Check Point SOFTWARE TECHNOLOGIES LTD

Harmony Email & Collaboration

CASE STUDY

The State of Email Security

Quantifying How Much Time is Spent on Managing the Email Threat

Introduction: Quantifying the Magnitude of the Email Threat

Managing email threats is time-consuming and costly for enterprises of all sizes. Between preventing malicious email from causing damage to reviewing end-user suspicious email reports and false positive reports, SOC employees are overwhelmed and overworked by the sheer state of email, both good and bad.

While this feeling of being overwhelmed is shared across the board, what hasn't been done is to quantify just how much time is spent by SOC employees on managing the email threat.

In order to quantify the scope of the email threat and how companies deal with it, Check Point surveyed over 500 IT managers and leaders. This is the first comprehensive research study that looks into the magnitude of what it takes to effectively deal with the phishing problem, and the first study that uncovers how much time and energy is spent by SOC employees in preventing, responding and investigating malicious emails.

To do so, Check Point released a detailed survey into the field, asking respondents about the time it takes to deal with the email problem from three perspectives: prevention, response and investigation. Within each category, Check Point asked respondents about the tasks completed as part of their duties. Of note, in some cases, respondent data and back-end data gleaned from Check Point's servers differ, with some respondent answers resulting in higher numbers than in actuality.

Highlights

- Managing email takes a significant toll on the operations of SOC teams, regardless of company size or email server.
- Little research has been done into just how much time is spent into preventing, responding and investigating malicious emails
- Over 500 IT managers and leaders were surveyed to build a comprehensive look into the time associate with dealing with malicious emails
- The SOC team spends 22.9%, or 2-3 hours a day, of their time on this. As the email threats continue to grow, this number will only increase, placing more burden on already overworked SOC teams, and depleting resources from other critical IT tasks
- In order to combat this, automating incident response can save time and money, while boosting output of the IT team

In anticipation of new vectors emerging as additional burdens on SOC teams, such as Slack and Microsoft Teams, we also asked respondents about how they view vulnerabilities inherent to these platforms, and when they anticipate it being incorporated into their eresponse duties.

After analyzing the raw data, Check Point researchers have come across the following findings, including that SOC teams say that they spend 22.9% of their time chasing email-borne attacks that the security layer misses.

Definitions

Prevention
Response
Investigation

We broke our questions into three categories: Prevention, Response and Investigation.

Prevention refers to any activity that aids in the configuration and management of your email security to prevent attacks from reaching an end-user's inbox. For example, tasks such as updating allow/block lists, creating new mail flow rules to block specific domains and updating ATP policies would be tasks related to prevention.

Response refers to any activities related to what happens after a phishing email is delivered to the end user. This can include malicious emails delivered, users clicking on malicious links, downloading malicious content or actual compromises.

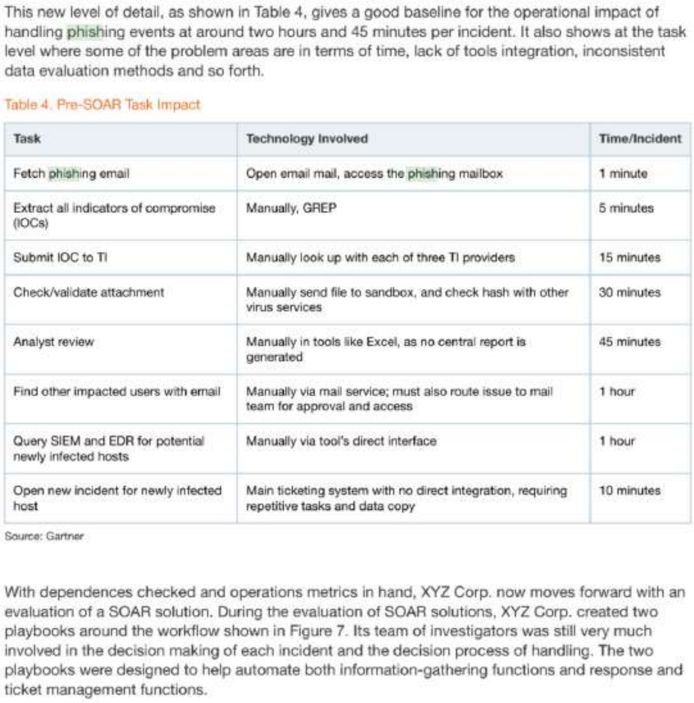
Investigation refers to any manual steps taken to decide if an email is malicious or benign. For example, tasks such as determining which links were clicked, identifying and locking down compromised accounts and data would be tasks related to investigation

