Check Point
SOFTWARE TECHNOLOGIES LTD

Harmony
Email & Collaboration

SECURE YOUR EVERYTHING™

How Check Point Harmony Email & Collaboration Compares to Microsoft ATP

Table of Contents

Executive Summary

Targeted and sophisticated email attacks bypass Office 365 default security (EOP) and require more advanced defensive technologies. To fill this need, Microsoft created Advanced Threat Protection (ATP) for Office 365, with additional security for anti-phishing, spoof intelligence, malware protection (Safe Attachments), and malicious link protection (Safe Links).

ATP is an improvement on EOP, but as reported by Gartner in "Market Guide for Secure Email Gateways," the security features of ATP are insufficient: "Gartner clients have found the email security capabilities of Office 365 to be lagging compared to other SEG market leaders. As a result, 35% of client organizations that move to Office 365 are supplementing its natively available email security capabilities with a third-party product."[1] In another report, "Fighting Phishing — 2020 Foresight," they add "As Microsoft's SEG market share increases, smart attackers will specifically target Microsoft's defenses. Vendors that have been fully focused on this market are responding more rapidly to changing threats than vendors that offer broad portfolios of security services."[2] In addition to its blind spots in detecting and blocking hackers, Office 365 lacks tools to quickly investigate and resolve successful attacks. To minimize the impact of attacks that go through, IT security teams require workflows and automations, as well as incident-response, forensic, and reporting. In these areas, Office 365 offers very little, and its built-in governance capabilities will frustrate most security professionals.

Many customers using ATP find that it is not enough, and seek out Check Point Harmony Email & Collaboration to add multiple layers to their existing security. After experiencing Check Point Harmony Email & Collaboration, they might use Check Point Harmony Email & Collaboration with ATP, but typically revoke their contract with ATP for Check Point Harmony Email & Collaboration. Check Point Harmony Email & Collaboration security for Office 365 works after Office 365 security; therefore, it can operate with or without ATP scanning first in front of it, and will report each detected attack whether or not it was flagged by ATP or EOP.

To deploy Check Point in the Office 365 environment, the admin approves the app, then adds anti-phishing, anti-malware, DLP and more to run advanced security technologies. Check Point Harmony Email & Collaboration security layers include anti-phishing, anti-malware, URL reputation, anomaly and compromised accounts detection, insider threat detection, insecure configuration detection, data-leakage prevention and encryption, and more.

Because Check Point Harmony Email & Collaboration scans content using multiple vendors after EOP and ATP complete their scans, Check Point Harmony Email & Collaboration analysts have been able to identify and study the advanced attacks that bypass Office 365. For this reason, Check Point Harmony Email & Collaboration was the first to report multiple obfuscation attacks ATP fails to block, such as baseStriker, ZeroFont, and Z-WASP. In this white paper, we examine ATP as a product and compare its offerings to Check Point Harmony Email & Collaboration platform.

We divided the analysis to two key sections:

1. Pre-attack: the technologies and their effectiveness in preventing attacks.

2. Post-attack: the forensic tools that scope and respond ("search and destroy") to successful attacks.

ATP Shortfalls (Pre-Attack)

SECURITY	WHAT IS MISSING IN ATP	CHECK POINT'S SOLUTION
Static Layer to Block Malicious URLs	• URLs are checked against a static database. • Safe Links fails when the URL is in an attachment. • Hackers use obfuscation methods to prevent ATP from properly parsing the URL. • Safelinks hides the original URL from the end-user, providing a false perception that it is secured.	• Feeds from 3 malicious URL blacklists coming from independent sources. • Reputation-based layer prevents the flaws of static analysis that hackers exploit in ATP. • Analyzes multiple parameters in the links including what they point to, the link format, the site.
Machine Learning for Anti-Phishing	• Static in nature — Blocks specific campaigns after they are learned. • Hackers bypass by making small variations in known attacks. • Anti-Spoof policies for targeted phishing campaigns apply to a maximum of 60 users. • Customers report that fine-tuning the policy requires multiple and confusing configurations. • Core algorithm is identical to all customers, not leveraging the unique characteristics of each organization.	• Dynamic — Looks for over 300 indicators of phishing in each email in order to block zero-day/unknown phishing campaigns. • Attack methods are added as indicators, working against the hacker. • Algorithm baselines the specific communication patterns of users at each organization. • Learns from historical emails.
Anti-Malware	• Poor detection results for malware in PDF formats. (Better results in Word and Excel files, especially for macro-based malware.) • Links to files aren't downloaded and scanned. Even with Safe Links, ATP will only sandbox the file upon click as not to delay the end-user, resulting in malware getting to the endpoint.	• Recursively scans for links in files and files downloaded from links.
Account Takeover Protection	• ATP doesn't come with user behavior analytics; Advanced Threat Analytics (ATA) must be purchased for this capability. • Can't send real time alerts for suspicious user behavior. • No per-customer and per-end-user baselining for typical logins. • Does not track outgoing phishing and malware, which is a key indicator of a compromised account. • Doesn't flag insecure configurations in use.	• Baselines safe behavior upon deployment using historical data. • **Alerts in real-time.** • Baselining is done per user and is specific to the organization. • Also tracks non-login activities like sending rate, mail-flow rule creation, outgoing phishing attacks, multiple recipients in BCC, etc. as ways to flag compromised accounts. • Flags insecure configurations in use, like mail-forwarding rules.

ATP Shortfalls (Pre-Attack)

SECURITY	WHAT IS MISSING IN ATP	CHECK POINT'S SOLUTION
Search and Destroy: a Missed Phishing Email	• Admin can only search campaigns by sender and subject. • It takes several hours for the data to be fully available in the logs.	• One-click blocking of campaigns that also removes all similar phishing emails from inboxes, as well as all future variations of this campaign. • Searching and blocking can be done by all relevant fields of the email: sender, subject, recipient, attachment name, sending IP, sending domain, email content, and more.
Incident Response: a Compromised Account	• No single-pane view for account activities, like configuration changes, emails sent, etc, making it harder to determine account compromise. • Not real time. In our analysis, even after 10K logins from 100+ countries, no real time alert is created.	• UEBA and login events generate alerts for admin, and historical scans identify compromised accounts upon deployment. • Incidents are reported in real time. • Drill-down and easy view of everything suspicious with the account.
Forensic Tools	• Threat Explorer only lists basic information about the attack, limiting the depth of forensics. • Reporting is limited to last 7 days. Admin must request a special report for older data, with no commitment on delivery time. • Top malware report only shows total count of malware, with no drill down to see the actual information.	• Reporting and exporting available from most screens, including: the main dashboard, analytics screens, and a request from an end-user to release from quarantine. Each provide full information for the admin to take the correct action. • Detailed email profile, with advanced header information, email attachment details, intel about suspicious activities, confidence scores, risk levels, and sandboxing emulation videos for files.
Policy Configuration	• Cumbersome configurations with limited flexibility of scope, workflows, and enforcement.	• Monitor only mode, Detect & Prevent mode, and Protect Inline let admin remediate manually or automatically using workflows that take effect within the inbox or before the inbox. • Per named-users and/or per group(s) policy for flexible deployment.
Workflows and Automation: Working with End Users	• End-user receives .txt file with 3 lines of information that is indecipherable to them. • End-users can't request restores from quarantine.	• End-users can request to restore content from quarantine from the email body. • Rich options for workflows, from self-remediation (end-user can release from quarantine) or require admin approval, with fully customizable templates for end-user interaction. • End-users' activity impact the machine learning to improve its decision.

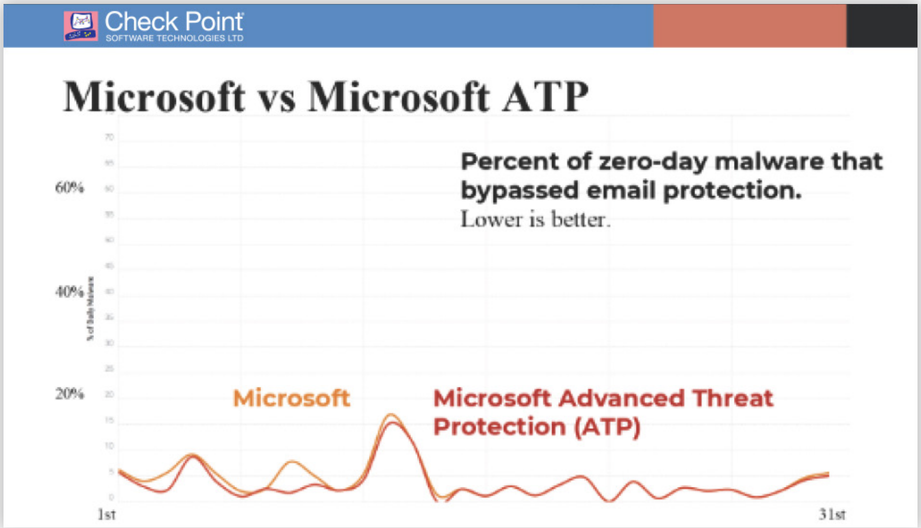
1. Threat Landscape

Email continues to be the primary source of compromise for companies of all sizes. Proliferation of obfuscation methods such as multiple redirections, HTML tag manipulation, polymorphic malware, and dynamic obfuscated scripts, bypass automated anti-phishing and anti-malware technologies. Publicly available information about employees facilitate sophisticated impersonation methods that trick the recipient of the email.

Most people who are going to click a phishing email do so in just over an hour.[3]

Microsoft created ATP to add onto EOP and stop targeted spear phishing attacks with four main policy engines for anti-phishing, spoof intelligence, Safe Links, and Safe Attachments. Despite these more advanced features, ATP remains a rules-based security technology that relies on static reputation-based filtering that hackers reverse engineer until they find ways in which to bypass ATP. As explained by Gartner in "What You Need to Know About Security in Office 365," "Despite Microsoft's continued investment in Office 365 security improvements, some Gartner clients report dissatisfaction with EOP and ATP."

The graph below compares EOP's basic security to ATP by pushing daily zero-day malware. ATP performs marginally better than EOP, the Office 365 default security, and misses between 5%-20% of same day malware.



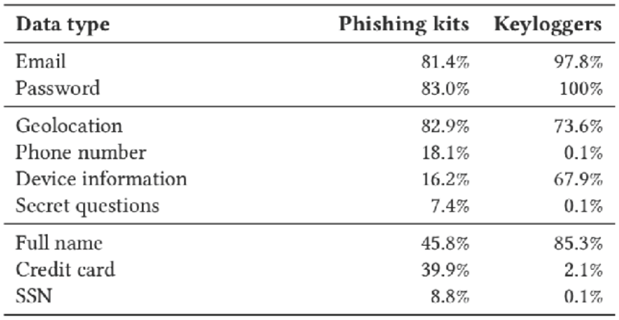
We tested ATP and found it made only a minor difference in how much malware got through the Office 365 environment compared to EOP alone.

1. Threat Landscape

Single sign-on (SSO) solutions add protection from account takeover,but are cumbersome to adopt, which is why most companies decide not to deploy them. For those companies who use Microsoft as their SSO, hackers have found ways to bypass it by making the user add second factor to a fake page.

Well developed criminal monetization channels are the driving force behind most phishing campaigns. Those include ransomware, fake financial transactions, compromised DocuSign accounts, PayPal spoofs, and more. All this amounts to the fact that nearly every organization has been targeted in an attack, regardless of company size.

Additional information stolen by phishing kits and keyloggers. We note that some phishing kits exclusively collect credit card details rather than usernames and passwords.



