YOU DESERVE THE BEST SECURITY

ESSENTIAL GUIDE TO
EMAIL SECURITY

impelix™ in partnership with CHECK POINT™

Table of Contents

Executive Summary

Overview

Email remains the #1 cybersecurity threat vector in 2024 through various attack types like phishing and malware. Default email solutions from Microsoft and Google provide some security, but not enough. A huge industry has emerged offering additional email security solutions, but wading through the options can be difficult. This guide helps create a framework for evaluating email security vendors.

Key Features

- Must have AI and machine learning to detect latest threats
- Flexible deployment options - inline before inbox or post-delivery
- Malware protection through sandbox detonation
- Protection beyond just email to collaboration platforms

Analyst Input

- Harmony Email & Collaboration named a leader by all major analysts for its superior efficacy, ease of analysis, wide threat protection, rapid deployment, and strong company backing

Understanding AI Claims

- AI is essential for email security due to volume and velocity of threats
- The quality of AI comes down to: people building it, math/algorithms used, and quantity/quality of data
- Check Point has extensive real-world threat data and proven prevention rate with its AI

Company Backing

- Balance of leading technology and strong company backing is ideal
- Check Point has 30+ years securing threats and invests $350M annually in R&D

Deployment Options

- Harmony offers inline API-based, monitoring, and post-delivery options
- Flexibility to balance security and productivity for each organization

Conclusion

- Many capable email security vendors to choose from, but hard to evaluate
- This guide provides facts and insights to empower the best choice

In 2024, you need email security beyond the default. Why? Because email-based attacks remain the number one vector for cybersecurity attacks. From simple phishing to complex malware chains, email is the easiest and often most successful avenue for hackers to begin their scams.

That's not to say the rest of the cybersecurity ecosystem isn't important—it is. But if you're not protecting email, you're leaving your organization exposed.

When you purchase a corporate email solution—most likely Microsoft or Google—you receive default security. With Microsoft, for example, you can pay for higher tiers of security.

Regardless, though, these companies, while they do block attacks, simply do not block enough attacks. Hackers can easily create free Microsoft accounts and learn exactly what will get past its defenses. Microsoft, as well as Google, is the training ground.

It's why a huge industry has exploded in email security. There are over three dozen different companies offering email security. Every organization that has email—which is every organization in the world—would benefit from email security. It's a marketplace ripe for growth.

But as end-users and organizations, how can you make sense of the different options?
How do you know which email security solution is right for you?

In this Buyer's Guide to Email Security, we break down what it means to be an effective email security solution, by focusing on:

- **Key Features**
- **Analyst Input**
- **How to Wade through AI Marketing Speak**
- **Company Strength**
- **Deployment Options**

State of the Market

The email security market is in a bit of flux.

It pays to start with a history lesson. In the beginning, the majority of security was delivered on-prem via gateways. Your email server sat somewhere in a data center, protected by a security stack that was designed specifically for on-premises email.

This led to the proliferation of gateways, like Mimecast and Proofpoint. These were effective in the on-prem world. But then email moved to the cloud. And organizations found that securing email within a single, on-premises server is a world apart from securing cloud-based email, which is a part of a much larger suite of cloud applications. Many of the tools for data-center email security do not apply to cloud-based email. Rather than a point solution, cloud based email must be understood as part of a much larger whole.

That's why we decided to pioneer the API approach. We created a patented solution that connects automatically inline via API. We remain the only solution that is built specifically for cloud email, leverages the cloud email API and secures email before it gets to the end user.

We were able to quickly demonstrate the technology's value and scale. And so, others started to come in.

Gartner quickly called these solutions ICES—or integrated cloud email security solutions. (Forrester calls them CAPES—cloud-native API-enabled email security, but they are referring to the same thing.) These are all very similar to how we operate, but have one major difference. Because of our patent, they cannot prevent the email from reaching the inbox. They can only retract after it reaches the inbox. This can be nearly instantaneous, but often it is not, and the malicious email is in the inbox, just waiting to be clicked on.

Still, many of these email security companies are still in the market and more are coming all the time. And because of the inherent advantages of API-delivered security, all of the major gateway players have made acquisitions to implement this technology.

In 2020, Mimecast acquired MessageControl, and then implemented it into their CyberGraph platform. In 2022, Barracuda acquired ClearedIn. In 2023 we saw two major acquisitions—Cisco acquired Armorblox and Proofpoint acquired Tessian.

This is a clear indication that gateways know that an API approach is preferable, and attempts to get there on their own have been rocky. They are now trying to make the transition from gateway to API, a transition that's not so simple. This has led to understandable optimism from next-gen API players, including ourselves.

