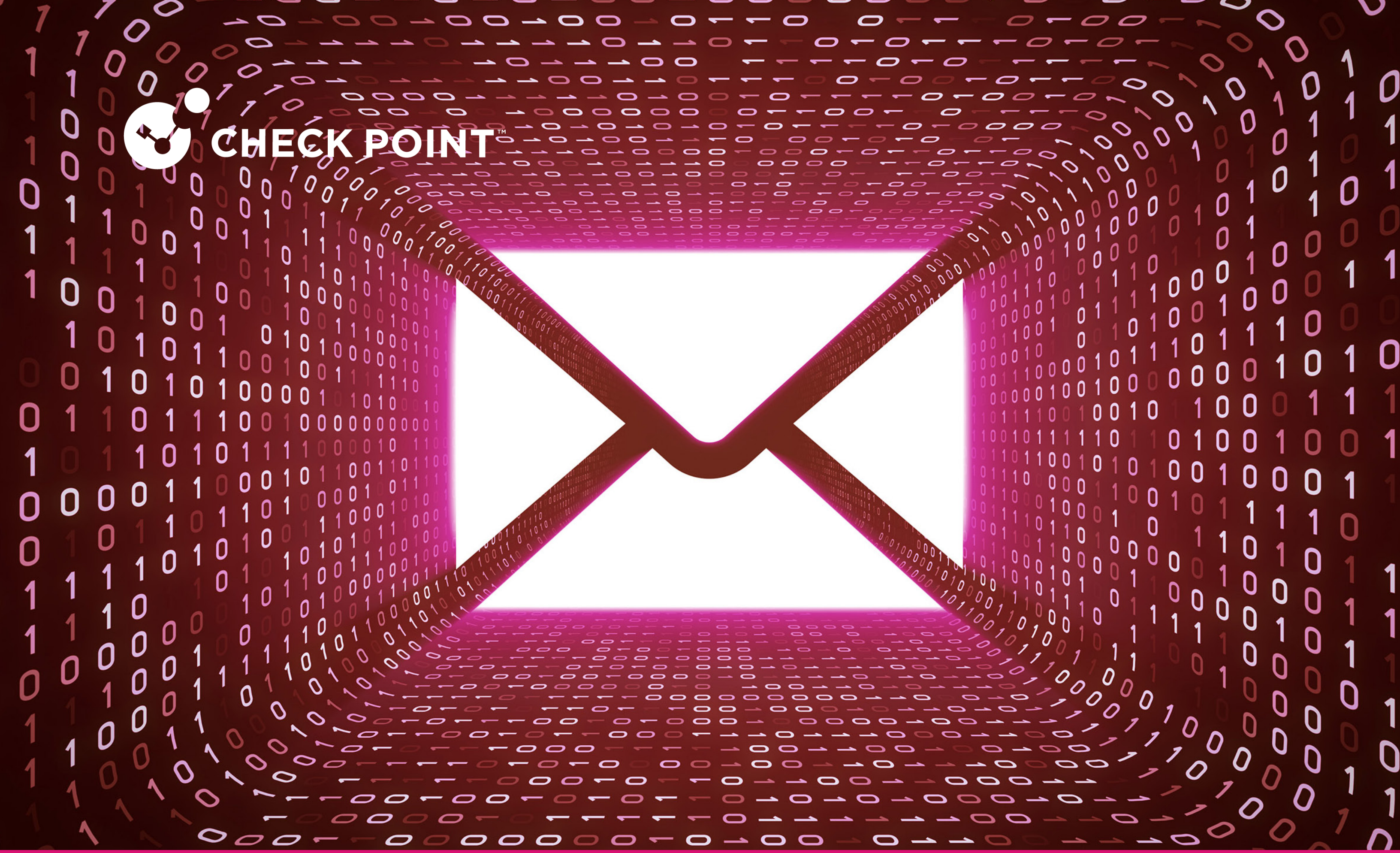


YOU DESERVE THE BEST SECURITY

Inbox Incursions Are More Than an Annoyance

They Are a Security Risk

Highlights

- Inbox incursions happen when a malicious email enters the end-user inbox, even for a moment, but often longer.
- These are the default posture of API-based apps. They add more time to the SOC's day and give more opportunities for a user to click and to implement damage to the organization.
- Inbox Incursions don't just foist bad emails upon users. They are a security risk.

