Battle Card – Harmony Email & Collaboration

OVERVIEW

Due to Covid-19, organizations have been forced to greatly expand remote working capabilities. As such, cloud email and collaboration apps have become the most fundamental tools for businesses. According to the Verizon Data Breach Investigation Report, phishing is the #1 threat resulting in breaches - 91% of breaches start with email, 94% of malware was delivered via email.

Harmony Email & Collaboration combines the power of Check Point Sandblast with the world's most advanced anti-phishing engine to protect your users from all imminent threats to cloud and on-premises mailboxes, as well as collaboration apps such as Teams, OneDrive, SharePoint and Google Drive. On top of providing the best security, Harmony Email & Collaboration offers operational simplicity with an easy to deploy, manage and use platform.

THE CHECK POINT ADVANTAGE

Harmony Email & Collaboration provides best protection for email and collaboration apps that is easy to manage**:**

- Complete protection for email & collaboration apps from all imminent threats in one platform
- Can be deployed **inline**, **blocking** the threat **before** it reaches the inbox, running **after and in addition to** all other security tools, providing unmatched defense-in-depth
- Easily configurable and simple to deploy & manage with intuitive user interface
- **Highest level of protection** with the industry's **best catch rate** for phishing and malware and #1 in Fall 2021 G2 Grid Report and Omdia Inbound Email Security
- Powered by ThreatCloud and SmartPhish, the world's most powerful threat intelligence databases, and 300+ advanced AI engines

MARKET LANDSCAPE

Harmony Email & Collaboration falls within the email security market.

The market is very mature with over 30 vendors operating in it.

The biggest trend in the market is migration to cloud email services.

According to a comprehensive research report by Market Research Future (MRFR), the market is speculated to cross the overall value of 6.8 billion USD with CAGR of 16.2 by Forecast 2025.

Top 3 vendors that dominate the market are Proofpoint, Microsoft and Mimecast.

Need more info? Contact Threat_Prevention_Sales@checkpoint.com

ELEVATOR PITCH – TOP 3 SELLING POINTS

Harmony Email & Collaboration is the only security solution that:

- Provides **complete protection** for both email & collaboration apps from **all imminent threats** in a single solution
- Can be deployed **inline**, **blocking** the threat **before** it reaches the inbox, running **after and in addition to** all other security tools
- **Highest level of protection** with the industry's **best catch rate** for phishing and malware. See how many threats would be missed by the competitor with the Threat Miss Calculator.

SALES RESOURCES

- Internal Resources
- Public Resources
- Partner Resources

Product Information available includes:

- Customer Presentation
- Product Page
- Solution Brief
- And More

Harmony
Email & Collaboration

CHECK POINT Battle Card – Harmony Email & Collaboration vs Solutions

General Feature Matrix	Harmony E&C	Defender For Office	Secure Email Gateway	API
Simple deployment	●	●	◎	●
Single interface for threat management	●	●	◎	◎
Breach detection – mailbox-level anomaly detection [2]	●	●	◎	◐
Post-delivery protection – automatic remediation of threats that hit user inbox	●	◎	◐ 1	●
Shadow IT visibility	●	◐ 4	◎	◎
Historical scanning	●	◎	◎	●
In-line scanning after native security	●	◎	◎	◎
DLP with OCR	●	◎	◎	◎
Secures Slack	●	◎	◎	◎
One-click mass quarantine (Mail Explorer) [3]	●	◎	◎	●

1. Additional cost
2. Uses behavioral analysis to determine suspicious activity
3. Simple way to mass quarantine phishing emails already in the inbox
4. Only as part of standalone CASB, separate product

The Harmony Advantage

Harmony

- **Complete protection** for email & collaboration apps from all imminent threats in one platform
- **Ranked #1** in the most recent **G2 Grid Report** and Omdia's Fundamentals of Inbound Email Security
- **Easily configurable** and based on native cloud email APIs with no MX record changes
- **Highest level of protection** with the industry's **best catch rate** for **phishing** and **malware.** See how many threats the competitors miss with the **Threat Miss Calculator**.
- **Powered by SmartPhish** (AI-enabled anti-phishing engine), **ThreatCloud** and **Sandblast** (#1 ATP)
- Combined with **Harmony Connect (SASE)**, provides the only **complete solution for remote workers**

How to Compete Against...