Data type	Phishing kits	Keyloggers
Email	81.4%	97.8%
Password	83.0%	100%
Geolocation	82.9%	73.6%
Phone number	18.1%	0.1%
Device information	16.2%	67.9%
Secret questions	7.4%	0.1%
Full name	45.8%	85.3%
Credit card	39.9%	2.1%
SSN	8.8%	0.1%

These are the top 10 brands impersonated by threat actors, according to this Google report.[4]

Microsoft's widespread adoption and success make it a target for every hacker — never before have so many mailboxes had exactly the same security. Hackers also leverage the fact Office 365 accounts are the source of authentication to other enterprise SaaS apps. This "transitive trust" makes compromised accounts a bigger risk to the organization. Once an account is compromised, hackers often leverage that to spread to other mailboxes — in some cases, they even respond to existing threads making the spoofed email appear very natural in the context of a legitimate conversation.

2. Preventing the Attack: Required Layers of Email Security

This section discusses the key layers of an effective Office 365 security strategy and compares ATP and Check Point Harmony Email & Collaboration's offerings for each.

2.I. Static Layer to Block Malicious URLs

Microsoft ATP

ATP adds SafeLinks as a time-of-click security layer to the Office 365 URL blacklist. Each URL is replaced with a rewritten URL that leads to Microsoft, which tests the URL against its database of known attacks upon the time of click, and redirects the end user's browser to the original URL if it's not a known attack. In "Fighting Phishing — 2020 Foresight,"[5] Gartner recommends this general approach:

Using best practices for preventing malicious URL links involves a two-step process:

1. The vendor first detects and removes any known bad URLs, then attempts to validate or verify the destination of unknown or "safe" URLs, discarding those that resolve to malicious sites or suspicious content.
2. Any remaining hyperlinks in the email are replaced with new encoded hyperlinks that act as a proxy via the anti-phishing provider, allowing a click-time URL reputation and website check.

Hackers fool this first step in multiple ways. First, this is still a static layer, and based on the data we collected, it usually takes 4 to 24 hours before Microsoft adds a malicious URL to the blacklist. In addition, multiple obfuscation methods prevent Office 365 from properly parsing the URL. Therefore, even after the URL is blacklisted, ATP won't identify it as URL and will fail to block it. (Some examples published by Check Point Harmony Email & Collaboration include the baseStriker[6], zeroFont[7] , and ZWSP[8] attacks). SafeLinks also fails when the URL is in an attachment. Another common method of attack is to use link shorteners,multiple redirections,and public links on file sharing platforms like Sharepoint and Google-Drive. Finally, hopping to a new link once the malicious one is exposed is a low cost operation for hackers, and access to Office 365 allows them to automate the process.

Check Point Harmony Email & Collaboration

Check Point Harmony Email & Collaboration feeds from 3 malicious link sources, including a leading AV vendor, Google Safe Browsing, and PhishTank. These sources were selected after benchmarking multiple URL reputation feeds. Based on our analysis, even the best of those tools are limited, catching only 15-17% of the malicious links at the time the link is clicked. As most of these attacks are zero-day, a reputation-based layer is required. This is a fundamental flaw in the static analysis provided by SafeLinks,

2. Preventing the Attack: Required Layers of Email Security

2.2. Machine Learning for Anti-Phishing

Microsoft ATP

Any organization that has an Office 365 account automatically has a default anti-phishing policy apply to all users. Microsoft ATP provides several additional analysis tools for detecting phishing attacks such as blacklisting, sender reputation, and more. After having read through Microsoft testing and performing tests, we observed that those layers are apparently static in nature, and do not seem to include advanced machine-learning. Even with ATP, Office 365 will be able to block specific campaigns only after they are learned because of this static layer. And if the hacker makes a small variation of the very same campaign, they will be able to bypass the static layer. Worst of all, custom policies for more targeted phishing campaigns characterized by impersonations and spoofs only apply to a maximum of 60 users[9] in Office 365.

"Microsoft has an opportunity and an incentive to solve the phishing issues, but based on historical results, it must become more agile and respond more rapidly to changing attacker tactics. As Microsoft's SEG market share increases, smart attackers will specifically target Microsoft's defenses." – Gartner, "Fighting Phishing — 2020 Foresight" [10]

Creating anti-phishing policies in ATP requires multiple configurations, each with different priorities for enforcement. Once the policy is set up, it takes 30 minutes for it to take effect. When the policy detects a threat, it will do 1of 3 things: quarantine the message, move the message to the recipient's junk folder, or not apply any action for admins who prefer to remediate manually.

"When we demonstrated attacks coming through to Microsoft, they recommended we purchase ATP. When we demonstrated attacks pass unblocked after purchasing ATP, Microsoft support told us we misconfigured ATP. After 3 months of failing to configure ATP with the Microsoft support, we just gave up." – Anonymous former ATP customer

2. Preventing the Attack: Required Layers of Email Security

2.2. Machine Learning for Anti-Phishing

Check Point Harmony Email & Collaboration

The power of A.I. and machine learning is such that when analyzing a specific attack, the machine learns numerous indicators of the attack to block similar attacks, even when the hackers try to change its characteristics. Check Point Harmony Email & Collaboration's machine-learning, SmartPhish, was built specifically to target the threats that EOP and ATP miss, using over 300 indicators in every email. When Check Point Security Analysts learn of a hacker trick for bypassing Office 365 — such as the link splitting that was weaponized in the base Striker attack — that method becomes an indicator as well. The indicators analyze every piece of the email using features like Natural Language Processing (NLP), user impersonation detection, brand impersonation detection, sender spoof detection, and more.

> ***"Generally, with AI, what you train the machine on, is what it's going to catch. So we trained specifically on the things Microsoft misses and specifically on the attack methods that people use in order to bypass Microsoft." – Gil Friedrich, Check Point*** [11]

In addition, the algorithm baselines the specific communication used in the organization — the past communication between its users, focusing on the language and words used. In doing so, SmartPhish's processing power is more specific to the organization it protects, resulting in more accurate detections for the company. The admin and the end users can continuously train the A.I by marking certain emails as clean and malicious.

Check Point Harmony Email & Collaboration's customer-specific configuration learns from historical emails. For example, the brand of one of our customers was frequently spoofed in the wild and used in far-reaching phishing campaigns. The company needed to distinguish between legitimate and illegitimate correspondences, and Check Point Harmony Email & Collaboration's ability to fine-tune the AI for them was key when it came to accurately identifying attacks and drastically reducing disruptions to business.

> ***"Microsoft ATP couldn't compare to the amount of phishing attacks caught by Check Point Harmony Email & Collaboration." – Hershell Foster, CIO, Capital Caring*** [12]

2. Preventing the Attack: Required Layers of Email Security

2.3. Anti-Malware

Microsoft ATP

ATP scans for malware in attachments, and in our tests, proved itself adept at blocking malware in file formats from the Office 365 suite, such as Word and Excel, but is more vulnerable to PDF formats. To study how much malware ATP misses, Check Point Harmony Email & Collaboration gathered the data collected by its malware partners, then pushed the known-to-be-malicious malware to Office 365. Check Point discovered that ATP missed between 5-12% of zero-day malware attacks. Common attack include links within files, and yet ATP will neither scan nor apply Safe Links on them. If the malware is downloaded as a link in the email body, ATP won't scan until the link is clicked, and will not be able to perform complete sandboxing of the file because it does not want to delay the end user. These complications amount in an unreliable anti-malware service.

Check Point Harmony Email & Collaboration

Check Point Harmony Email & Collaboration scans links to files in the email body and links within files, recursively scanning every link for malware. We also enlist help from the industry's best anti-malware vendors. NSSLabs, an authority on cybersecurity tools, released empirical data[13] proving that Check Point has the highest security effectiveness in the malware category, where Microsoft was neither mentioned nor tested.

Admin can deploy the strictest anti-malware policies on Check Point Harmony Email & Collaboration, because users can take advantage of the "release from quarantine" workflow. When the admin open the request, they are linked to rich reporting and forensics on the suspected malware. When suspicious files are quarantined, users can ask to release them, and the admin can review a full sandbox report and threat emulation video (which Microsoft doesn't provide) that shows exactly what actions the malware takes when it is opened. These features help the admin to make an informed decision that takes the needs of users into account.

2. Preventing the Attack: Required Layers of Email Security

2.4. Account Takeover Protection

Microsoft ATP

ATP for Office 365 doesn't come with user behavior analytics. Organizations must purchases Azure AD or Advanced Threat Analytics (ATA) for machine learning to understand the safe behavior of users in the Office 365 environment. Without these additional tools, ATP can't send real-time alerts for suspicious user behavior,or connect with auto-action to force MFA and immediately disable accounts suspected to be compromised. Office 365 lacks user-specific or customer-specific data about suspicious behavior, such as logins from countries where business is not conducted. While ATP offers static layers for this function, it requires the admin to setup each configuration. For example, Office 365 will not base-line the countries the organization is using or flags logins from foreign countries.

Check Point Harmony Email & Collaboration

Upon deployment, Check Point Harmony Email & Collaboration automatically baselines safe behavior on a per-user, per-company basis. On the threat management dashboard homepage, Check Point Harmony Email & Collaboration provides a login map showing both suspicious and safe logins. When a suspicious login is detected, Check Point Harmony Email & Collaboration automatically sends alerts. Each alert can easily become a geo-restriction static layer, blocking all logins from outside the US, for example, or other global regions where the specific business would normally not be conducted. Beyond suspicious logins, there are certain configurations that point to a compromised account, and Check Point Harmony Email & Collaboration flags them as such. While some configurations might be legitimate, they still can be a security issue. One common example of such configuration Check Point Harmony Email & Collaboration flags is email forwarding, when a user forwards all their email to an external address — a common configuration in business email compromise that conceals a hacker's activity. Microsoft doesn't flag insecure configurations in use.

2. Preventing the Attack: Required Layers of Email Security

2.5. DLP

Microsoft ATP

DLP is not part of ATP—therefore,we will keep this section brief. EOP offers basic compliance rules and scans regular expressions, but doesn't scan word- vicinity, keyword relations, OCR scanned documents, or other methods used by advanced DLP tools.

Check Point Harmony Email & Collaboration

Check Point Harmony Email & Collaboration offers best of breed DLP tools, such as Symantec and GTB. Our DLP policy can sync with on-prem DLP and existing DLP rules. When the end user sends a message where data leakage was identified, flexible workflows present an "Are you sure?" message, letting them send it using encryption options from Microsoft or other third party tools.

PCI DSS COMPLIANT
FISMA COMPLIANCE
HIPAA COMPLIANCE
SOX COMPLIANCE
FERPA COMPLIANT
GDPR

3. Email Security: Post-Attack

Some attacks will inevitably get through, given that "currently, an average of roughly one out of every 4,500 emails is a phishing attack."[14] A real-time incidents-response platform with the relevant forensic capabilities and the ability to "search and destroy" emails from end users' mailboxes, is key, and most admins of Office 365 have been frustrated when investigating phishing attacks in Office 365.

In this section,we explore threat management in ATP and Check Point Harmony Email & Collaboration, comparing the features for remediation post-breach with a focus on how using each platform factors into the overall email security posture.

3.1. Search and Destroy: a Missed Phishing Email

Microsoft ATP

In ATP, it is up to end users to report of a phishing campaign that went to their Office 365 mailbox. When admin are notified of a potential attack, they lack a few key capabilities they would need in this use case:

1. A one-click button that shows all similar emails.
2. A list of which users clicked the link and fell victim to the attack.
3. Real-time data on the phishing campaign.