But it underscores an important truth. The vision we set out with in 2015 was the correct one, and the market continues to try to catch up.

Because so many of these solutions are so similar, and everything is coalescing around the API framework, it makes it incredible difficult for buyers to sort through the noise.

Key Features

Any email security solution needs to have a few features to be worth its salt.

- **AI-enabled.** If it's not using cutting-edge AI, it's not worth it. Utilizing machine learning and AI, particularly ones that are trained on the most sophisticated attacks, is crucial to preventing attacks
- **Flexibility in Deployment.** Every organization is different. Being able to deploy inline before the inbox or as a post-delivery layer is crucial. Even better? Being able to customize it for certain business groups depending on organizational need
- **Malware protection.** Being able to detonate all files in a sandbox and block the malicious ones is a key feature of email security that not all vendors have.
- **Full-Suite security.** The use of messaging and file-sharing apps are expanding and protections developed for the inbox need to extend to these platforms.

These are table stakes for email security. If you are evaluating a vendor and they don't have these, it's time to look elsewhere.

The whole idea of email security is that when an end-user sees an email hit their inbox, they know it's safe. Without these key protections, you're adding too much risk into the environment.

Analyst Input

Every analyst that has ever covered email security has named Harmony Email & Collaboration as a leader in the industry.

Read any analyst report and they all say essentially the same thing. Every analyst calls our inline API deployment unique and powerful, providing us the ability to protect against a wide variety of threats.

We are rated as leaders for the same reasons across the board. Whether it's Forrester touting our "superior efficacy"; Omdia praising our "notable analysis" around sophisticated BEC threats; Kuppinger Cole noting how our inline protection allows us to implement "a wide variety of analytical and protective measures against a variety of threats"; GigaOm highlighting our "rapid deployment"; or Frost & Sullivan calling out our inline security as a differentiator from "the other vendors in the market," as well as our "market-leading email security revenue growth rate percentages"; HEC has clearly established itself as the darling of analysts and customers alike.

How to Wade Through AI Marketing Speak

Every cybersecurity company says their AI is revolutionary.

As consumers, it's nearly impossible to understand what that means or why it makes your security better.

Let's start with this basic truth: It's impossible to provide email security without AI. There are just too many threats, at too high a velocity, for a human or a team of humans to keep up.

But, using a human example, we can break down how it works.

Let's say your company hired someone, and their sole job was to read everybody's email, in real-time, to determine whether an email was phishing or not. If an email was clean, they would let it go right into the inbox. If it were phishing, the email would be quarantined. Before this person starts their job, you would need to train them. First, you have to explain to them what to look for in a phishing email. To do this, you would take one million examples of phishing emails. You'd print them out and have the new hire review every single one. Then, you'd have them indicate why a particular email was phishing. Every email would have a different reason as to why it was declared phishing. In some emails, there would be clear phishing language in the body. In other emails, links would go to a newly registered domain. Some emails would come from individuals the company had never heard of before. In fact, there could be hundreds of reasons in every single email to indicate that it could be phishing.

After a period of time learning what to look for in a phishing email, you'd then test this person with real examples. If they did a better job of detecting phishing emails, with lower false positives, than what was in place beforehand, you'd turn your new "Real-Time Security Analyst" loose. Sometimes, this person would get something wrong. Then, through a feedback loop, you'd understand why and correct it going forward.

This is a fictional example—but it's essentially how AI and ML is used to identify and stop phishing attacks.

So all AI solutions are essentially doing the same thing. But not all AI are created equal. So what gives?

It all starts with data—quality and quantity. As IBM notes, ""Data is the fuel that powers artificial intelligence. Despite being critical to the AI equation, data often gets overlooked or minimized—often at enormous costs. It takes hard work to get data to the point where it's usable for AI, but ultimately it comes down to hitting two big checkboxes: quantity and quality."

The breadth and depth of data is crucial for training AI to be effective.