Microsoft

A. **Complex to configure –** Microsoft defender require to configure **five different policies** each located in a different section which cause confusion when the administrator is unable to see a unified view of all his policies, it **can cause conflicts and security breach.**
B. **Defender For office One of the most targeted products and has low rate of detecting sophisticated spoofing attacks (https://www.avanan.com/compare)**
C. **According to Avanan's** recent **Global Phish Report, 25% of phishing emails bypassed** Office 365's native security (https://www.avanan.com/global-phish-report)
D. **Many attacks are crafted to bypass Defender For office** because it's **widely used** and **easily available** to hackers – see example of **malformed URL bypass** HERE
E. **Defender for office doesn't provide Shadow IT visibility, or one-click mass quarantine options**

API vendors

GreatHorn
Abnormal

A. **API** solutions **retract threats after delivery,** sometimes after as long as five minutes
B. **API** solutions are **not inline,** so they **can't prevent malware, prevent data leakage, or** wrap URLs for **click-time protection**
C. **API** solutions are **throttled,** depending on usage, making them **much less scalable**
D. **API** solutions **only protect email, not file sharing and collaboration apps**

Secure Email Gateways

proofpoint
mimecast

A. **By sending an email** to your **root domain address**, attacks can **bypass your gateway** and **reach the inbox** with SEGs
B. **SEGs are blind to internal emails** and thus will **miss internal threats, which make up 35% of attacks**
C. **SEGs have no internal context** for users so they **cannot effectively stop BEC attacks**
D. **SEGs can't protect the full suite** and require **add-ons** to protect **collaboration apps**

Public comparison for all features

Battle Card – Harmony Email & Collaboration vs Vendors

Comparison Matrix	Harmony	MS EOP	O 365 E3P2/E5	proofpoint Essentials	mimecast M2	Google G-mail Business
Advanced Phishing/Social Engineering (Extortion /Payments/Impersonation)					A,C	
Email Threat Protection – AV/Spam/Reputation						
Zero Day Protection – Sandboxing			D	A	B	B
Content Disarm & Reconstruction (Extraction)			B	B		
Email Link Rewriting (Click-time URL Protection)			B,F	1,F		
Email DLP	6		8		E	
Collaboration Apps (inc Slack/Citrix)	6,7	2	2	C	E	
Management & Reporting		D	C	5	5	
Deployment methods	9	3	3	D	D	A
Annual Price-list per user	$55	Inc w O365 G	G,4 $96/$180	$43	$48	$72

1. Links to files not analyzed
2. Part of Cloud App Security (separate product)
3. On-prem deployment provides limited security features
4. Plan 2 can only be purchased on top of Plan 1
5. Complex management requires training to understand
6. Available for additional cost
7. MS365 (SharePoint, OneDrive, Teams), G-suite, Box, DropBox, Slack, Citrix
8. Plan 1 doesn't include DLP, E3 includes partial DLP
9. MTA on roadmap (2022)

Competitive Benefits of Harmony

- **Complete protection** for email & collaboration apps from all imminent threats in one platform
- Patterned Inline protection including API Integration for incoming & internal emails Inspection
- **Ranked #1** in the most recent **G2 Grid Report** and Omdia's Fundamentals of Inbound Email Security
- **Can easily tap into existing infrastructure** with no MX record changes needed
- **Highest level of protection** with the industry's **best catch rate** for **phishing** and **malware.** See how many threats are missed by the competitors with the **Threat Miss Calculator**.
- **Powered by SmartPhish** (AI-enabled anti-phishing engine), **ThreatCloud** and **Sandblast** (#1 ATP)
- Combined with **Harmony Connect (SASE)**, provides the only **complete solution for remote workers**

How to Compete Against...

