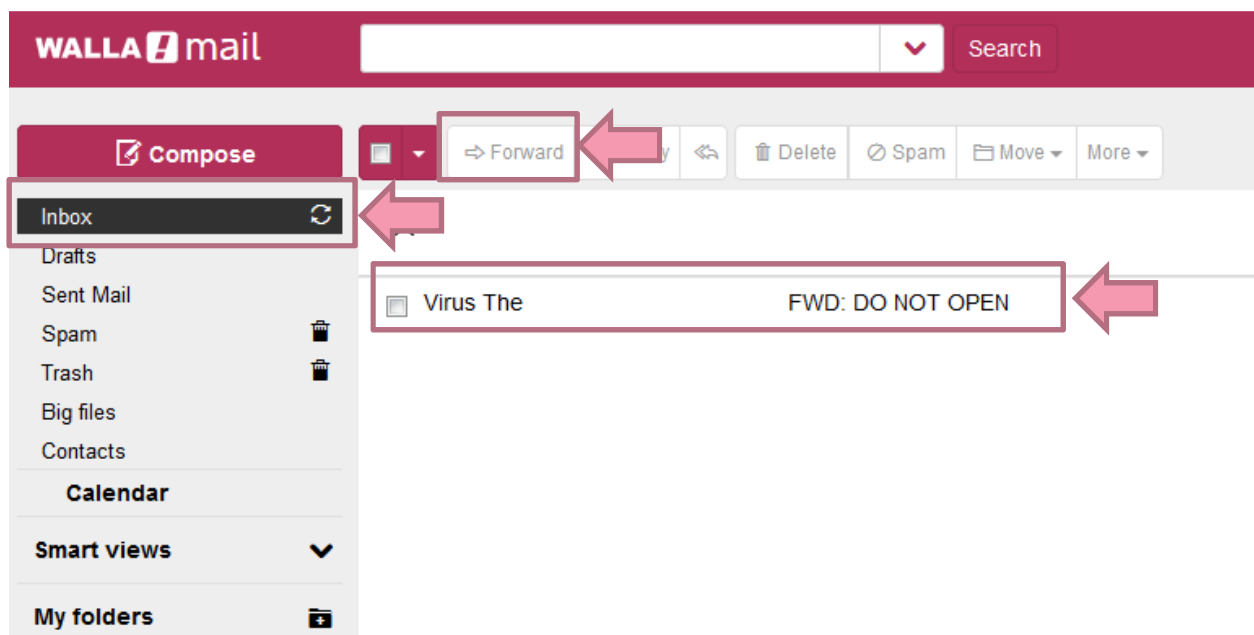
Username - ama365demo@walla.com

Password - Cpwins1!

Click on Login

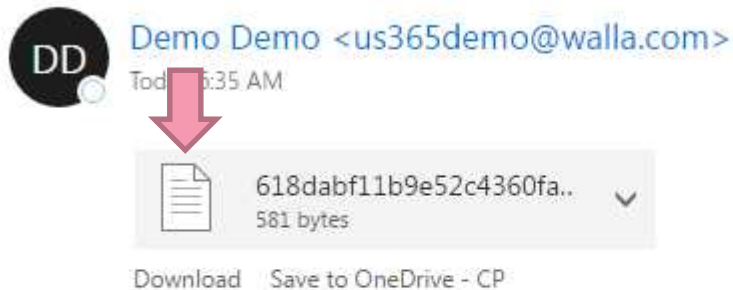


After login go to “Inbox” and forward the malicious email with subject “Do Not Open” send it to the office365 email address user1@ama-demo.com And click “SEND”