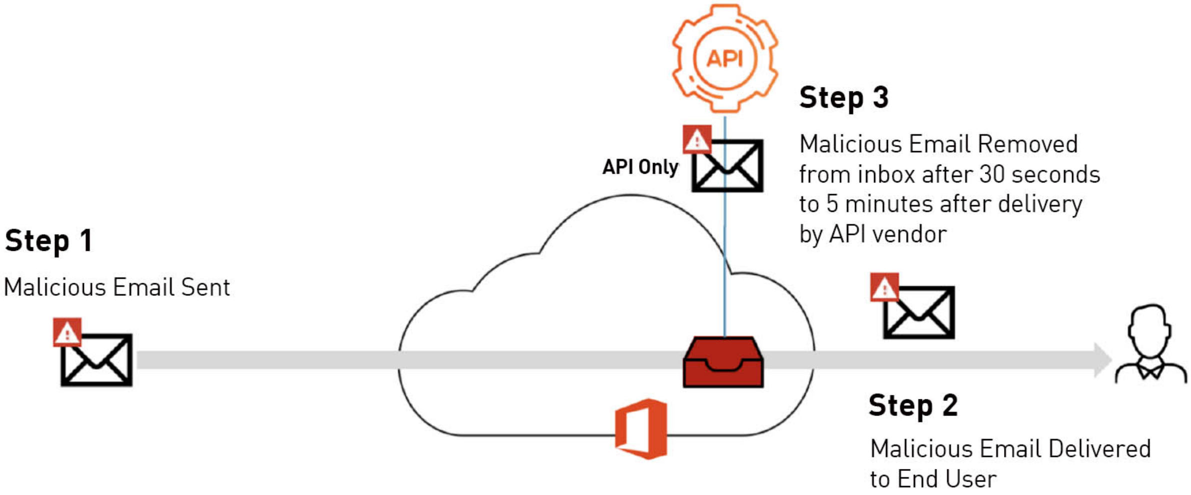
An inbox incursion is when phishing emails are available to the end user for any length of time. In such cases, the vendor remediates them post-delivery. This means the email is available for the end-user to open up and click on the link. Most marketing literature around inbox incursions will say that the message is in the inbox for barely any time. However, Avanan's research shows that the average length of time is 183 seconds.

Letting the email into the inbox for any period of time is not ideal and not the best form of email security. It gives users the ability to make mistakes and in the game of email security, the goal should be to avoid the chances for mistakes.

Consider the following analogy of the automated brake systems that many cars have. These are brakes that stop the car automatically when it senses an object coming. If the brake stops the car before it hits the object, it's protecting the driver. If it stops the car after, even if it's a second late, it's not protecting you or your car. Full protection only happens when the car stops before hitting anything.

It's the same with the inbox. If you don't protect malicious emails from reaching the inbox, then you are not providing email security. You're just reacting.

Here's how it works:


API
Step 3
Malicious Email Removed from inbox after 30 seconds to 5 minutes after delivery by API vendor
API Only
Step 1
Malicious Email Sent
Step 2
Malicious Email Delivered to End User

These solutions remediate after the email reaches the inbox. That means that inbox incursions are happening all the time. This happens all the time because, due to their architecture, these other API-based solutions cannot block before the inbox. All malicious emails, therefore, reach the inbox. The malicious ones stay there for, on average, three minutes and three seconds. That's more than enough time for a user to click on a phishing link. **Allowing malicious emails into the inbox is not providing real security. Allowing malicious emails into the inbox for as long as three minutes and three seconds is not real security.**

Inline security means that the solution scans emails after default or advanced security, but before the content reaches the inbox. That means that anything that gets past the first layers and would've otherwise hit the inbox, can get properly stopped. This type of solution means you can completely get rid of an SEG because the inline layer scans and remediates before the inbox. With this type of solution, you can stop inbox incursions, which is when a malicious email hits the inbox before being remediated. While there are several other API-based solutions on the market, none of them prevent inbox incursions. In other words, they don't block malicious emails from reaching the inbox. What's the point if end users can still have access to malicious emails? Without prevention, you have nothing but a form of remediation.

Another way of saying this is by saying that these vendors offer an email response: removing the email after it has already been delivered, typically after 30 seconds or more. For new, zero-day threats or malware that requires additional analysis, the delay can be measured in minutes or require manual intervention which could take much, much longer.

This delay gives far too much time for a user to click on a malicious message. According to the Verizon Data Breach Investigation Report:

- In 93% of data breaches, compromise occurred in minutes or less
- The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds

CESS vendors emphasize their "low response time" and the "simplicity of an administrator to respond to threats." Any response time greater than zero is too long. A manual response is too late.

Worse, these response times grow even longer in large deployments. The problem that other API-based vendors have not been able to solve is scalability. Their response time is directly correlated to the size of the environment. More users and greater email volume lead to more simultaneous API calls which lead to longer response delays resulting in a greater window of opportunity for users to click on a malicious email.

The response times promoted in sales and marketing literature reflect ideal conditions in small environments. During peak times of day, when users are busiest and most likely to be fooled by a phishing attack, response times grow longer. Five minutes, ten minutes. Even a few seconds is a security risk. And scanning the email itself can take time.

There are a few steps involved here.

First, the two systems have to establish a connection. That can take a second, but it can take even longer when hundreds of connections need to be made. After the connection is made, the email in question needs to be downloaded. The connection needs to be terminated. Then it needs to be scanned. If the email is malicious, then another connection needs to be made to quarantine. Then it needs to be quarantined.

Once all that is done, which can take as long as five minutes in some environments, then it takes milliseconds to remove from the inbox. And all the while, as the Verizon Data Breach Report reminds us, it takes just one minute and 40 seconds for a user to click on a phishing link. The race condition is on.

How do we know this? Because this was how our V1 worked before we created the ability to scan before the inbox. It's why we created our patented inline system.

