Check Point
SOFTWARE TECHNOLOGIES LTD.

ONE STEP AHEAD

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

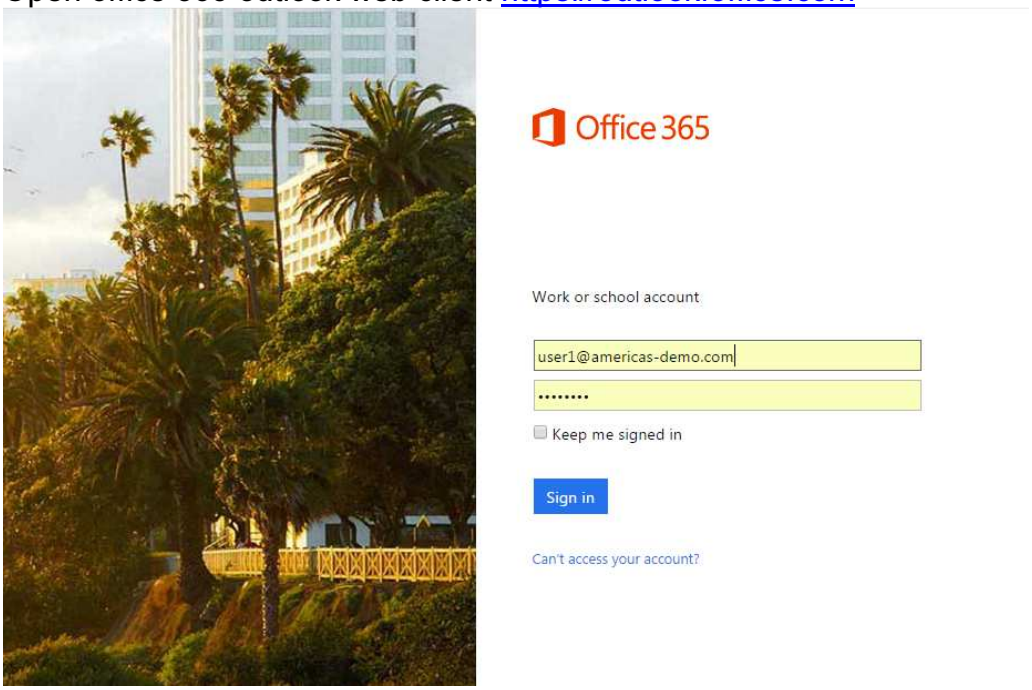
Office 365 – https://outlook.office.com
Username – user1@ama-demo.com
Password – Cpwins1!