Office 365 makes it difficult to see similar malicious emails that the organization received. Furthermore, it's complex to report who click the links—assuming Safe Links is used. Because the data is not real time, it takes several hours before it is fully available in the logs.

Check Point Harmony Email & Collaboration

The Check Point Harmony Email & Collaboration UI provides a full incident response suite. The end users can easily report an email as suspicious, and the admin can quickly see who else in the organization received and interacted with the email. It then allows the admin to take actions, such as:

1. One-click blocking. By adding a static rule, the admin can immediately delete all similar emails from the end users' mailboxes.
2. Blocking any future emails of the same attack.
3. Adding the email to the machine-learning sample so it improves the catch rate and can learn of similar, future campaign.

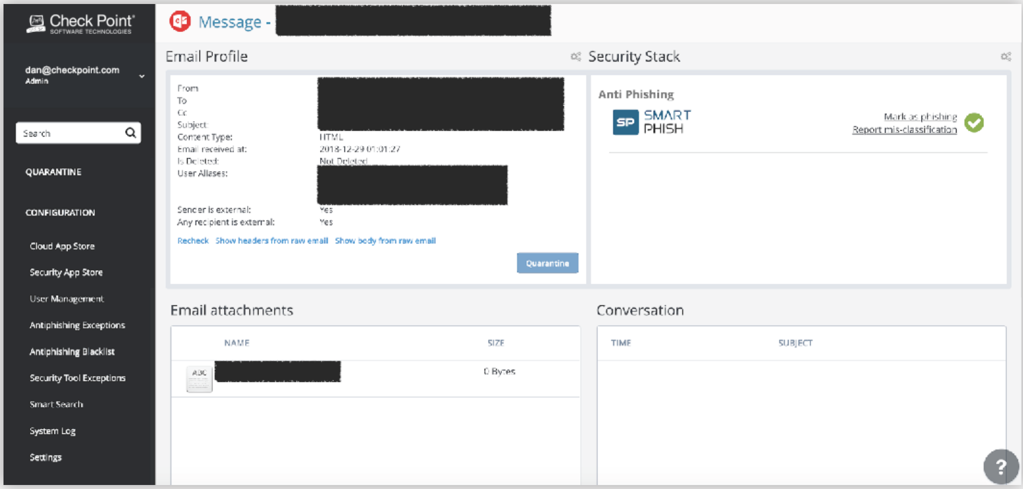
These workflows are all one-click away from the Check Point Harmony Email & Collaboration portal, making it easier to block campaigns and improve the model for future attacks.

3. Email Security: Post-Attack

3.1. Search and Destroy: a Missed Phishing Email

Check Point Harmony Email & Collaboration

The example below demonstrates this process in Check Point Harmony Email & Collaboration, starting from a clean email and clicking "Report Misclassification."



Message - [redacted]

Email Profile

From
To
Cc
Subject: [redacted]
Content Type: HTML
Email received at: 2018-12-29 01:01:27
Is Deleted: Not Deleted
User Aliases: [redacted]

Sender is external: Yes
Any recipient is external: Yes

Recheck Show headers from raw email Show body from raw email

Email attachments

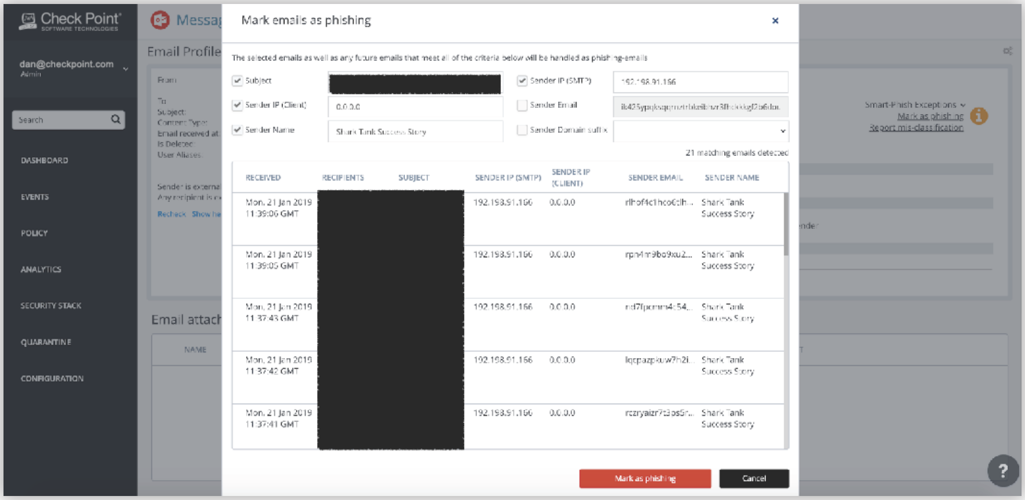
NAME	SIZE
[redacted]	0 Bytes

Conversation

TIME	SUBJECT

Admin see all similar emails sent to the organization, and in one click can:

- Delete those emails from all end users.
- Block future attacks.
- Have the machine-learning add this as a sample of phishing to block similar attacks in the future.



Mark emails as phishing

The selected emails as well as any future emails that meet all of the criteria below will be handled as phishing-emails

☑ Subject [redacted]
☑ Sender IP (SMTP) 192.198.91.166
☑ Sender IP (Client) 0.0.0.0
☐ Sender Email ik425ypqksqqmztrbkeibhzr3flhckkkgf2b6dor
☑ Sender Name Shark Tank Success Story
☐ Sender Domain suffix

21 matching emails detected

RECEIVED	RECIPIENTS	SUBJECT	SENDER IP (SMTP)	SENDER IP (CLIENT)	SENDER EMAIL	SENDER NAME
Mon, 21 Jan 2019 11:39:06 GMT	[redacted]	[redacted]	192.198.91.166	0.0.0.0	rlhof4c1hco6tlh...	Shark Tank Success Story
Mon, 21 Jan 2019 11:39:05 GMT	[redacted]	[redacted]	192.198.91.166	0.0.0.0	rpn4m9bo9xu2...	Shark Tank Success Story
Mon, 21 Jan 2019 11:37:43 GMT	[redacted]	[redacted]	192.198.91.166	0.0.0.0	nd7fpcmm4c54...	Shark Tank Success Story
Mon, 21 Jan 2019 11:37:42 GMT	[redacted]	[redacted]	192.198.91.166	0.0.0.0	lqcpazpkuw7h2i...	Shark Tank Success Story
Mon, 21 Jan 2019 11:37:41 GMT	[redacted]	[redacted]	192.198.91.166	0.0.0.0	rczryaizr7t3psSr...	Shark Tank Success Story

3. Email Security: Post-Attack

3.2. Incident Response: a Compromised Account

Microsoft ATP

ATP will notify the admin of a potentially compromised account. In addition, Microsoft documentation 15 recommends reviewing all activities of an account suspected to be compromised in the Office 365 Unified Audit Logs in the Security & Compliance Center. Filter the results by date range spanning from immediately before the suspicious activity occurred to the current date. Microsoft advises not to filter by activities during the search, because the information is delayed and not updated in real time.

The time it takes to flag an account as compromised is the biggest reported caveat with the built-in algorithm in ATP. This year, Check Point Harmony Email & Collaboration has identified an account protected by ATP that had 10,296 logins from different countries and continents, an account compromise which ATP did not report.

Check Point Harmony Email & Collaboration

Check Point Harmony Email & Collaboration will monitor all end user activity in the account, including:

- Logins from unknown locations.
- Sending more email than usual, or an email characteristic unusual for this sender (such as multiple recipients in the BCC).
- Sending phishing attacks to other users within and outside of the organization.
- Forwarding all mail to external mailboxes.
- Unusual email signatures.
- Rules that automatically delete all responses to hide activity.
- Multiple password changes.
- Nickname changes.

All of these are reported as indications of potential account take-over or an insecure configuration. The key differences between ATP and the Check Point Harmony Email & Collaboration algorithm are that:

1. Incidents are reported in real-time.
2. Check Point Harmony Email & Collaboration learns the specific characteristics of the organization and end user. The customer-specific baseline enables faster and more accurate detection.

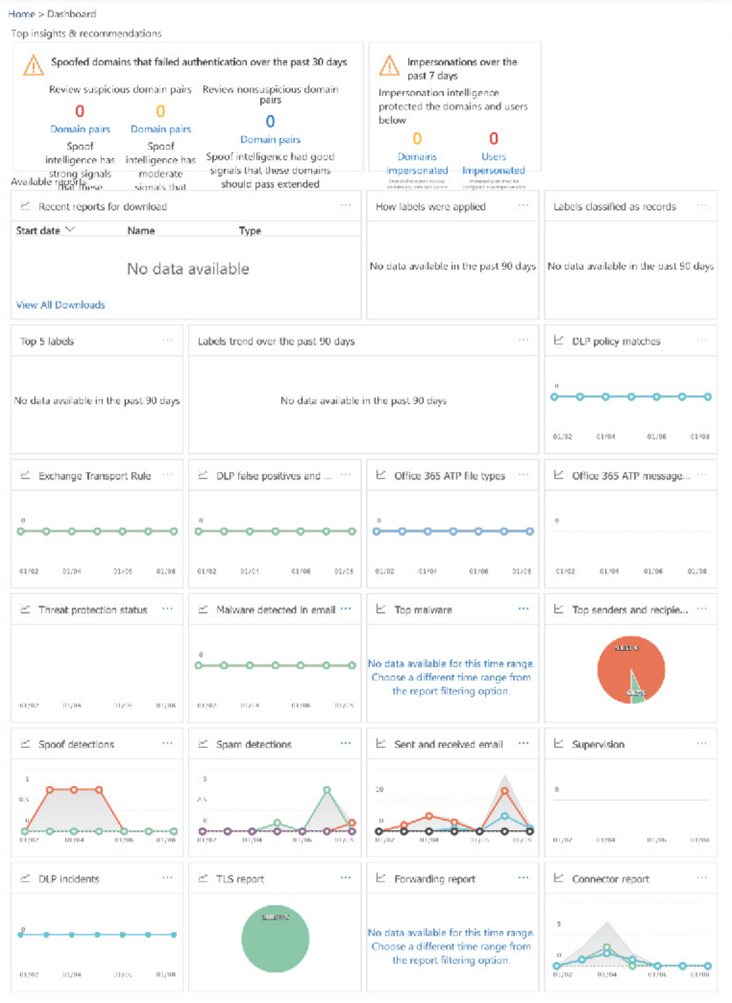
3. Email Security: Post-Attack

3.3. Forensic Tools

Microsoft ATP

ATP presents admin with an overwhelming amount of reports. Despite the sheer number of these reports, the level of detail ATP offers is minimal.

This is what Spoof Mail report looks like in ATP.