We then classified activities that take place within each of these categories.

High Level Findings

Based on our survey, SOC teams say they spend 22.9% of their time chasing email borne attacks that the security layer misses.

Before this survey was conducted, there was little data on how much time the email threat took to manage. Gartner has published research on how long an individual phishing event can take to remediate, which they estimate at two hours and 45 minutes per incident.



This new level of detail, as shown in Table 4, gives a good baseline for the operational impact of handling phishing events at around two hours and 45 minutes per incident. It also shows at the task level where some of the problem areas are in terms of time, lack of tools integration, inconsistent data evaluation methods and so forth.

Table 4. Pre-SOAR Task Impact

Task	Technology Involved	Time/Incident
Fetch phishing email	Open email mail, access the phishing mailbox	1 minute
Extract all indicators of compromise (IOCs)	Manually, GREP	5 minutes
Submit IOC to TI	Manually look up with each of three TI providers	15 minutes
Check/validate attachment	Manually send file to sandbox, and check hash with other virus services	30 minutes
Analyst review	Manually in tools like Excel, as no central report is generated	45 minutes
Find other impacted users with email	Manually via mail service; must also route issue to mail team for approval and access	1 hour
Query SIEM and EDR for potential newly infected hosts	Manually via tool's direct interface	1 hour
Open new incident for newly infected host	Main ticketing system with no direct integration, requiring repetitive tasks and data copy	10 minutes

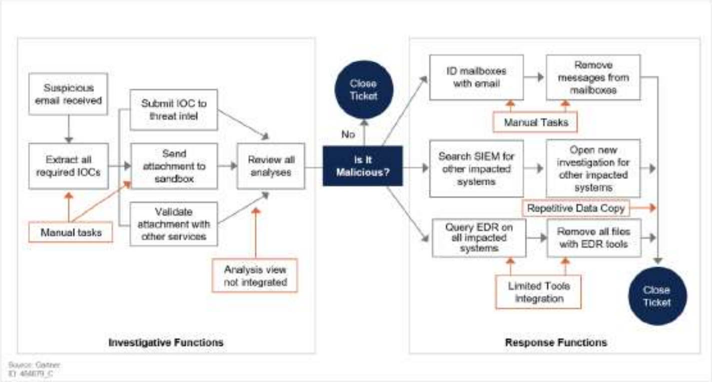
Source: Gartner

With dependences checked and operations metrics in hand, XYZ Corp. now moves forward with an evaluation of a SOAR solution. During the evaluation of SOAR solutions, XYZ Corp. created two playbooks around the workflow shown in Figure 7. Its team of investigators was still very much involved in the decision making of each incident and the decision process of handling. The two playbooks were designed to help automate both information-gathering functions and response and ticket management functions.