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

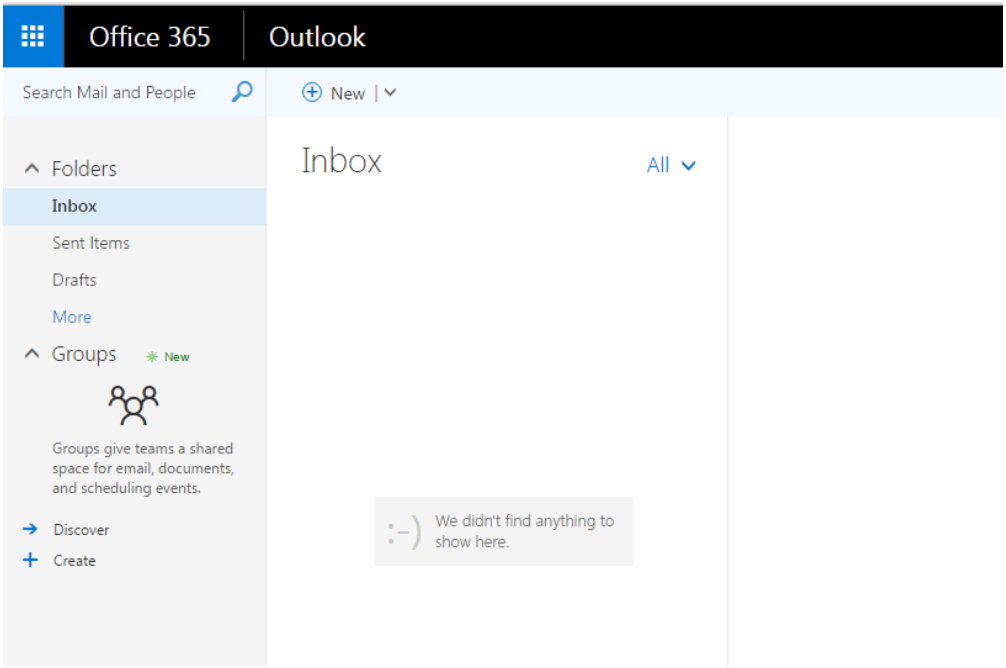
Preparation

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

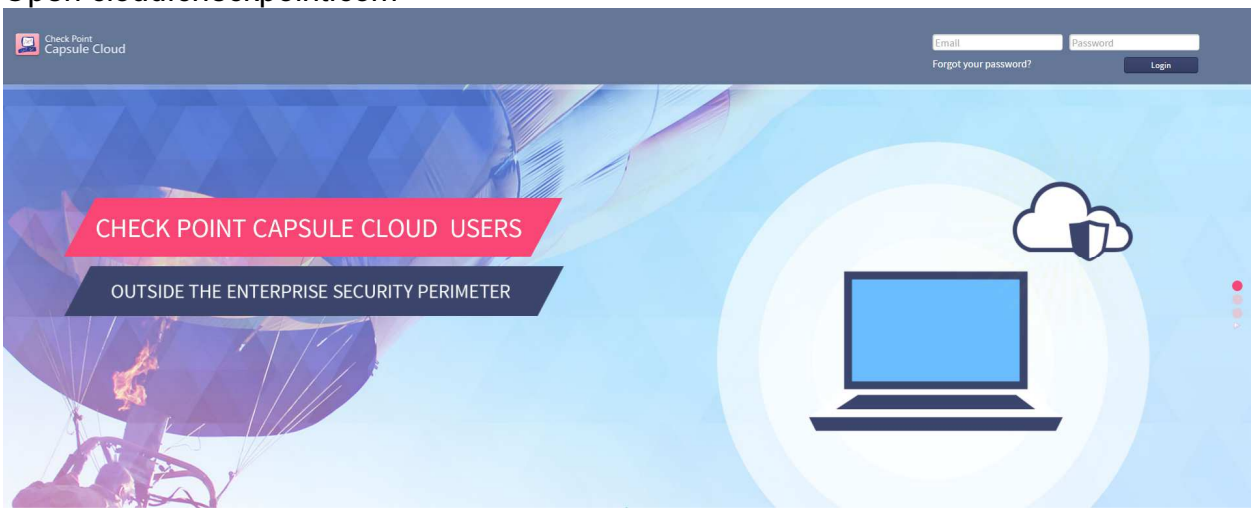


Type in the user and password
Username – user1@ama-demo.com
Password – Cpwins1!