Home > Dashboard
Top insights & recommendations
Spoofed domains that failed authentication over the past 30 days
Review suspicious domain pairs
Review nonsuspicious domain pairs
0
Domain pairs
0
Domain pairs
0
Domain pairs
Impersonations over the past 7 days
0
Domains Impersonated
0
Users Impersonated
Available reports
Recent reports for download
Start date
Name
Type
View All Downloads
How labels were applied
Labels classified as records
Top 5 labels
Labels trend over the past 90 days
DLP policy matches
Exchange Transport Rule
DLP false positives and ...
Office 365 ATP file types
Office 365 ATP message...
Threat protection status
Malware detected in email
Top malware
Top senders and recipie...
Spoof detections
Spam detections
Sent and received email
Supervision
DLP incidents
TLS report
Forwarding report
Connector report
01/02
01/04
01/06
01/08

Spoof intelligence has strong signals that these

Spoof intelligence has moderate signals that

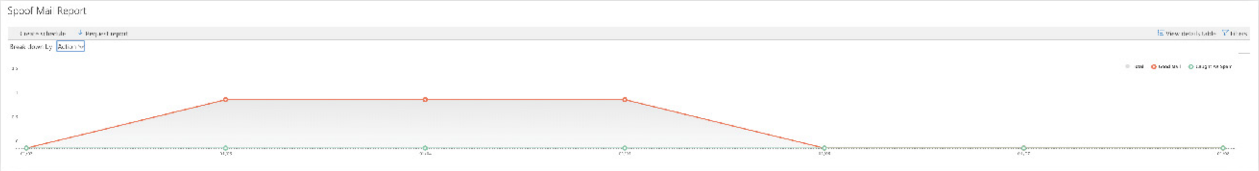
Spoof intelligence had good signals that these domains should pass extended

Impersonation intelligence protected the domains and users below

No data available

No data available in the past 90 days

No data available for this time range. Choose a different time range from the report filtering option.



After clicking on "View details table," ATP only provides the date, spoofed sender, true sender, sender IP, action, and message count.

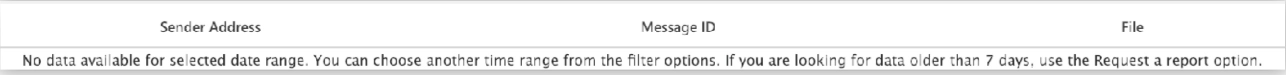
3. Email Security: Post-Attack

3.3. Forensic Tools

Microsoft ATP

Using ATP Threat Explorer feature, admin can gather details on active phishing attacks, with information on the sender, recipient, source IP address, file hashes, subject lines, and URL links to identify the impact on the Office 365 environment. ATP does not offer more information beyond merely listing these components of an attack.

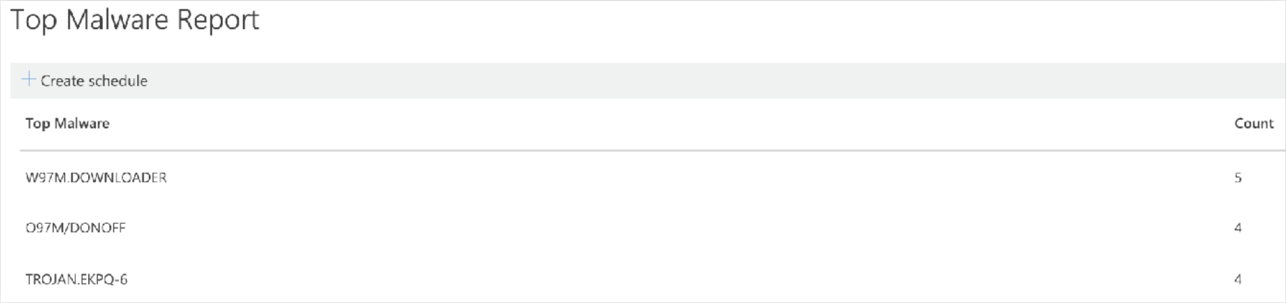
If the admin is investigating an event older than 7 days, they will encounter this message from ATP: "No data available for selected date range. If you are looking for data older than 7 days, use the Request a report option."



Sender Address	Message ID	File

No data available for selected date range. You can choose another time range from the filter options. If you are looking for data older than 7 days, use the Request a report option.

After clicking "View details table," ATP's "Top Malware" report still has very limited insights. The admin can only see the total count of malware.



Top Malware Report

Top Malware	Count
W97M.DOWNLOADER	5
O97M/DONOFF	4
TROJAN.EKPQ-6	4

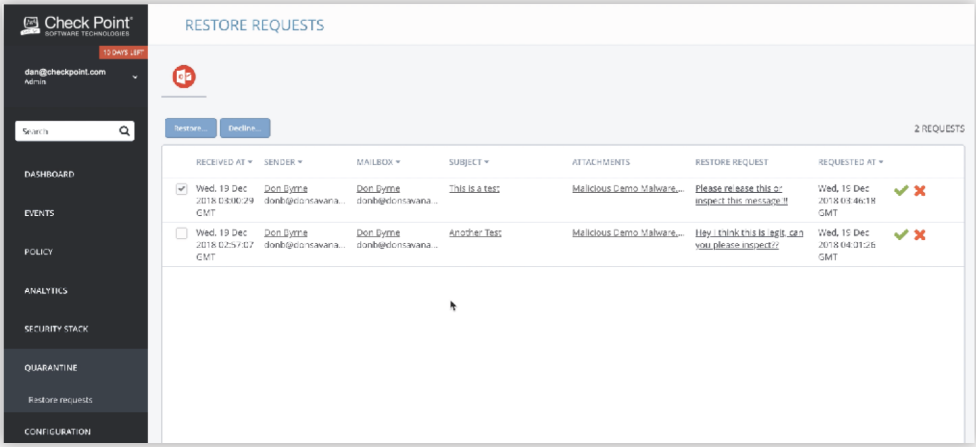
3. Email Security: Post-Attack

3.3. Forensic Tools

Check Point Harmony Email & Collaboration

Check Point Harmony Email & Collaboration's rich reporting is available at a glance on the dashboard homepage. Check Point Harmony Email & Collaboration's custom queries are flexible, which speeds up the pace of a forensic search. Admin can search by sender, subject, recipient, or attachment name. Within the query tool, admin can click on any "Sender" or "Recipient" to see a user profile detailing their top collaborators,whether they are internal users or external partners, and if their account is enabled with Check Point Harmony Email & Collaboration. Clicking on "Subject" reveals an email profile, with detailed information on the email header, attachments, all the links in the body and attachment. The query enables admin to quarantine individually or en masse.

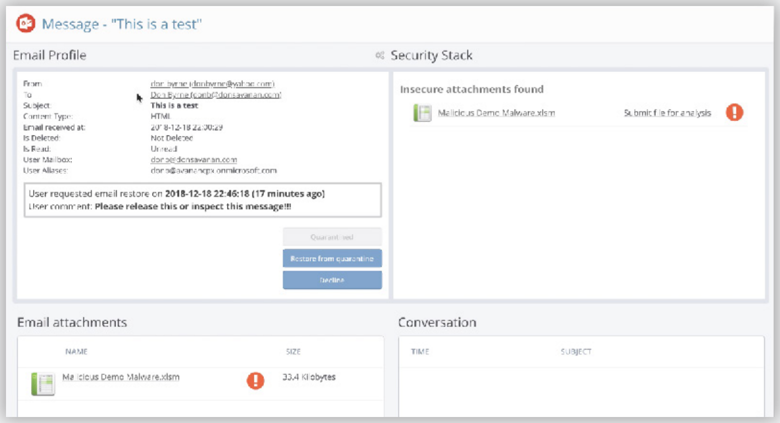
To investigate threats further, select either "Analytics" in the main navigation, or document restore requests submitted by end users whose attachments have been flagged as potentially malicious. In this section, I focus on what reporting looks like when it stems from a restore request, because it speaks to the logical flow of navigation on the platform that differentiates Check Point Harmony Email & Collaboration from ATP.



RESTORE REQUESTS

2 REQUESTS

	RECEIVED AT	SENDER	MAILBOX	SUBJECT	ATTACHMENTS	RESTORE REQUEST	REQUESTED AT	
☑	Wed, 19 Dec 2018 03:00:29 GMT	Don Byrne donb@donsavana...	Don Byrne donb@donsavana...	This is a test	Malicious Demo Malware,...	Please release this or inspect this message !!	Wed, 19 Dec 2018 03:46:18 GMT	✓ ✗
□	Wed, 19 Dec 2018 02:57:07 GMT	Don Byrne donb@donsavana...	Don Byrne donb@donsavana...	Another Test	Malicious Demo Malware,...	Hey I think this is legit, can you please inspect??	Wed, 19 Dec 2018 04:01:26 GMT	✓ ✗



Message - "This is a test"

Email Profile

From:	don byrne (donbyrne@yahoo.com)
To:	Don Byrne (donb@donsavanan.com)
Subject:	**This is a test**
Content Type:	HTML
Email received at:	2018-12-18 22:30:29
Is Deleted:	Not Deleted
Is Read:	Unread
User Mailbox:	donb@donsavanan.com
User Aliases:	donb@avanancpx.onmicrosoft.com

User requested email restore on **2018-12-18 22:46:18 (17 minutes ago)**
User comment: **Please release this or inspect this message!!!**

Security Stack

Insecure attachments found

Malicious Demo Malware.xlsm Submit file for analysis !

Email attachments

NAME		SIZE
Malicious Demo Malware.xlsm	!	33.4 Kilobytes

Conversation

TIME	SUBJECT

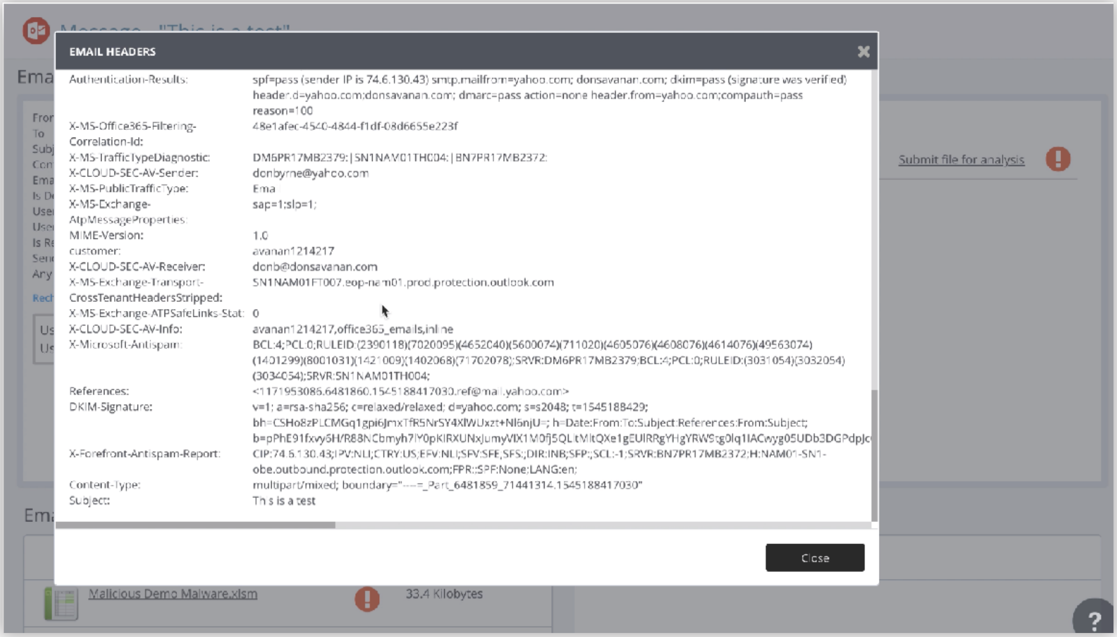
After clicking on the subject "Another Test," admin see a comprehensive report showing the email profile, header information, and the security that found the threat.