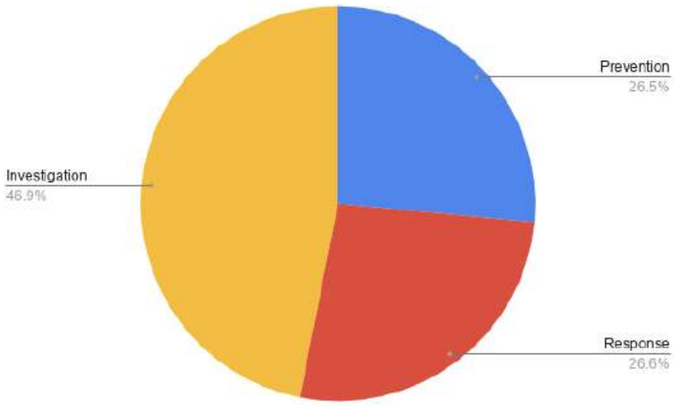
What hasn't been quantified is how much of a burden that places on SOC teams.

When there's one email to remediate, two hours and 45 minutes isn't too bad. But when combined with the sheer amount of email-based attacks, it not only presents a large risk but it takes up a large burden—22.9% of our respondents' workload. As one customer said, "We were constantly bombarded."

Security operations centers (SOCs) are overwhelmed with all the elements related to managing the email threat. Sample workflows, like this one from Gartner, can be confusing and overwhelming:


Suspicious email received
Extract all required IOCs
Manual tasks
Submit IOC to threat intel
Send attachment to sandbox
Validate attachment with other services
Review all analyses
Analysis view not integrated
Investigative Functions
Close Ticket
No
Is It Malicious?
ID mailboxes with email
Remove messages from mailboxes
Manual Tasks
Search SIEM for other impacted systems
Open new investigation for other impacted systems
Repetitive Data Copy
Query EDR on all impacted systems
Remove all files with EDR tools
Limited Tools Integration
Close Ticket
Response Functions
Source: Gartner
ID: 464679_C

The average SOC, regardless of email provider, spends about 22.9% of their time managing the email threat.



Of that time, we've quantified how much is spent on each task.

- **SOC teams spend 46.9% of that time on Investigation**
- **SOC teams spend 26.6% of that time on Response**
- **SOC teams spend 26.5% of that time on Prevention**

This burden is broken down into several categories.

- SOC teams spend, on average, spend about 5.59 hours on prevention tasks
- SOC teams receive about 68.7 end-user reports per week. In reviewing those emails, SOC employees spend an average of nearly 7.7 minutes inspecting it. **Of those emails, 33.8% turn out to be malicious.**
- For release from quarantine requests, there are an average of 16 requests per week.
- Of those emails, 30.73% are false positives
- The average SOC team spends 1,380 hours a year dealing with release from quarantine
- **By using Check Point Harmony Email & Collaboration, customers say they save on average 5.3 hours per week in email security related tasks**

The survey also asked respondents which email server they use. The vast majority, 78.0%, use Microsoft 365, while just 3.78% use G-Suite. In total, 88.44% use cloud-based email servers.

We also asked which email security company these respondents use to protect their email. The majority, 43.09% use Microsoft ATP; 23.09% use a Secure Email Gateway; and 17.4% use an API-based email security. Check Point Harmony Email & Collaborator customers make up 21.7% of the respondents.

Finally, given the increasing threat that both Slack and Microsoft Teams may provide in the future, we asked respondents when they thought they would need to invest resources into protecting these platforms. Overall, 76.1% of respondents either agree or strongly agree that "vulnerabilities in collaboration tools such as Slack and Teams pose a security risk," and believe that it will require security within the next eight months.

The following survey report will detail the findings in regards to prevention, response and investigation, as well as exploring vulnerabilities in Slack and Teams.
regards to prevention, response and investigation, as well as exploring vulnerabilities in Slack and Teams.