This is the screen you will get

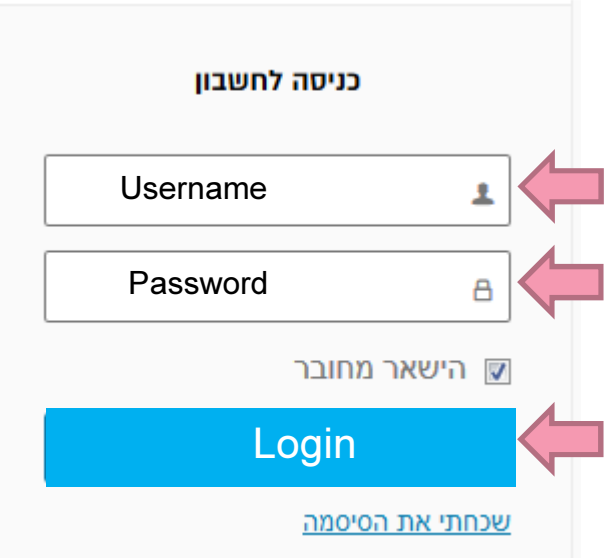


Open cloud.checkpoint.com

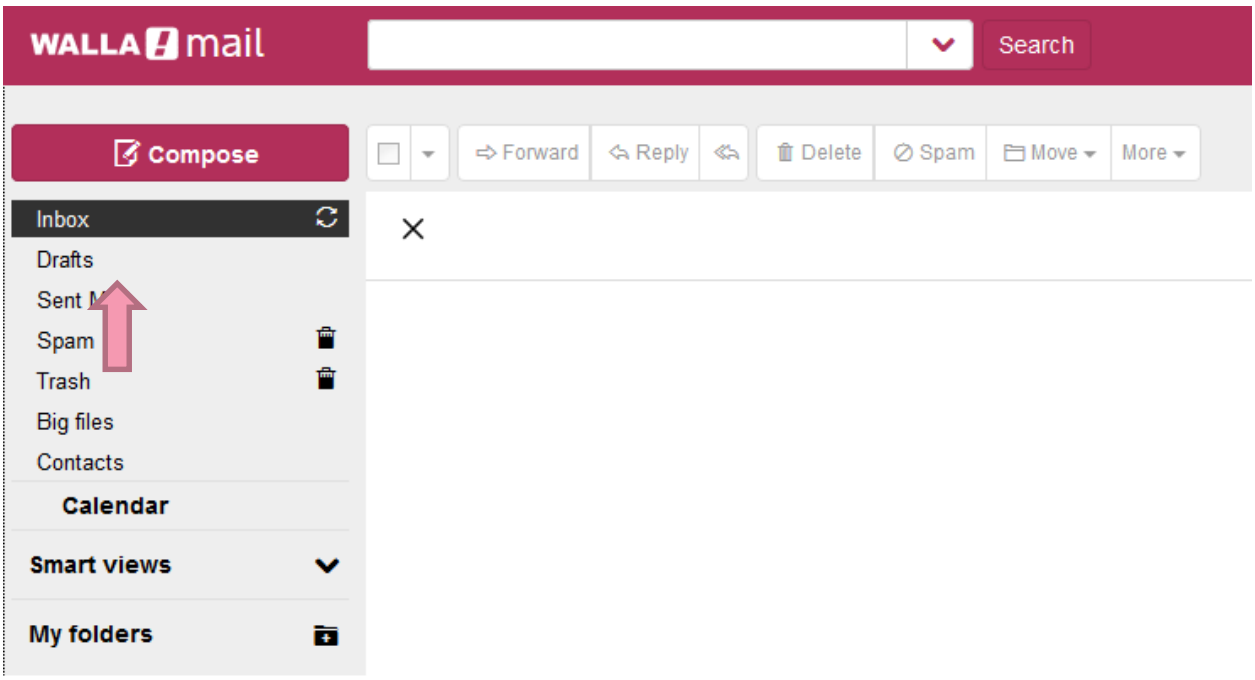


Enter your credentials based on the invitation you have received.
If you have not received an invitation please contact sagy@checkpoint.com and ask for credentials (please allow up to 24 hours)