Microsoft

A. **Complex** Policy Controls**, Require five different policies and now unified view**
B. **Safe Links isn't enforced** within files or with Dynamic Delivery **& creates slowness** in access to legitimate sites
C. **Uses multiple** management Interfaces Which complicates the procedure of configuring and monitoring
D. **Sandboxing cannot** detect **advanced evasion techniques** like HE&C; HEC provides **industry-leading catch rate**
E. **Dynamic Delivery** only provides **preview of files,** but Harmony provides **permanent**, **risk-free document**
F. **limited forensics capabilities** on malicious verdict files which lead to **additional labor hours for forensics**
G. **EOP is included** with all Microsoft O365 packages**. Defender Plan 1 & 2 are add-ons**
H. **Safe Links** is vulnerable to **bypass by malformed URLs** – see HERE for full explanation

Google

A. **Full featured phishing protection, but inferior catch rate – see HERE**
B. **No sandbox for advanced malware analysis**
C. **No URL rewriting capability, only warning** when user clicks through **unknown external link**
D. **Lacks CDR capability,** users must wait to receive clean files
E. **No email DLP capability,** sensitive data in email is not protected
F. **Only protects native collaboration apps –** e.g. Google Drive
G. Business Email Compromise (BEC) phish are sent to recipient with warning banners, not blocked

proofpoint

A. **Sandbox not available in Essentials**, requires purchase of more **expensive package** for zero-day
B. **Lacks CDR capability**, users must wait to receive clean files
C. **Must** have a **separate solution** for **SaaS application protection** (CASB), which adds add'l cost and IT overhead
D. **Uses MTA** for O365 email protection, a **complex deployment** with MX record changes, single point of failure
E. **Deployment** includes **disabling MS security features**, such as spam filtering – **see here**
F. **Proofpoint's URL protection** is vulnerable to **bypass by malformed URLs** – see HERE for full explanation

mimecast

A. **Anti-phishing** protection is **missing dynamic analysis** of email contents; includes only **basic anomaly detection**
B. **Sandboxing cannot** detect **advanced evasion techniques**; Harmony provides **industry-leading catch rate**
C. **Social engineering protection** is limited to **impersonation detection** – based on **static dictionary match; no real-time analysis** like Harmony
D. **Deployment** for email protection is **complex via MTA only** and less secure due to single point of failure & includes **bypass of MS security features**
E. **No Threat Protection for collaboration apps** like SharePoint and Teams – only archiving and data protection

Battle Card – Harmony Email & Collaboration vs Vendors

Comparison Matrix	Harmony	Abnormal	Barracuda Advanced	FortiMail	Trend M Cloud App	Netskope
Advanced Phishing/Social Engineering (Extortion /Payments/Impersonation)	○	◔	◔ A,F	◔	◔	◎
Email Threat Protection – AV/Spam/Reputation	○	◔	○	◔	○	◔
Zero Day Protection – Sandboxing	○	◎	◔ B	◔	◔ G	◔ B
Content Disarm & Reconstruction (Extraction)	○	◎	◎ C	◔	◎	◎
Email Link Rewriting (Click-time URL Protection)	○	◔ C	○	◔	○	◎
Email DLP	○ 6	◎	◔	◔	○ C	○
Collaboration Apps (inc Slack/Citrix)	◔ 6,7	◎	Only for "Premium Plus"	◎	◔ 4	○
Management & Reporting	○	○	◔ E	◔	◔	○
Deployment methods	◔ 9	◔	◔ D	○	○	◔ A
Annual Price-list per user	$55	$36	$96	$36	$72	$96