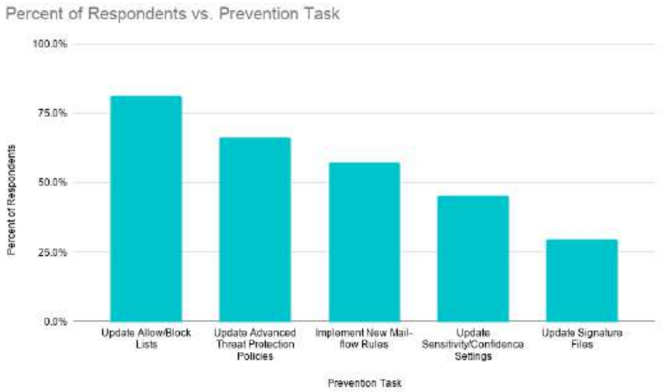
Time Spent Preventing Malicious Emails

Prevention
Response
Investigation

In addition to asking about the time spent on prevention duties, we also asked what duties are performed in preventing malicious emails from reaching end users.

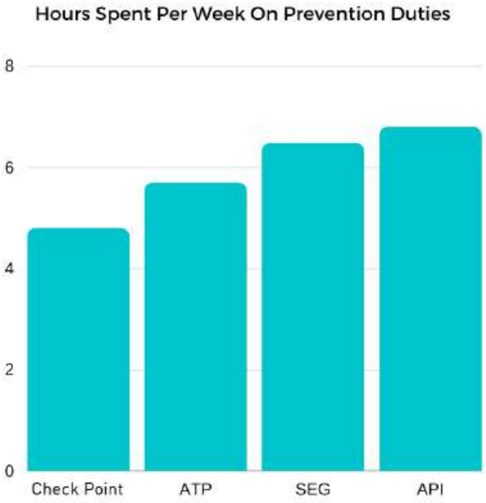
The most commonly performed task associated with prevention was updating allow tand block lists. 79.6% of respondents utilize this in their prevention duties.

Second to that was updating ATP policies, of which 64.9% performed this. From there, 56% implemented new mail-flow rules, while 44.3% update sensitivity and confidence settings. That was followed up by 28.9% who updated signature files.



All of these tasks led to an average of 5.59 hours spent per week on prevention duties, . As one customer said, "It used to take me hours to find malicious things and take care of them."

When broken down by email security providers, those who employ Check Point Harmony Email & Collaboration spend the least amount of time preventing bad emails, at 4.8 hours per week. Those with other API-based solutions spend the most, at 6.9 hours.



Check Point Harmony Email & Collaboration customers saved, on average, 4.875 hours per week on prevention tasks.

Time Spent Responding to end-user requests and release from quarantine

Prevention
Response
Investigation

We broke the question about responding to emails into two categories: user-reported messages, and release from quarantine. (see figure 7.1).

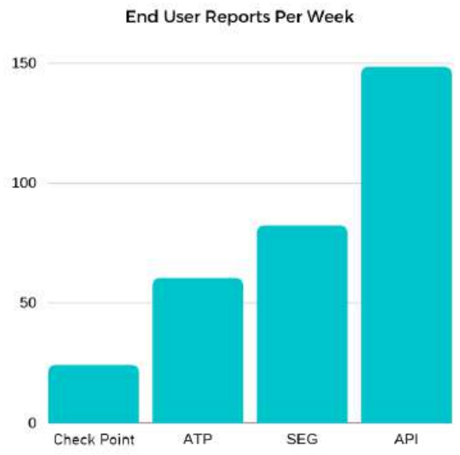
We first asked respondents if their end-users have a way to report suspect emails that have reached the inbox. 88.3% said yes, though there was variation in how that process played out. For 43.4% of respondents, users clicked on a button within the email client; for 40.6% of respondents, the users forward the email to an admin.

Regardless of how the user reports the email, it totals to an average of 68.7 end-user reports per week.