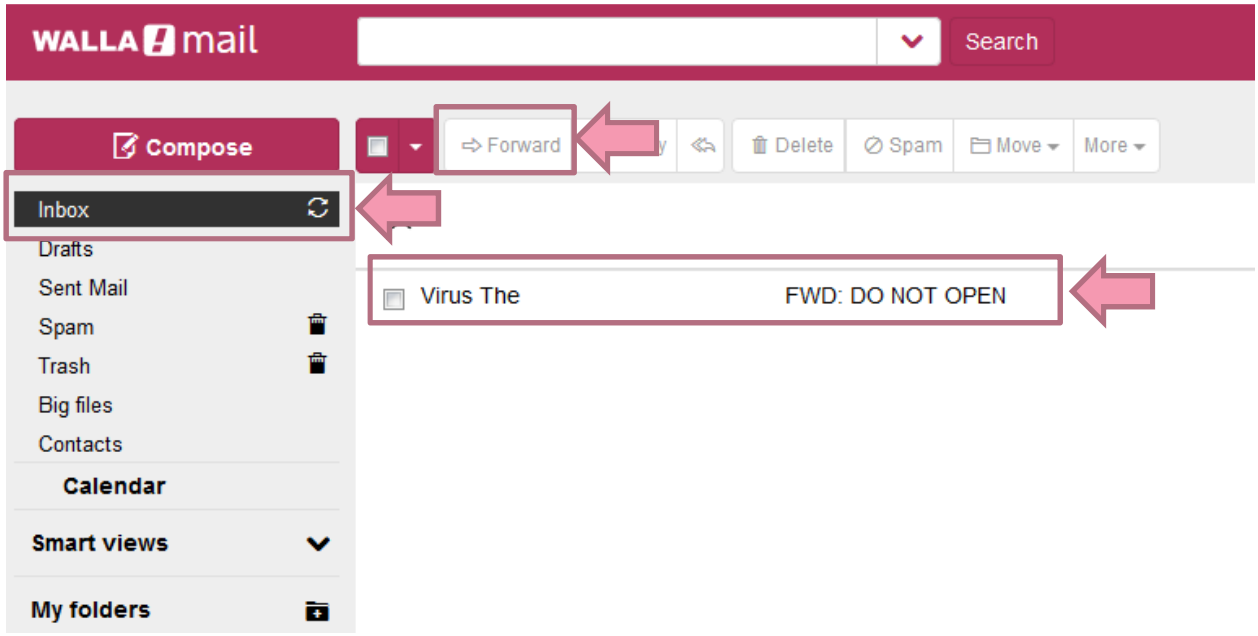
Login to an external email web client
https://friends.walla.co.il/#/login