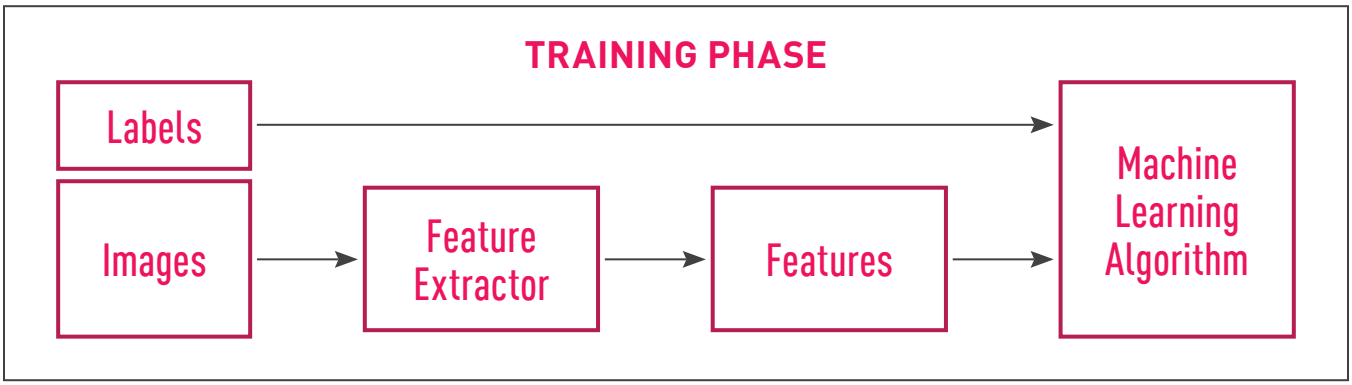
To create quality AI systems, you need three things:

1. **People**, to build it
2. **Math**, with the most tested algorithms
3. **Data**, and lots of it

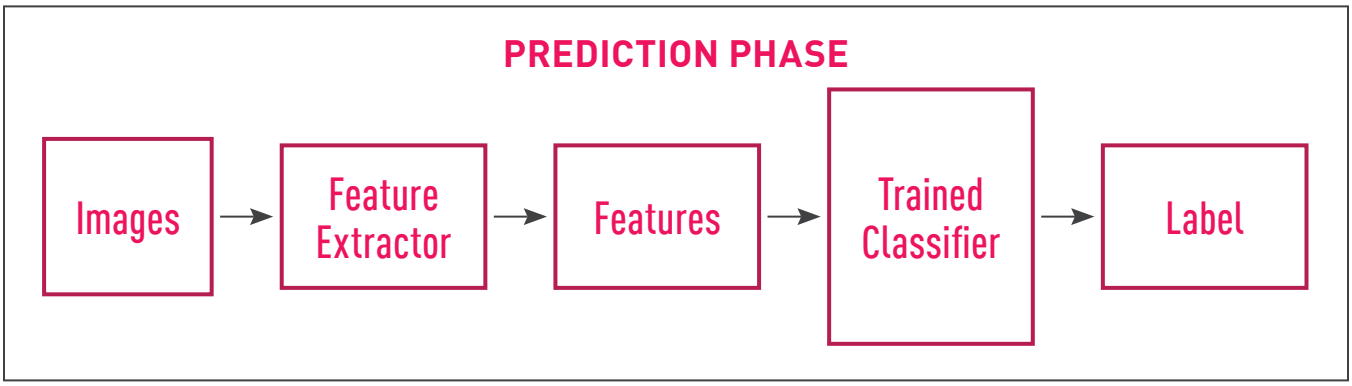
To achieve AI/ML representation in cyber intelligence we need to classify data and represent that data to the computer. Extracting features (attributes) for each data item are used to train the ML system.

If you are classifying fruit you have color, weight, and shape as features. The math will dictate which ML classifiers are best used. As we build the training data we use labels to define the truth, which the math/algorithm will learn.

In the fruit example, as we collect samples we extract our features and the labels and build the ML algorithm. This output is a function that has the logic from the collection input. This function is called a model.



Function has been created



Machine Learning Phases

There are two main types of Machine Learning

- **Supervised** – give the ML the data (labels) and desired output. This is to establish truth
- **Unsupervised** – we don't give labels and in cyber security we look for hidden structures or clusters—for example in malware families, we look for anomalies

These types of ML are the backbone features for any AI-based system.

And when it comes to three main items—people, math, and data—no one can beat Check Point.

PEOPLE Check Point has 30 years of experience in securing the evolving threat landscape; this history has driven our leadership up and down the organization to set the strongest cyber security vision that aligns with challenges. This includes our research team and data scientists that collect and analyze global cyber-attack data stored to train, test, and improve AI models.

MATH ThreatCloud AI and the over 40 AI engines can provide the best prevention.

- **Intelligence** – Machine-generated signatures, Anonymizer models, reputation, external sources
- **Static Analysis** – Executables, applications, documents, code, emails, classification
- **Dynamic Behavioral Analysis** – Dynamic executables, documents, applications
- **Correlation and Elimination Models** – Machine-based incident correlation, signatures, accuracy

DATA being a core component of AI—below is an illustration of how much data is counted daily

Big data threat intelligence:

2,000,000,000
Websites and files inspected

73,000,000
Full content emails

30,000,000
File emulations

20,000,000
Potential IoT devices

2,000,000
Malicious indicators

1,500,000
Newly installed mobile apps

1,000,000
Online web forms

Counted **Daily!**

The effectiveness of Check Point's ThreatCloud AI in preventing attacks is due to the vast amount of real-world data of threat and domain experts who develop, train and validate the models. Check Point has developed a proprietary labeling methodology that establishes a trustworthy ground truth. Additionally, a unique feature set, data enrichment, and integration of the algorithm approach result in the industry's leading prevention rate.