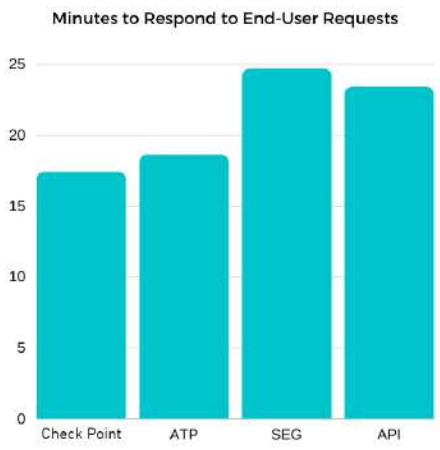
SOC analysts spent an average of 7.7 minutes reviewing each of these emails. Just over one-third, or 33.79% of these emails, turn out to be malicious.

The average SOC team, according to respondent data, sees about 3,574 end-user reports a year, with 1,207 of these being phishing emails. They'll spend 1,183 hours or just over 49 days responding to these. Considering that time burden, one customer noted, "I have a lot of users managed by a tiny IT team so I'm always looking for ways to simplify tasks that eat up much of our time."

When seeing how many end-user reports per week based on the email security provider, a clear pattern emerges. Those who use Check Point Harmony Email & Collaboration, according to their responses, see an average of 24.1 emails from end-users, over 30 fewer than the next highest, which is ATP, and more than 100 fewer than than other API-based vendors.



In terms of minutes spent per end-user review, Check Point Harmony Email & Collaboration customers report spending the least amount of time, with an average of 17.4 minutes, while SEGs come out at the highest, with an average of 24.7 minutes.



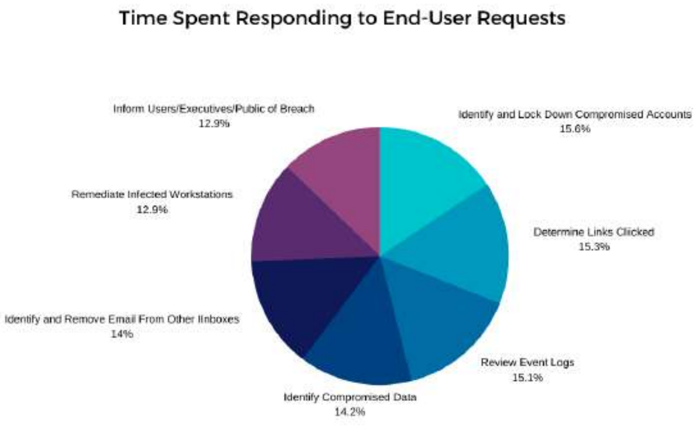
For user release from quarantines, we found that 89.7% of respondents had a way for users to request a release from quarantine. 57.9% of respondents have end-users click a button or link in the email client; 31.9% send or forward an email to an admin (see figure 8.2).

The average SOC team receives about 16 release from quarantine requests each week. It takes about 12.1 minutes to analyze a single email. Per week, the SOC spends 1,592 minutes, or 26.53 hours, per week on reviewing the requests.

Of these emails, 30.73%, or 40.6, turn out to be false positives.

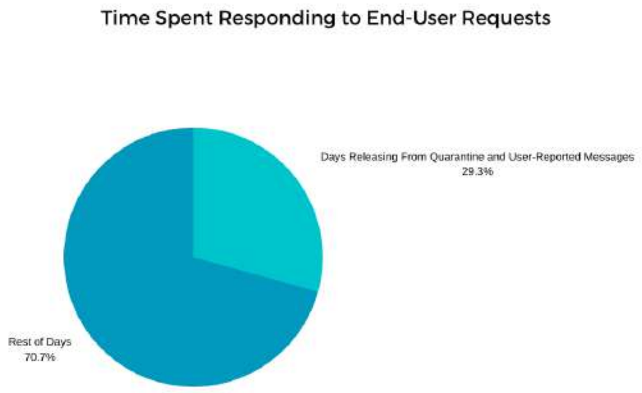
In responding to emails, we asked respondents which tasks they most commonly utilized:

There were a number of tasks that were all jumbled towards the top. 69.0% of respondents identify and lock down compromised account(s); 67.7% respondents determine which links were clicked; 66.5% review event logs; 62.6% identify compromised data; 61.9% identify and remove email from other user inboxes; 56.7% inform users/executives/public of a breach; and 56.7% remediate infected workstations.