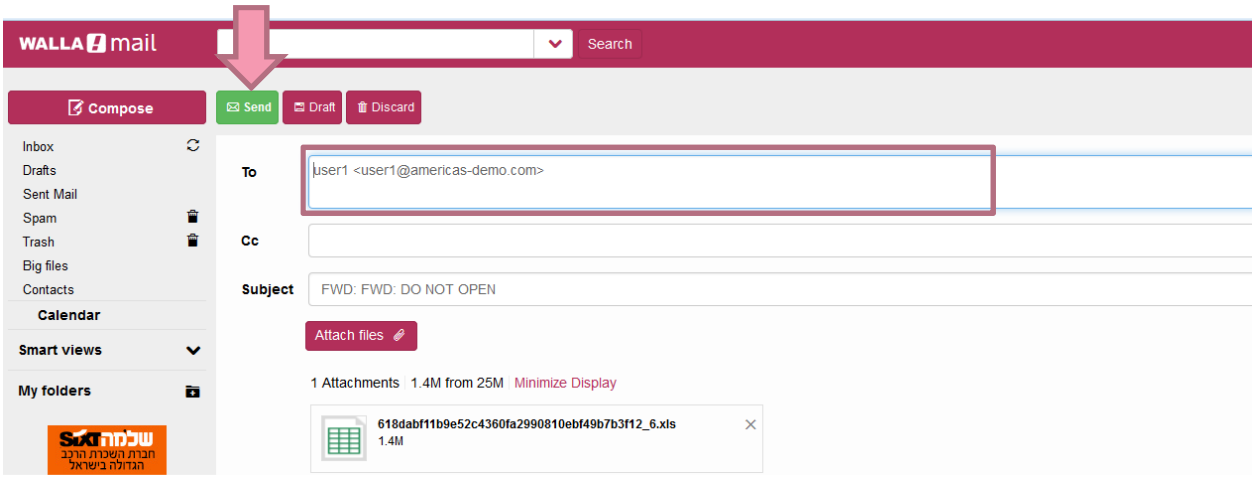


Username - ama365demo@walla.com
Password - Cpwins1!
Click on Login

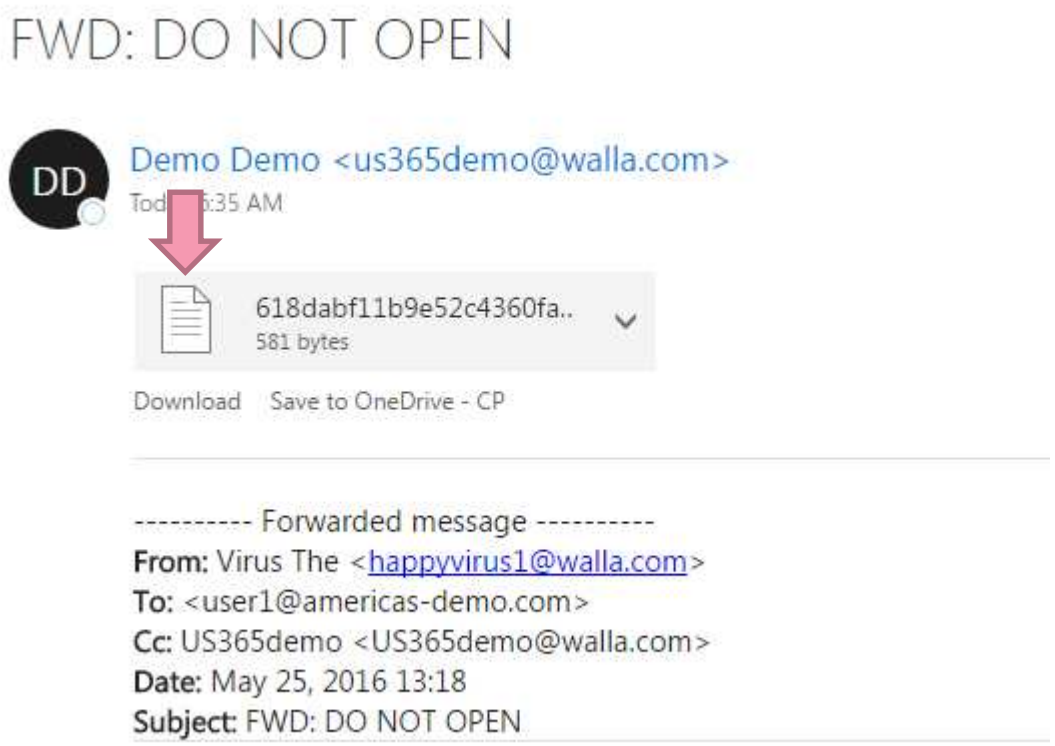


After login go to “Inbox” and forward the malicious email with subject “Do Not Open” send it to the office365 email address user1@ama-demo.com
And click “SEND”