3. Email Security: Post-Attack

3.3. Forensic Tools

Check Point Harmony Email & Collaboration

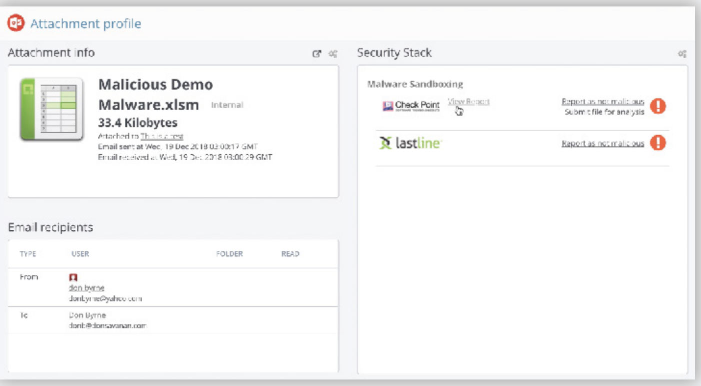
When admin click on the gear icon next to Security Stack (in the screenshot above) and click the "Advanced" checkbox, they see a detailed header report.



EMAIL HEADERS

```
Authentication-Results:           spf=pass (sender IP is 74.6.130.43) smtp.mailfrom=yahoo.com; donsavanan.com; dkim=pass (signature was verified)
                                  header.d=yahoo.com;donsavanan.com; dmarc=pass action=none header.from=yahoo.com;compauth=pass
                                  reason=100
X-MS-Office365-Filtering-         48e1afec-4540-4844-f1df-08d6655e223f
Correlation-Id:
X-MS-TrafficTypeDiagnostic:       DM6PR17MB2379:|SN1NAM01TH004:|BN7PR17MB2372:
X-CLOUD-SEC-AV-Sender:            donbyrne@yahoo.com
X-MS-PublicTrafficType:           Ema
X-MS-Exchange-                    sap=1;slp=1;
AtpMessageProperties:
MIME-Version:                     1.0
customer:                         avanan1214217
X-CLOUD-SEC-AV-Receiver:          donb@donsavanan.com
X-MS-Exchange-Transport-          SN1NAM01FT007.eop-nam01.prod.protection.outlook.com
CrossTenantHeadersStripped:
X-MS-Exchange-ATPSafeLinks-Stat:  0
X-CLOUD-SEC-AV-Info:              avanan1214217,office365_emails,inline
X-Microsoft-Antispam:             BCL:4;PCL:0;RULEID:(2390118)(7020095)(4652040)(5600074)(711020)(4605076)(4608076)(4614076)(49563074)
                                  (1401299)(8001031)(1421009)(1402068)(71702078);SRVR:DM6PR17MB2379;BCL:4;PCL:0;RULEID:(3031054)(3032054)
                                  (3034054);SRVR:SN1NAM01TH004;
References:                       <1171953086.6481860.1545188417030.ref@mail.yahoo.com>
DKIM-Signature:                   v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1545188429;
                                  bh=CSHo8zPLCMGq1gpi6JmxTfR5NrSY4XlWUxzt+Nl6njU=; h=Date:From:To:Subject:References:From:Subject;
                                  b=pPhE91fxvy6H/R88NCbmyh7lY0pKIRXUNxJumyVIX1M0fj5QLltMltQXe1gEUlRRgYHgYRWStg0lq1IACwyg05UDb3DGPdpJc
X-Forefront-Antispam-Report:      CIP:74.6.130.43;IPV:NLI;CTRY:US;EFV:NLI;SFV:SFE;SFS:;DIR:INB;SFP:;SCL:-1;SRVR:BN7PR17MB2372;H:NAM01-SN1-
                                  obe.outbound.protection.outlook.com;FPR::SPF:None;LANG:en;
Content-Type:                     multipart/mixed; boundary="----=_Part_6481859_71441314.1545188417030"
Subject:                          Th s is a test
```

When admin click on the email attachment "Malicious Demo Malware.xlsm" from the screenshot on the previous page, they are taken to another window showing the attachment profile.



Attachment profile

Attachment info

Malicious Demo Malware.xlsm Internal
33.4 Kilobytes
Attached to This is a test
Email sent at Wed, 19 Dec 2018 03:00:17 GMT
Email received at Wed, 19 Dec 2018 03:00:29 GMT

Email recipients

TYPE	USER	FOLDER	READ
From	don byrne donbyrne@yahoo.com		
To	Don Byrne donb@donsavanan.com		

Security Stack

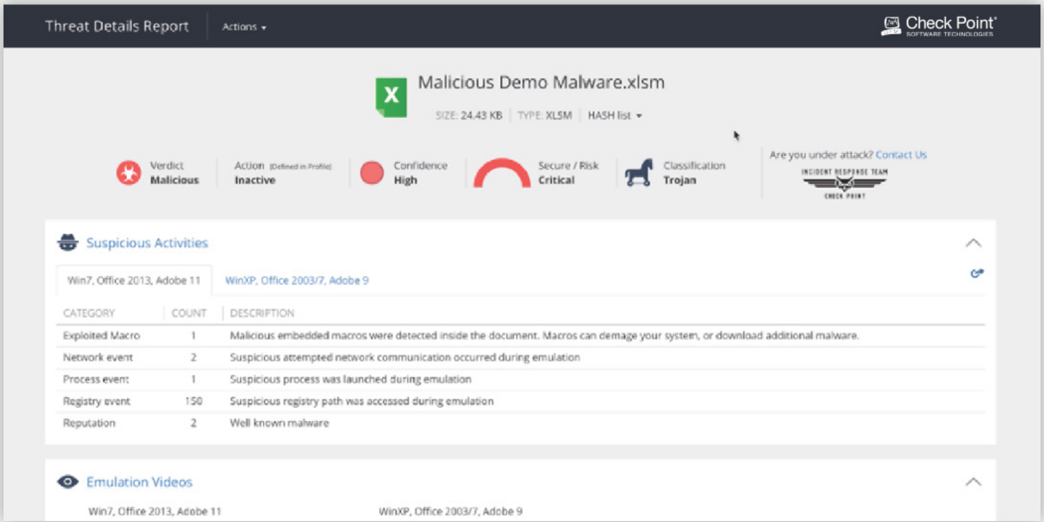
Malware Sandboxing

3. Email Security: Post-Attack

3.3. Forensic Tools

Check Point Harmony Email & Collaboration

The screenshot below displays what admin would see after clicking Check Point's Malware Sandboxing report shown in the previous page. This threat report is not segregated into the Reporting page on the main dashboard, as it would be in the ATP Security & Compliance platform. Admin can see helpful insights, such as the algorithm's verdict, risk level of the attack, and malware activities. The admin can study threat details, view quick summaries, and observe how the malware affects different operating systems.


Threat Details Report
Actions ▾
Check Point SOFTWARE TECHNOLOGIES
INCIDENT RESPONSE TEAM CHECK POINT

Malicious Demo Malware.xlsm

SIZE: 24.43 KB | TYPE: XLSM | HASH list ▾

Verdict Malicious | Action (Defined in Profile) Inactive | Confidence High | Secure / Risk Critical | Classification Trojan

Are you under attack? Contact Us

Suspicious Activities

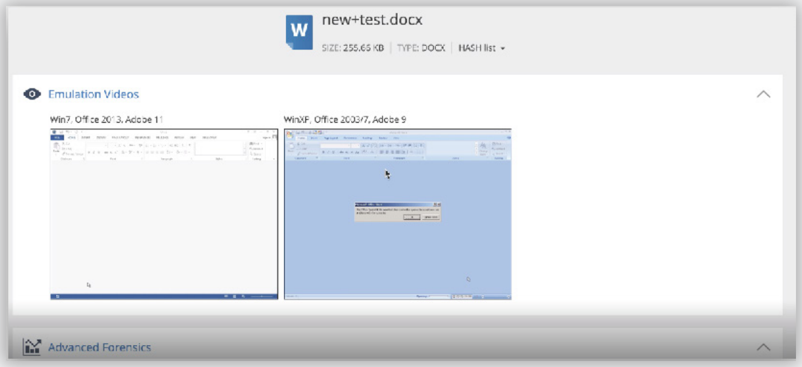
Win7, Office 2013, Adobe 11 | WinXP, Office 2003/7, Adobe 9

CATEGORY	COUNT	DESCRIPTION
Exploited Macro	1	Malicious embedded macros were detected inside the document. Macros can demage your system, or download additional malware.
Network event	2	Suspicious attempted network communication occurred during emulation
Process event	1	Suspicious process was launched during emulation
Registry event	150	Suspicious registry path was accessed during emulation
Reputation	2	Well known malware

Emulation Videos

Win7, Office 2013, Adobe 11 | WinXP, Office 2003/7, Adobe 9

But this is the most exciting feature: admin can watch a threat emulation video showing exactly what would happen if this file were opened.



new+test.docx

SIZE: 255.65 KB | TYPE: DOCX | HASH list ▾

Emulation Videos

Win7, Office 2013, Adobe 11 | WinXP, Office 2003/7, Adobe 9

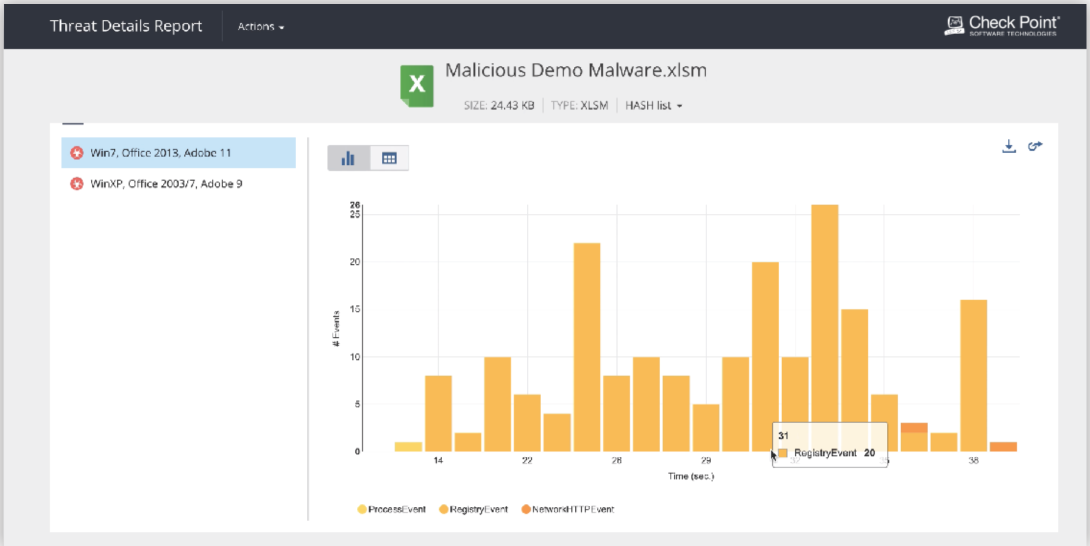
Advanced Forensics

3. Email Security: Post-Attack

3.3. Forensic Tools

Check Point Harmony Email & Collaboration

With Check Point Harmony Email & Collaboration's advanced forensics feature, admin can see a timeline showing the steps malware took as it detonated in the sandbox. This exportable visualization of advanced malware forensics comes in the form of a bar chart, with insight into process, registry, and Network/HTTP Events.



Malicious Demo Malware.xlsm

SIZE: 24.43 KB | TYPE: XLSM | HASH list ▾

Because Check Point Harmony Email & Collaboration sees so much detail into threats, admin can, too. Check Point Harmony Email & Collaboration was designed with the admin inmind so that clicking into report details flows and feels intuitive, presenting the right information and theright time.