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

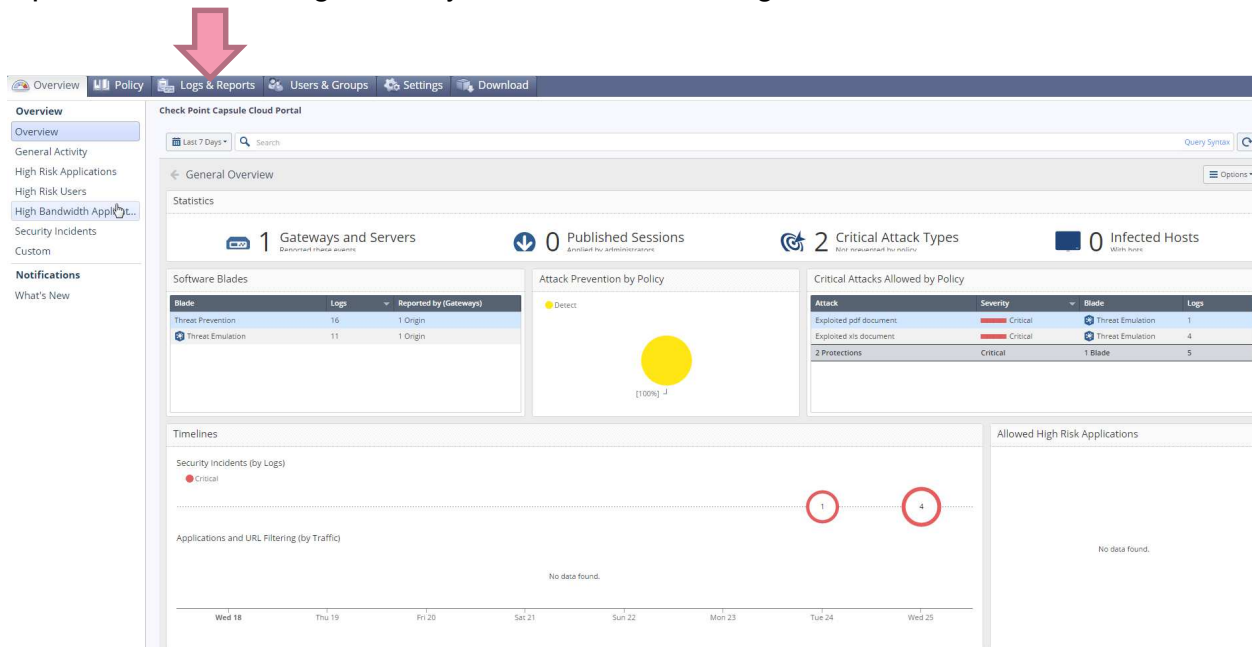
FWD: DO NOT OPEN



----- 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



The screenshot displays the Log Viewer (BETA) interface with several panels:

- Log Viewer (BETA) Header:** Includes filters for "Last 7 Days" and a search bar.
- Top Blades:** A bar chart showing "Threat Prevention" and "Threat Emulation" with values around 10.
- Top Applications:** A section indicating "No data found."
- Top Users:** A section indicating "No data found."
- Timeline:** A horizontal bar chart showing activity from 6:00 AM to 6:00 PM.
- Logs Table:** A detailed table of log entries with columns: Time, Blade, Severity, Action, Origin, Source, User, and Destination. It lists multiple "Threat Emulation" events with "Critical" severity and "Detect" actions, originating from "gr-lucy-mta365.ge.cloud.checkpoint.com".
- Threat Emulation Details:** A section for the selected event (May 25, 2016 1:36:07 PM, Critical) showing:
 - Account:** 176 Threat Emulation
 - Blade:** Germany
 - Destination Country:** user@americas-demo.com
 - Email Recipient:** 8ed1801ed70d797708b0ad56dc...
 - File MD5:** xfs
 - File SHA1:** 300000-4700-5300-5ca7-8da2...
 - Interface Name:** MTA
 - Log ID:** 40K
 - Malware Activity:** Behaves like a known malware...
 - Packet Capture:** 6a0b8b9-6447057-820c0-1199...
 - Product_Family:** 0000000-0002-9047-A200-A75...
- Threat Detection Details:** A section showing:
 - Action:** Detect
 - Confidence Level:** 25
 - Destination Port:** 618da8f11b952c4360ea299081...
 - Email Subject:** c64ac0d01e4833ca001d3497...
 - File Name:** MTA
 - Log Server IP:** 2147483647
 - Log Server IP:** GS-FWPCPD01-LOGS
 - Malware Rule Name:** S19851f5-287f-6240-9f49-8ba2...
 - Protection Name:** gr-lucy-mta365.ge.cloud.check...
 - Threat:** Threat
- Destination Details:** A section showing:
 - Destination:** Check Point Threat Cloud
 - Destination:** gr-lucy-mta365.ge.cloud.check...
 - Email Subject:** 1
 - File Size:** FWD: FWD: DO NOT OPEN
 - File SHA1:** 1.1M
 - Interface Direction:** 887115e12dc8b0e8dbf6d6f...
 - Last Update Time:** Inbound
 - Log Server ID:** 1646172507000
 - Malware Rule Name:** 217.68.8.6
 - Packet Capture:** Exploited via document

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.