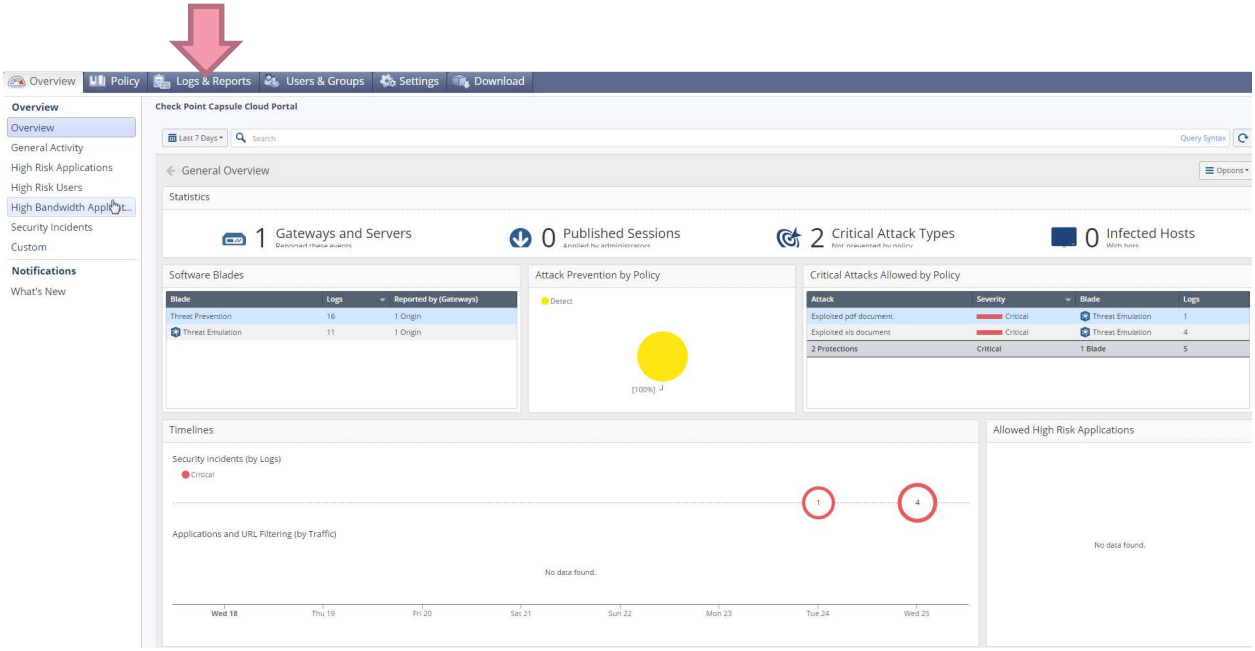


After clicking “SEND” go to the office 365 console and look for the email.
If you are in prevent mode the email will appear with a text file attachment stating that the malicious XLS file was removed

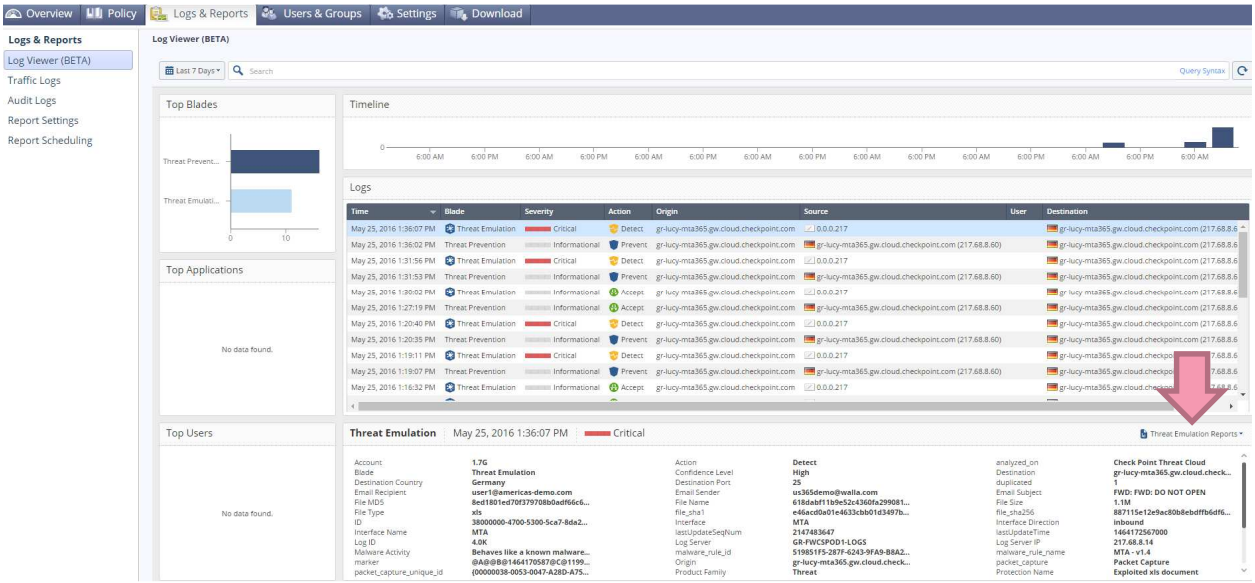


If you are working in detect mode the email with malicious attachment will arrive as is.

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



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.