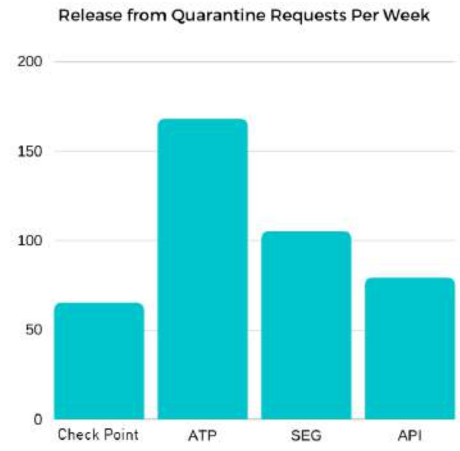


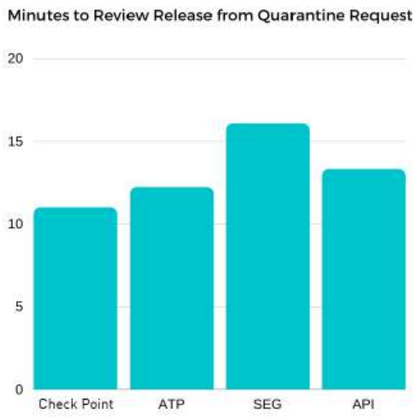
In all, SOC teams will review 6,862 release from quarantines requests, totaling 1,380 hours.

Between releasing from quarantine and user-reported messages, the average SOC team 2,572 hours, or just over 107 full days, responding to these emails.



With release from quarantine requests, Check Point Harmony Email & Collaboration customers, according to their responses, put forth the fewest, at 65 per week, while ATP customers had the most, at 168.





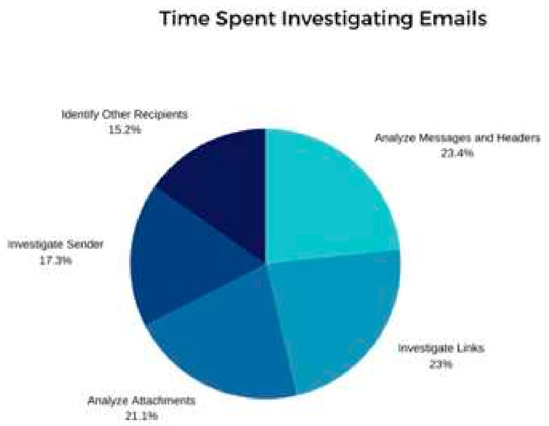
In minutes spent on each email, those with Check Point Harmony Email & Collaboration, according to their responses, spent just 11 minutes on average; those with SEGs spent 16.08 minutes. As one customer said about Check Point Harmony Email & Collaboration, "Our security team enjoys the workflow from within the portal to respond to users submitting a request for restores if something is in quarantine. It has given our team time back during the day to move onto other tasks (see figure 9.3)."

In all, Check Point Harmony Email & Collaboration customers save 3.812 hours per week in response tasks.

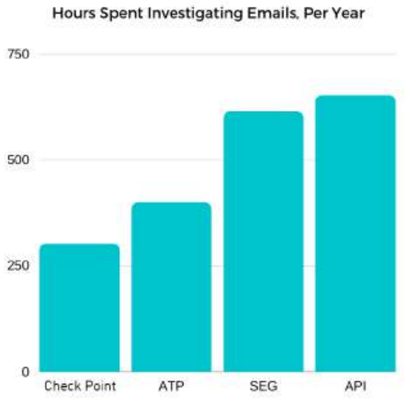
Time Spent Investigating Emails

Prevention
Response
Investigation

In investigating an email, SOC analysts have a number of tools at their disposal. We asked professionals how often they analyze messages and headers, investigate links, analyze attachments, investigate senders and identify other recipients.