Better Time Savings

Better security starts with prevention. But better security isn't the entire story. Prevention will not only make you more secure, but it will save you more time.

n a study we conducted last year, 23% of the SOC Team's time is spent managing the email threat. This includes reviewing end-user reports of suspicious emails to the SOC or security team. In one case, 70% of the daily support cases were related to email security issues. With each end user report taking on average 7 minutes to investigate, it's easy to understand how these alerts can collectively take up considerable resources. No wonder we are experiencing burnout of the SOC.

When it comes to which solution will save you more time, compare the workflows side by side. We've seen companies dramatically reduce the time the SOC has spent on email issues. One company went from nearly 600 end-user requests a day, and a SOC team simply unable to respond to all of them in a day. With Avanan, that has gone to two or three per day.

This comes down to the ability of Avanan to prevent emails before the inbox and it does this through advanced AI/ML. The threat intelligence for which the AI/ML is trained is the single most important factor in determining the effectiveness of the AI/ML algorithm. The richer the intelligence, the better the catch rate. For the "stand-alone" email security vendors, their intelligence is limited. It's limited in terms of the types and magnitude of their threat feeds. In general, they are only looking for email threat intelligence with a small sample size (only hundreds of customers). This is myopic.

Avanan's AI is powered by the world's most extensive cyber threat intelligence database and extends well beyond email threat data to include threat data from millions of devices including mobile, network, endpoint, and cloud

Compare the difference in threat intelligence datasets below:

150,000

Number of connected networks reporting into Check Point's ThreatCloud with millions of endpoints worldwide

12

Number of device types reporting into ThreatCloud including endpoint, mobile, network device, cloud, and email

86 billion

Number of transactions processed by ThreatCloud per day

7,000

Detections of zero-day threats detected each day

650,000

Suspicious websites detected per day

6.8 billion

Malicious website connections blocked last year

185 million

Malware downloads blocked last year

778 million

Vulnerability exploit attempts last year

200+

Of the world's renowned threat research team - full time threat researchers discovering some of the most significant unknown software vulnerabilities

30+

AI Technologies under one single product

The C-Suite

By now, you know what inbox incursions are. It's when API-based email security solutions allow a malicious email into the inbox before remediating. This process can take, on average, three minutes and three seconds. But the user will click on a phishing link in an average of 82 seconds. Thus begins a race condition in which the user will likely win–meaning a major loss for your organization.

Should a user click on a phishing link that leads to a damaging and costly ransomware attack, the IT team that implemented this API-based tool that can only respond to emails will have to answer some tough questions from the C-Suite and board.

Question 1: How does this security solution work?

Answer: It responds to malicious emails after they reach the inbox

Question 2: So it lets all threats into the inbox?

Answer: Yes

As you can imagine, this won't be a fun conversation. All it takes is just one click on a phishing link for damage to occur. With the average data breach costing $4.24 million per incident, that one click can bring an organization down. In fact, 60% of SMBs will go out of business within six months of being hacked.

But here's the thing, and here's where IT teams should pay attention: Avanan gives you the capability to stop all threats before the inbox. Choosing that form of security is always an option.

Avanan gives you the capability to stop all threats before the inbox. You had that option. You did not take it and then you got popped. What will you say to the CEO? The Board? "I liked the colors on the other dashboard? The company had a lot of funding?"

A third of all data breaches lead to job losses. The most affected person? Anyone in a senior IT role.

To protect your company–and yourself–from damage, you need a security solution that actually protects you. You need a solution that prevents inbox incursions and stops threats before the inbox. Only Avanan can do that.

Conclusion

Since our founding, several other API-based solutions have popped up. But they are, as Omdia puts it, "helper apps" since they can't replace the full functionality of gateways or native security, or serve as the sole protector of an enterprise. That is because they can't prevent inbox incursions. In other words, they can't stop malicious emails from reaching the inbox, and they can't stop end-users from interacting and clicking on them.

This has a number of downstream effects. For one, the SOC bears the brunt, having to deal with tons of user-reported phishing emails, not to mention cleaning up after a breach. Second, the C-Suite will want to know why action wasn't taken to block the offending emails from reaching end-users.
The only way to do that is to deploy an inline, API-based solution, that leverages the world's largest threat intelligence database to create the most sophisticated AI and ML. Doing so not only dramatically reduces the chance that malicious emails reach the inbox, it reduces the chance that users click on it, and it reduces the impact on the SOC.

When a company suffers an inbox incursion, it's not an isolated event that only happens for a minute.

So think about this when you hear this story we recently heard. One company, using an API-based email security company, saw a threat get delivered to a number of users. It sat in those users' inboxes for eight hours before being removed.

It wasn't just sitting idly by. The threat caused damage and caused the company to be attacked.

Remember, if you're not preventing the threat from coming into the inbox, it will enter the inbox. Once a threat is in your environment, whether it's three for five minutes or eight hours, it's already too late. But here's the thing, and here's where IT teams should pay attention: Avanan gives you the capability to stop all threats before the inbox. Choosing that form of security is always an option.

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