3. Email Security: Post-Attack

3.4. Policy Configuration

Microsoft ATP

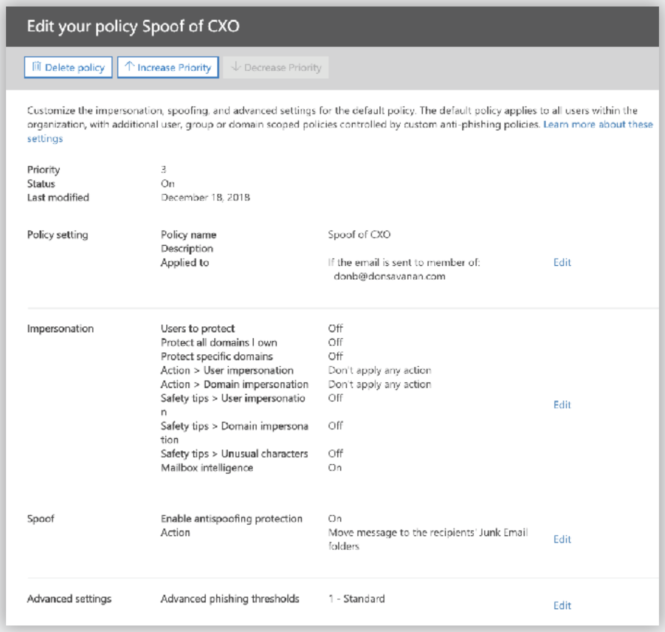
ATP policy configuration takes place within the Security & Compliance platform. Policy engines include anti-phishing, anti-spam, anti-malware, attachment scanning, link scanning, and DKIM. To create an anti-phishing policy in ATP, the admin must outline the conditional logic that dictates the engine's response when it is confronted with attacks. Overall, policy configuration in ATP is cumbersome and limited in the flexibility of its workflows, scope, and enforcement.

Spoof Policy

Rather than having the policy creation occupy a single window,ATP breaks the policy creation process down into "Policy setting," "Impersonation," "Spoof," and "Advanced Settings." Admin have to "Edit" each setting, navigating between windows to create the policy.

There are a few options that make up the Impersonation policy section.

- **Add users to protect:** This allows up to 60 addresses to be specified for protection, an immediate limitation of their protection. (Check Point Harmony Email & Collaboration can apply its policies to an unlimited number of users)
- **Actions:** This describes how the impersonation policy will trigger workflows in your Office 365 environment. Near the bottom of this section is the option to "Turn on impersonation safety tips," which add security warnings within emails for end users in the event that a user or domain might be impersonated.
- **Add trusted senders and domains:** This allows users and domains to be exempted from the impersonation policy. Admin should know that in ATP, it isn't possible to whitelist sender addresses, only recipient addresses. To get around this, admin must write a transport rule that adds a message header to bypass ATP scans. This will cause a 2- 3 minute delay. (Still, allowing permanent exemptions from policies is generally not a best practice.)
- **Adjust the aggression threshold of the policy:** Admin must recognize that with ATP, the more aggressive the policy, the more false positives.



Edit your policy Spoof of CXO

Customize the impersonation, spoofing, and advanced settings for the default policy. The default policy applies to all users within the organization, with additional user, group or domain scoped policies controlled by custom anti-phishing policies. Learn more about these settings

Priority	3		
Status	On		
Last modified	December 18, 2018		
Policy setting	Policy name	Spoof of CXO	
	Description		
	Applied to	If the email is sent to member of: donb@donsavanan.com	Edit
Impersonation	Users to protect	Off	
	Protect all domains I own	Off	
	Protect specific domains	Off	
	Action > User impersonation	Don't apply any action	
	Action > Domain impersonation	Don't apply any action	
	Safety tips > User impersonation	Off	Edit
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	On	
Spoof	Enable antispoofing protection	On	
	Action	Move message to the recipients' Junk Email folders	Edit
Advanced settings	Advanced phishing thresholds	1 - Standard	Edit

3. Email Security: Post-Attack

3.4. Policy Configuration

Microsoft ATP

Safe Attachments Policy

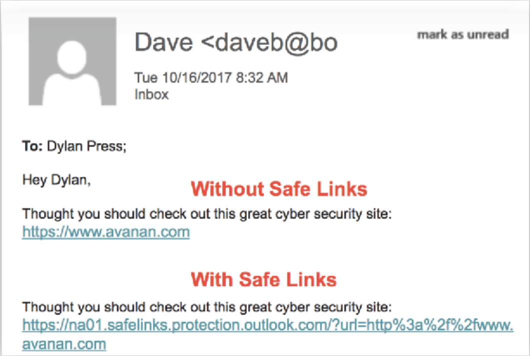
Configuring a Safe Attachments policy has similar limitations. Here are the modes in which the policy can run.

- **Monitor mode:** continues delivery after malware is detected and keeps a record of scan results.
- **Block mode:** stops emails and attachments containing malware.
- **Replace mode:** blocks attachments in which malware was detected, but delivers the rest of the message.
- **Dynamic delivery mode:** immediately removes attachments on all messages until the scan is complete, whereafter the attachment is reattached.

Safe Links Policy

Upon activating the policy,ATP will perform a link reputation check, and Safe Links will rewrite the URL. URLs identified as malicious in Office 365 reputation checks will be marked as spam, and the user will be unable to click them.

The Safe Links feature is counterintuitive to security best practices, however. Safe Links makes it harder to identify the clues users would use to identify a dangerous email, such as a misspelling. In "Fighting Phishing—2020 Foresight," Gartner stresses that "Phishing education needs to account for URL rewriting, as it should not be treated as giving license to click on anything."[16]



Dave <daveb@bo
Tue 10/16/2017 8:32 AM
Inbox

To: Dylan Press;

Hey Dylan,

Thought you should check out this great cyber security site:
https://www.avanan.com

Thought you should check out this great cyber security site:
https://na01.safelinks.protection.outlook.com/?url=http%3a%2f%2fwww.avanan.com

A comparison of the original URL to the Safe Links rewritten URL shows that the original is buried underneath Microsoft information.[17]

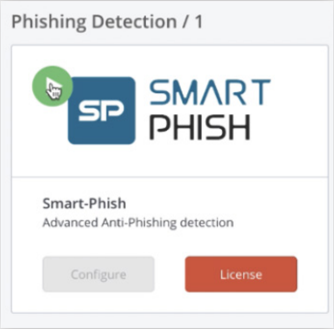
In this way, Safe Links is actually detrimental to anti-phishing education, because it gives users a false sense of security. If Microsoft has cleared the link, then there is no need to parse the URL for suspicious spelling that might indicate an unsafe domain.

3. Email Security: Post-Attack

3.4. Policy Configuration

Check Point Harmony Email & Collaboration

To simplify the configuration of security policies, Check Point Harmony Email & Collaboration SmartPhish AI has a one-click deployment for anti-phishing.This is as out-of-box as a policy can get. SmartPhish detectsthe threats targeting ATP's vulnerabilities, such as baseStrikerand ZeroFont, which ATP failed to identify as threats.



Phishing Detection / 1

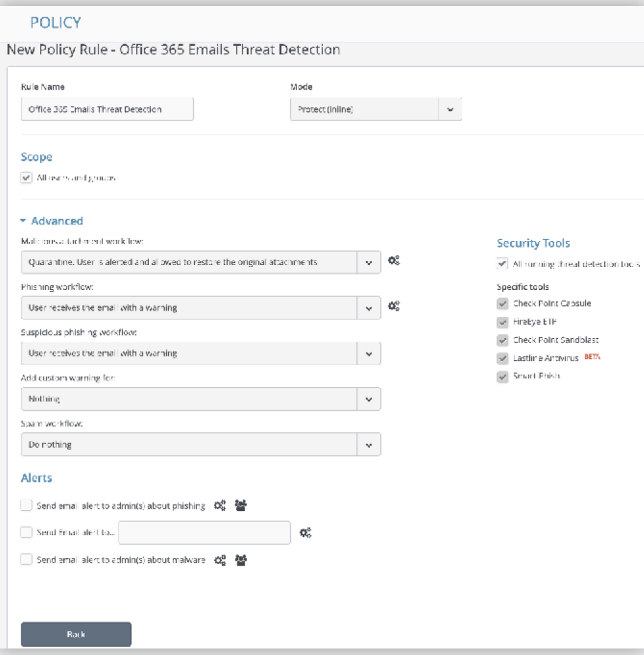
SP SMART PHISH

Smart-Phish
Advanced Anti-Phishing detection

Deploy an anti-phishing policy in a single click with Check Point's SmartPhish algorithm.

The custom policy wizard creates workflows to manage threats in Office 365, and runs in 3 possible modes:

- **Monitor Only:** Detects threats for the admin to remediate manually.
- **Detect and Prevent:** Scans messages when they land in the users' inboxes and automatically remediates.
- **Protect Inline (Recommended):** Blocks threats before they hit end users' inboxes.



POLICY

New Policy Rule - Office 365 Emails Threat Detection

Rule Name: Office 365 Emails Threat Detection

Mode: Protect (Inline)

Scope

☑ All users and groups

Advanced

Malicious attachment workflow: Quarantine. User is alerted and allowed to restore the original attachments

Phishing workflow: User receives the email with a warning

Suspicious phishing workflow: User receives the email with a warning

Add custom warning for: Nothing

Spam workflow: Do nothing

Security Tools

☑ All running threat detection tools

Specific tools

☑ Check Point Capsule
☑ FireEye ETP
☑ Check Point Sandblast
☑ Lastline Antivirus BETA
☑ Smart Phish

Alerts

☐ Send email alert to admin(s) about phishing
☐ Send Email alert to...
☐ Send email alert to admin(s) about malware

The custom policy wizard creates workflows to manage threats in Office 365.

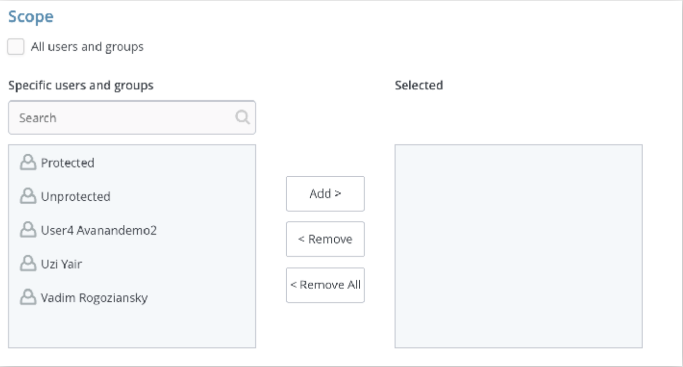
3. Email Security: Post-Attack

3.4. Policy Configuration

Check Point Harmony Email & Collaboration

With Check Point Harmony Email & Collaboration, custom policies apply to all users, and selecting those users is much simpler than in ATP.

How to apply the scope of your policy in Check Point Harmony Email & Collaboration.



Scope

☐ All users and groups

Specific users and groups

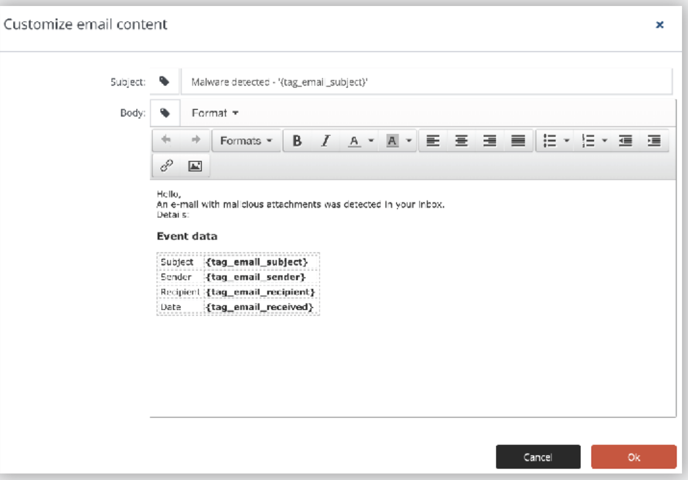
Search

- Protected
- Unprotected
- User4 Avanandemo2
- Uzi Yair
- Vadim Rogoziansky

Selected

Flexible workflows involve users and admins in the security process with detailed email workflows that alert them to potential threats:

- Send email alert to admin(s) about phishing (or malware).
- Send Email alert to...[specific person(s)].
- Alert recipient. This last one is very useful for keeping users in the loop about threats facing their inboxes.