1. Links to files not analyzed
2. Part of Cloud App Security (separate product)
3. On-prem deployment provides limited security features
4. Plan 2 can only be purchased on top of Plan 1
5. Complex management requires training to understand
6. Available for additional cost
7. MS365 (SharePoint, OneDrive, Teams), G-suite, Box, DropBox, Slack, Citrix
8. Plan 1 doesn't include DLP, E3 includes partial DLP
9. MTA on roadmap (2022)

Q2 2022

Competitive Benefits of Harmony

Harmony

- **Complete protection** for email & collaboration apps from all imminent threats in one platform
- Patterned Inline protection including API Integration for incoming & internal emails Inspection
- **Ranked #1** in the most recent **G2 Grid Report** and Omdia's Fundamentals of Inbound Email Security
- **Can easily tap into existing infrastructure** with no MX record changes needed
- **Highest level of protection** with the industry's **best catch rate** for **phishing** and **malware.** See how many threats are missed by the competitors with the **Threat Miss Calculator**.
- **Powered by SmartPhish** (AI-enabled anti-phishing engine), **ThreatCloud** and **Sandblast** (#1 ATP)
- Combined with **Harmony Connect (SASE)**, provides the only **complete solution for remote workers**

How to Compete Against…

Abnormal

- **A. No policy administration –** product policy is Configurable, any changes (including enforcement actions, exceptions and white-listing) require support cases.
- **B. Rely on Microsoft** to prevent known and unknown malicious, and flag only unusual emails without threat analysis
- **C. Protection after the fact** – detected Phishing emails are removed **after** reaching the inbox, since they use **API only approach**. Harmony supports **both API & inline approach**, allowing it to block the threat before it reaches the user
- **D. Lacking URL protection** – links to domains not appearing in the obsolete Alexa top 1M are rewritten, leading to a generic warning message about the site's reliability
- **E. Abnormal is a niche solution** – Only provides email and phishing protection. Harmony Email protects multiple applications with advanced security features such as DLP and sandbox protection against 0-day malware

Barracuda

- **A. Very low catch rate for phishing** compared to leading vendors – see HERE for full report
- **B. Sandboxing cannot** detect advanced evasion techniques like HE&C, which provides industry-leading catch rate
- **C. Lacks CDR capability,** users must wait to receive clean files
- **D. Uses MTA** for O365 email protection, **a complex deployment** with MX record changes, single point of failure
- **E. Limited reporting,** very basic reports with no customization possible
- **F. Language analysis** for phishing protection **only works for emails with 11 words or more** and **must be manually tuned** with 200 legitimate and 200 spam messages - see HERE

Trend Micro

- A. When phishing/spam email is blocked by Microsoft Exchange, it will not show up on Trend Micro console
- **B. Protection after the fact** – detected threats are removed **after** reaching the inbox, since they use **API only approach**. Harmony supports **both API & inline approach**, allowing it to block the threat before it reaches the user
- C. lacking rich data analysis, provide quarantine/spam/phishing verdict without which indicators flagged it.
- D. DLP is "Pre-release" It is not fully supported and require mail flow change to activate
- E. If deployed as a email GW mode, will be unable to inspect internal emails.
- **F. Sandboxing** Ability require additional license/"Advanced" license which increase TCO

Fortinet — Premium with Office365 API

- **A. Sandboxing** Ability require additional license which increase TCO
- B. Spam protection requires **continuously manually training databases to accurately detect Spam**
- C. focus only on good price rather than Security+
- D. Deployment is either MTA/MX, which is complex, or MS 365 API**, which provide prevention after the fact**

Netskope

- **A. Must deploy** an **Agent solution** for Inbound email inspection, leading to complex deployment
- **B. Sandboxing** is **basic** and supports **limited file types;** for more **advanced threats, 3rd-party sandbox** supported
- **C. Costly**, **must purchase expensive** Professional Services days for every bundled solution
- **D. CASB-focused** solution with **complex proxy configuration**, **forcing all traffic** through **single point of failure**