Here's the key. Everyone has AI, but in order to ensure you're getting the best security, you need to actually know what the AI is doing. Saying, "we have the best AI' is not enough. Indeed, as Forrester notes about email security vendors:

> "Most CAPES vendors rely heavily on the power of AI and machine learning to stop sophisticated phishing and BEC attempts by learning communication or individual employee behavioral patterns to spot anomalies and neutralize threats. But this capability is limited to several underlying factors, including the quality of the algorithm training data, cadence of algorithm retraining, and how anomalies detected by the algorithm combine with traditional alerts. If a potential vendor's answers about how their AI/ML works are vague or defensive, keep looking."

Curious about our AI? Just ask. We're happy to do an incredibly thorough deep dive. And be sure, as Forrester notes, to thoroughly investigate any vendor's AI—ours included. Here's some questions we recommend asking:

- How many AI and machine learning technologies are actively used to identify threats?
- Does your AI technology mainly focus on collecting and analyzing data from email or SaaS application threats?
- Is your AI technology updating in real-time?
- Do you have analysts monitoring AI decisions and what is their role?
- Does your email security solution use AI technologies to prevent threats before they reach the mailbox?
- Does your email security solution provide visibility on the AI decision making process and analysis?
- How does the AI interact with the CSI team?
- Does the AI disseminate new found threats across the entire global install base with immediacy?
- How does AI help if your users get to threats before your product does?

Experience vs Flash

Security is important, and when you partner with a vendor to provide security, you want to know that you're getting the best of the best.

There are so many companies, established and otherwise, delivering security solutions. It's hard to wade through the options to find the best option for your organization.

A good rule of thumb is understanding a vendor's backing. In other words, what's driving the company's success? Ideally, there's a balance between top-of-the-line tech with company strength.

Check Point has been at the top of security for three decades. HEC itself has over 20,000 customers, and is able to leverage the entirety of the Check Point solution to improve its capabilities. Check Point spends $350 million annually on R&D and is consistently investing in the efficacy of its security.

We've seen this in competitive deals. In one head-to-head against a buzzy startup, the customer noted that Check Point's presence in the cybersecurity space was a huge plus for them.

Startups are great. HEC began as a startup.

But experience is great, too. When you combine bleeding-edge technology with a strong company history and track record , you get a hard-to-beat combination.

Deployment Options

Most email security vendors offer one deployment method. Just gateway. Or just post-delivery remediation.

HEC is the only enterprise email security to vendor to provide an in-line API-based deployment option that works with both Microsoft and Google. This is HEC's patent.

But there's more. HEC can deploy in three modes. Monitor mode, which most customers use as part of their POCs. There's inline mode. And then detect-and-remediate, which identifies malicious emails after they reach the inbox, and removes them accordingly.

Every organization tries to balance security and productivity in different ways. Some want absolutely no delays in their email ever. Others want to ensure that every email that reaches the inbox is scanned and cleared, no matter the delay. Regardless of this balance, all organizations want to ensure that their company, people and data are protected in the best possible way. With our solution, you can easily find that delicate balance between security and productivity. Want to use our patented inline mode for everyone? Go for it. Prefer to use our detect-and-remediate mode for everyone? No problem. Want to use inline for some folks and detect-and-remediate for others? Can do it in a click. Want to change things after six months or six days? Easy.

Since every organization is unique, we want to provide organizations with the ability to create unique security.

And this is a unique feature of HEC's. In fact, in Forrester's most recent Wave, HEC was the only vendor to receive a "5"—the highest score—for deployment options.

Conclusion

It has never been more important to implement email security, and there has never been more email security vendors to choose from. Forrester calls this a "golden age" of email security, and we agree. The market is lucky to have dozens of vendors, all trying to constantly improve and innovate to bring the best possible security.

Having options as a consumer is great, but it can also make things difficult. Evaluating every single vendor is not practical, and knowing which vendor is just right for your organization can be a long process—especially when so many of the vendors are so similar.

This guide is designed to help you think through the decision to buy email security, and what should be prioritized.

In the end, every organization will make the best security decision for their business.
Being empowered with the facts and insights will help you make the best possible choice.

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
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

© 2024 Check Point Software Technologies Ltd. All rights reserved.