Customize email content

Subject: Malware detected - '{tag_email_subject}'

Body:

Hello,
An e-mail with malicious attachments was detected in your inbox.
Details:

Event data

Subject	**{tag_email_subject}**
Sender	**{tag_email_sender}**
Recipient	**{tag_email_recipient}**
Date	**{tag_email_received}**

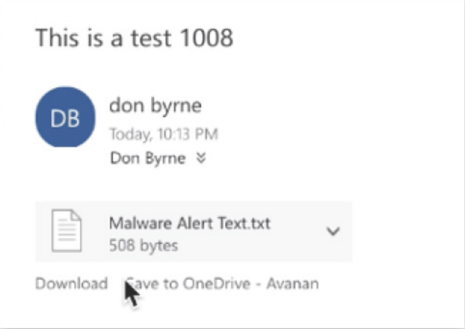
3. Email Security: Post-Attack

3.5. Workflows and Automation: Working with End Users

Microsoft ATP

Reporting

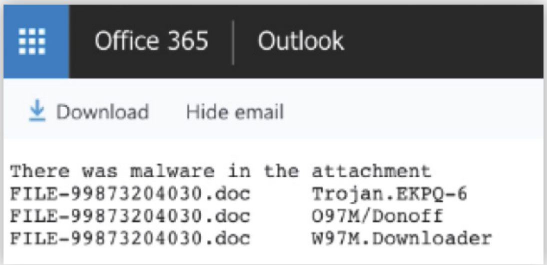
With ATP, the end user experience can be disruptive. If an end user receives a phishing document with a malware trojan, Microsoft will send an alert to them in the form of a .txt attachment. There are no actions for the user to take, other than opening the alert. They can't request to release the quarantined document.



This is a test 1008

don byrne
Today, 10:13 PM
Don Byrne

Malware Alert Text.txt
508 bytes



```
There was malware in the attachment
FILE-99873204030.doc     Trojan.EKPQ-6
FILE-99873204030.doc     097M/Donoff
FILE-99873204030.doc     W97M.Downloader
```

When the user opens the alert to learn more, they are greeted with this unfriendly, 4-line text summary that really just tells them there's trojan malware.

Reporting rates of phishing campaigns

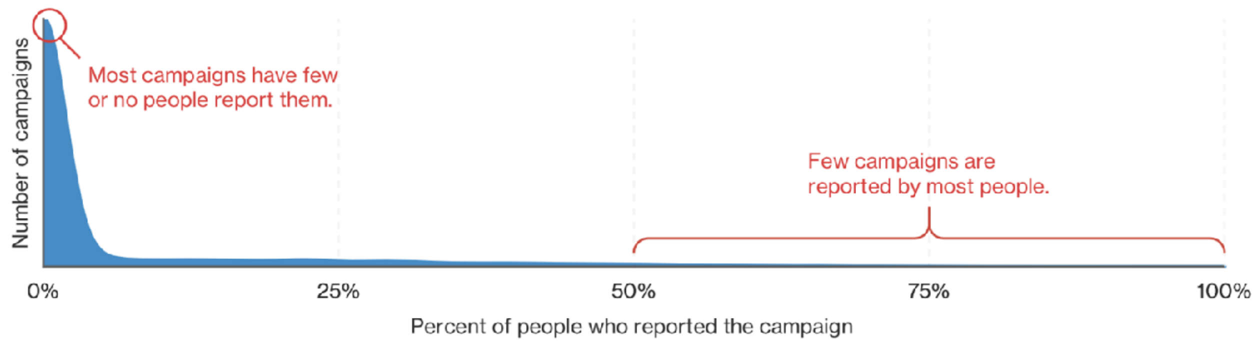


Figure 14. Reporting rates of phishing campaigns (n=9,697)

Only 17% of phishing campaigns were reported. Reducing the amount of time to detect and ultimately respond to phishing attacks is another key component in your defense.[18]

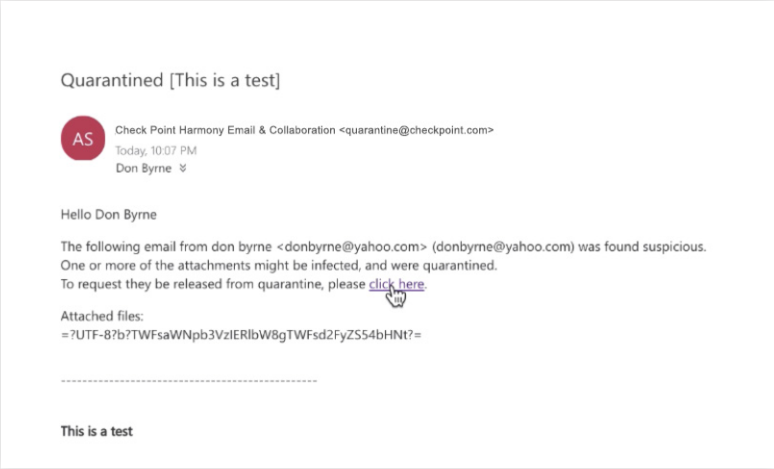
3. Email Security: Post-Attack

3.5. Workflows and Automation: Working with End Users

Check Point Harmony Email & Collaboration

Reporting

Avavnan describes the situation to the end user and provides a link to request document removal from quarantine.



Quarantined [This is a test]

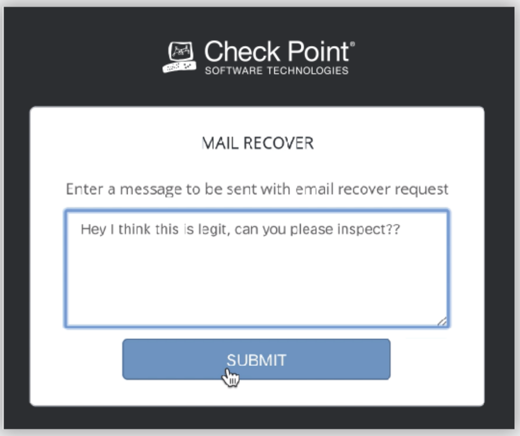
Check Point Harmony Email & Collaboration <quarantine@checkpoint.com>
Today, 10:07 PM
Don Byrne

Hello Don Byrne

The following email from don byrne <donbyrne@yahoo.com> (donbyrne@yahoo.com) was found suspicious.
One or more of the attachments might be infected, and were quarantined.
To request they be released from quarantine, please click here.

Attached files:
=?UTF-8?b?TWFsaWNpb3VzIERlbW8gTWFsd2FyZS54bHNt?=

This is a test



MAIL RECOVER

Enter a message to be sent with email recover request

Hey I think this is legit, can you please inspect??

End users can message admin to report amisclassification and ask that a quarantined document be released after a review.

3. Email Security: Post-Attack

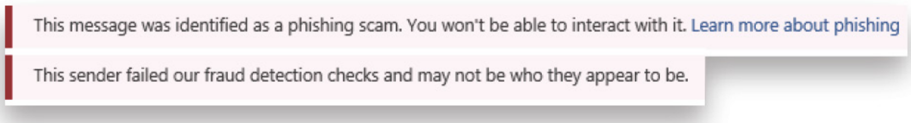
3.5. Workflows and Automation: Working with End Users

Microsoft ATP

Email-native education opportunities

ATP provides end users with safety tips. Four different colors mark the safety of the message content.

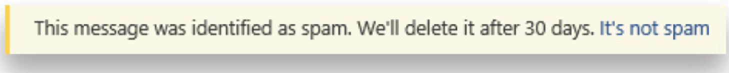
Suspicious Mail (Red)



This message was identified as a phishing scam. You won't be able to interact with it. Learn more about phishing

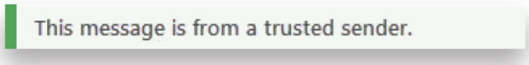
This sender failed our fraud detection checks and may not be who they appear to be.

Spam (Yellow)



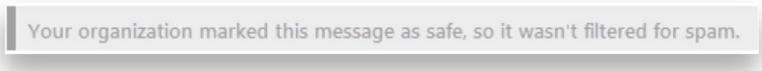
This message was identified as spam. We'll delete it after 30 days. It's not spam

Safe (Green)



This message is from a trusted sender.

Unfiltered (Grey)



Your organization marked this message as safe, so it wasn't filtered for spam.

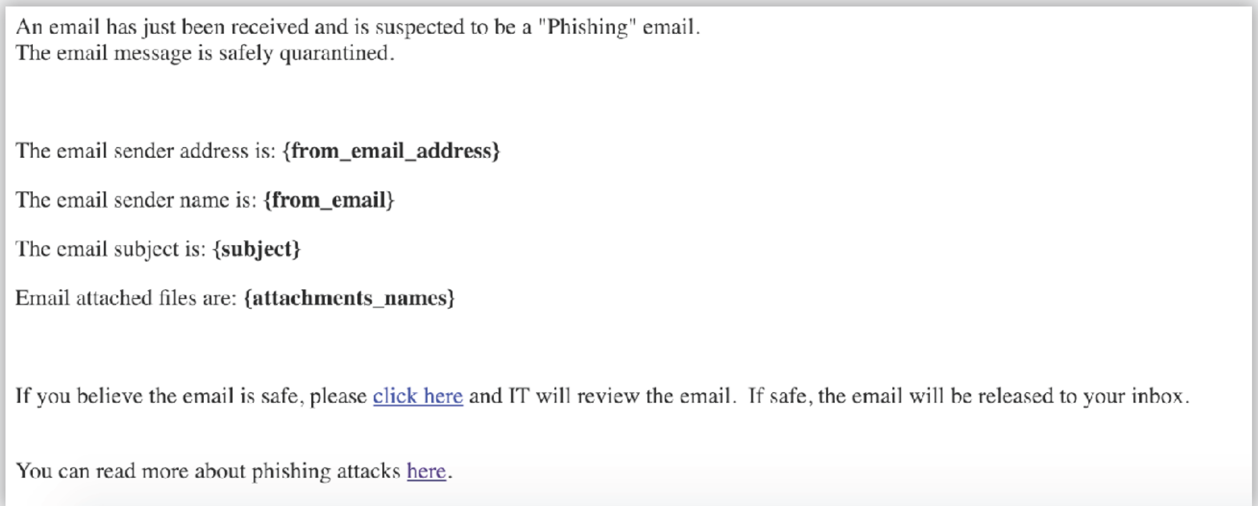
3. Email Security: Post-Attack

3.5. Workflows and Automation: Working with End Users

Check Point Harmony Email & Collaboration

Email-native education opportunities

Check Point Harmony Email & Collaboration recognizes that user education about phishing is integral to preventing attacks at your organization. Automated emails alert end users to threats, provide key details into the malicious message, and provide a link to further reading about phishing attacks.



An email has just been received and is suspected to be a "Phishing" email.
The email message is safely quarantined.

The email sender address is: **{from_email_address}**

The email sender name is: **{from_email}**

The email subject is: **{subject}**

Email attached files are: **{attachments_names}**

If you believe the email is safe, please click here and IT will review the email. If safe, the email will be released to your inbox.