When looking at how much time is spent on analyzing malicious emails per year, those with Check Point Harmony Email & Collaboration report spending 301 hours, or just over 12 full days. As one customer said, Check Point provides an easy-to-understand analysis of exactly why an email has been deemed to be safe or malicious." Added another customer: "We're able to do in minutes a day, via their single pane of glass, what used to take multiple tools and hours per week to achieve." The highest amount of time in terms of analyzing malicious emails came with other API solutions, at 652 hours, or just over 27 full days.



Check Point Harmony Email & Collaboration customers saved 4.88 hours per week on investigation tasks (see figure 10.3).

Vulnerabilities in Slack and Microsoft Teams

We also asked respondents about their views on vulnerabilities in collaboration tools like Slack and Teams. As these increase in popularity, we expect that responding to threats and events will become ever more part of the SOC's days.

To best assess this, we asked respondents a number of questions. Overall, 76.1% of respondents either agree or strongly agree that "vulnerabilities in collaboration tools such as Slack and Teams pose a security risk."

Of the key concerns, the following rated highest:

72.6% were most concerned with leakage of sensitive data; 60.7% were most concerned about messages with phishing links; 53.3% were concerned about messages containing malicious files; and 50% were concerned with hosting of malicious files or compromised accounts.

In all, respondents thought that they would be forced to address these vulnerabilities in the next eight months.

Additionally, we asked respondents who used ATP what particular issues, if any, they had with the product. 26.7% of ATP users said that it was "difficult and/or time consuming to administer" while 24.4% said "false positives" was their biggest concern.

Conclusion

The email threat is worse than ever and it is overwhelming SOC employees across all industries, regardless of what email server they use or what email security they use.

A survey released by Check Point, completed by over 500 IT professionals, found that SOC employees spend about 22.9% of their time managing the email threat. That comes out to over 131 full working days, simply on prevention, response and investigation.

The majority of this time is spent reviewing end-user phishing reports, which takes about 1,183.2 hours per year, as well as reviewing release from quarantine requests, which take up 1,380 hours. This is over 106 days working days.

In 2020, in an effort to help alleviate this burden from enterprises, Check Point introduced an Incident Response as a Service program. Also known as IRaaS, this program routes end-user requests to restore from quarantine or to mark as suspicious to our team of experts. It's reviewed by our analysts, usually in about five minutes, but in no more than 30 minutes. Our highly-trained experts, who are available around the clock, either approve or deny the request. For malicious emails, the analyst will search and destroy similar emails, both current and future ones.

One major corporation using Check Point's services has saved 20 hours per week in the SOC, and have been able to free up SOC employees for other critical tasks.

This product allows overwhelmed IT teams to focus on other critical issues. As one customer said, "IraaS adds value by having security experts review each restore request for validity. IT offloads efforts spent by the internal IT team. And in a job where 60% of SOC employees have considered leaving their jobs or changing careers altogether because of burnout, anything that can be done to make the job easier is crucial.

The more platforms that come online, like Slack and Teams,will mean that SOC employees will have even more response work to dealing with, minimizing the time spent on other issues even further.

At a time when cyber threats of all kinds are worse than ever, SOC professionals are hampered by dealing with the email problem. Though email is a significant issue, that incident response can be automated, allowing SOC professionals to deal with other issues.

Check Point Harmony Email & Collaboration is a cloud email security platform that pioneered and patented a new approach to prevent sophisticated attacks. It uses APIs to block phishing, malware, and data leakage in the line of communications traffic. This means Check Point Harmony Email & Collaboration catches threats missed by Microsoft while adding a transparent layer of security for the entire suite that also protects other collaboration tools like Slack. The solution has been recognized as the top-rated cloud email security solution by customers and can replace the need for multiple tools that surround email and file sharing.