You can read more about phishing attacks here.

End users can educate themselves about phishing by clicking on the link at the bottom of automated alert emails.

Conclusion

The threat landscape demands that email security has to do more than ever before, and that requires looking at email from a new perspective. This perspective must consider how the widespread use of Office 365 makes it a lucrative target for every hacker in the world. The default security of the service is inadequate, as indicated by Microsoft's strong push on its customers to add the ATP package to their plan.

Microsoft ATP suffers from some of the same fundamental problems that the Office 365 basic package has:

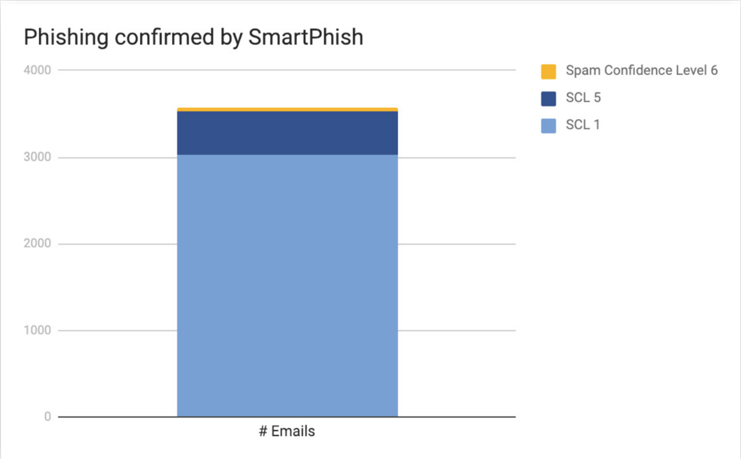
1. It is available for hackers to trial and error until they manage to bypass it.
2. It uses a lot of shared code with Office 365's default security, so a vulnerability in the basic package exists in both.

Malware authors write their scripts specifically for Office 365 EOP and ATP clients due to the widespread adoption of Microsoft's productivity tools and security solutions. Because Microsoft products and security are so simple to acquire, study, target, and manipulate, EOP and ATP are simply inadequate for enterprises whose goal is to be phish-free. This doesn't mean that Office 365 as a business tool is fundamentally insecure; it merely means that Office 365 is popular with enterprises, its architecture is highly visible,and it gets constant attention from hackers.

Password managers and 2FA can stop many phishing attacks, as researchers have found time and time again[19], but this simply isn't enough to protect even the most security-conscious users from email-borne threats. User education and password protection are worthy efforts, but they fall short if users cannot get context on or report suspicious emails.

Check Point Harmony Email & Collaboration knows this, and has created a security solution that puts users and admin first. Advanced user behavior analytics assess and remember the communication patterns of every user, from entry-level to C-suite, Check Point Harmony Email & Collaboration gives users the chance to report misclassifications, request restores of quarantined content, and provides key details about why certain content has been blocked from their inbox with automated alerts.

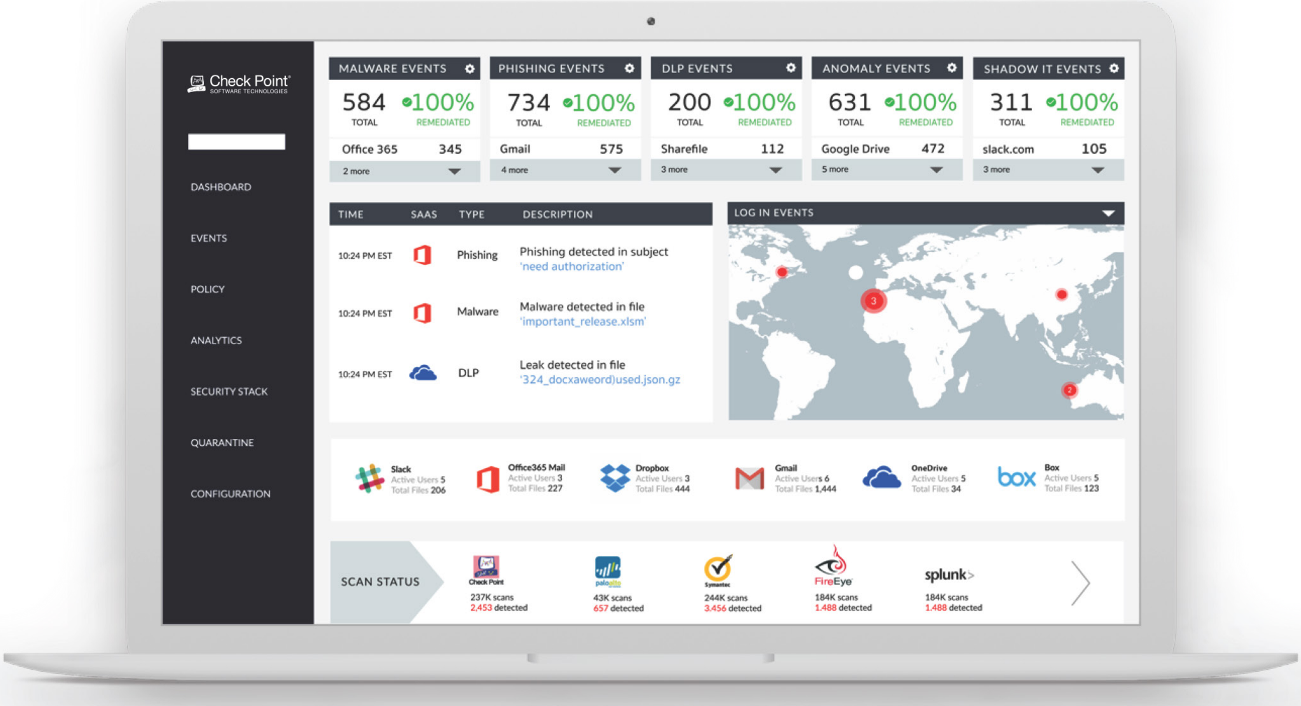
With the most customized machine learning on the market, Check Point Harmony Email & Collaboration secures beyond the Office 365 environment, covering collaborative chat and business apps (like Slack and Box) connected to email accounts,working seamlessly with 2FA, and identifying threats that ATP and EOP fail to block on user inboxes. Check Point Harmony Email & Collaboration supports defense in depth with best of breed security providers. These features combine to actively promote a culture of security in the workplace with easy threat reporting features and educational opportunities for users.



Works Cited

1. Firstbrook, Peter. "Market Guide for Secure Email Gateways," Gartner, 3 May, 2017, https://www.gartner.com/en/documents/3698932/market-guide-for-secure-email-gateways
2. Wynne, Neil. "Fighting Phishing—2020 Foresight," Gartner, 19 July, 2018, https://www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight
3. Widup, Suzanne."Data Breach Investigation Report." Verizon Enterprise, 27 Feb, 2018, enterprise.verizon.com/resources/reports/dbir/. (13)
4. Thomas, Kurt, et al. "Data Breaches, Phishing, or Malware?" Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS'17, 2017, doi:10.1145/3133956.3134067. (1)
5. Wynne, Neil. "Fighting Phishing—2020 Foresight," Gartner, 19 July, 2018, https://www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight
6. Nathaniel, Yoav. "BaseStriker: Office 365 Security Fails To Secure 100 Million Email Users." Avanan, 8 May 2018, www.avanan.com/resources/basestriker-vulnerability-office-365.
7. Nathaniel, Yoav. ZeroFont Phishing: Manipulating Font Size to Get Past Office 365 Security. Avanan, 13 June 2018, www.avanan.com/resources/zerofont-phishing-attack.
8. Nathaniel, Yoav. Z-WASP Vulnerability Used to Phish Office 365 and ATP. Avanan, 9 Jan, 2019, www.avanan.com/resources/zwasp-microsoft-office-365-phishing-vulnerability.
9. Vangel, Denise. "Set up Office 365 ATP Anti-Phishing Policies." Microsoft Docs, 10 Oct, 2018, docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies.
10. Wynne, Neil. "Fighting Phishing—2020 Foresight," Gartner, 19 July, 2018, https://www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight
11. Kerner, Sean Michael. "Avanan Boosts SaaS Application Security With Cloud-Native Approach." | TAKEitGAME - News Feed, www.takeitgame.com/link/191232_avanan-boosts-saas-application-security-with-cloud-native-approach.
12. Landewe, Michael. Capital Caring: Avanan Cloud Security for Healthcare. Avanan, 6 Mar, 2018, www.avanan.com/resources/capital-caring-secures-healthcare-avanan.
13. "Check Point SandBlast Receives Highest Security Effectiveness and Lowest TCO Scores in NSSLabs' First-Ever Breach Prevention System Test." Check Point Software, 21 Dec, 2017, www.checkpoint.com/press/2017/check-point-sandblast-receives-highest-security-effectiveness-lowest-tco-scores-nss-labs- first-ever-breach-prevention-system-test.
14. Wynne, Neil. "Fighting Phishing—2020 Foresight," Gartner, 19 July, 2018, https://www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight
15. Xu, Simon. "Responding to a Compromised Email Account in Office 365." Microsoft Docs, 27 Sept, 2018, docs.microsoft.com/en-us/office365/securitycompliance/responding-to-a-compromised-email-account.
16. Wynne, Neil. "Fighting Phishing—2020 Foresight," Gartner, 19 July, 2018, https://www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight
17. Press,Dylan. "4 Reasons Microsoft 'Safe Links' Make Office 365 Less Safe." Cloud Security Platform for Every SaaS, 19 Oct, 2017, www.avanan.com/resources/microsoft-atp-safe-links.
18. Widup, Suzanne."Data Breach Investigation Report." Verizon Enterprise, 27 Feb, 2018, enterprise.verizon.com/resources/reports/dbir/. (13)
19. Thomas, Kurt, et al. "Data Breaches, Phishing, or Malware?" Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS'17, 2017, doi:10.1145/3133956.3134067. (13)
20. Guida, Reece. ATP Anti-Phishing Compared to Avanan. Avanan, 20 Dec, 2018, www.avanan.com/resources/atp-anti-phishing-compared-to-avanan.

Harmony
Email & Collaboration



MALWARE EVENTS	PHISHING EVENTS	DLP EVENTS	ANOMALY EVENTS	SHADOW IT EVENTS
584 TOTAL	734 TOTAL	200 TOTAL	631 TOTAL	311 TOTAL
100% REMEDIATED	100% REMEDIATED	100% REMEDIATED	100% REMEDIATED	100% REMEDIATED
Office 365 345	Gmail 575	Sharefile 112	Google Drive 472	slack.com 105
2 more	4 more	3 more	5 more	3 more

TIME	SAAS	TYPE	DESCRIPTION
10:24 PM EST		Phishing	Phishing detected in subject 'need authorization'
10:24 PM EST		Malware	Malware detected in file 'important_release.xlsm'
10:24 PM EST		DLP	Leak detected in file '324_docxaweord)used.json.gz

LOG IN EVENTS

Slack Active Users 5 Total Files 206
Office365 Mail Active Users 3 Total Files 227
Dropbox Active Users 3 Total Files 444
Gmail Active Users 6 Total Files 1,444
OneDrive Active Users 5 Total Files 34
Box Active Users 5 Total Files 123

SCAN STATUS

Check Point	paloalto	Symantec	FireEye	splunk>
237K scans	43K scans	244K scans	184K scans	184K scans
2,453 detected	657 detected	3.456 detected	1.488 detected	1.488 detected

Check Point®
SOFTWARE TECHNOLOGIES LTD

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