2019 EMAIL SECURITY

CHALLENGES, TRENDS, BENCHMARKS

2ND ANNUAL SURVEY REPORT

GreatHorn

INTRODUCTION

The GreatHorn team conducts an annual survey to get a pulse on email security. This survey research allows for a better understanding of today's pervasive email-borne threats and the ways in which information security and IT teams are defending this "venerable, yet vulnerable"* (phrase credit: Neil Wynne, former Gartner Analyst) communications platform.

The 2019 Email Security Trends, Challenges, and Benchmark Survey Report provides an in-depth look at the facts and figures that tell the story of the current state of email security. This year's survey panel consisted of more than 1,021 email security and white-collar professionals from various industries. The diversity of the panel enabled us to explore how different characteristics (e.g. level of involvement in email security, company size, email platform, etc.) correlated into different and in some cases, surprisingly similar trends.

For our analysis, we categorized a survey respondent as an "email security professional" (representing 56.8% of our total survey panel) if he or she was involved in one or more of the following activities for email security:

- Owns technical requirements
- Owns the budget
- Is a technical evaluator
- Sets overall security strategy (e.g. CISO)

We're terming the survey respondents who have "limited or no involvement in email security" or "business evaluators" as "white-collar professionals" (representing 43.2% of our total survey panel).

1021

RESPONDENTS

EMAIL SECURITY PROFESSIONALS

Respondents involved in activities for email security

WHITE-COLLAR PROFESSIONALS

Respondents with "limited or no involvement in email security" or "business evaluators"

Source: GreatHorn, "2019 Email Security Benchmark"

EXECUTIVE SUMMARY

This year's key takeaways validate what we're hearing anecdotally, but are still startling in their severity.

Traditional email security is failing to keep up

- Half (49.8%) of respondents see malicious emails reach their inboxes every week, despite a multi-layered defense strategy that includes an average of more than two email security solutions.
- In the past three months, more than 1 in 5 respondents (22%) reported experiencing a data breach (defined as a compromised account, loss of confidential data, credentials, fraudulent financial transaction) due to an email-borne attack.
- Since last year, there's been a steep rise in email remediation rates from 20% of respondents needing to take direct actions every week to more than 34% this year.

The cybersecurity awareness training gap is faintly narrowing. As an industry, we still have a long way to go.

Our data also shows that the individuals with limited or no involvement in email security are 3x more likely to say "I don't see anything but spam in my inbox," compared to those respondents involved in email security (48.5% vs. 16.4%). This illustrates a clear gap despite the large sums of money having been spent on cybersecurity awareness training programs. According to recent research, since 2015 more than $1.2 billion has been spent on computer-based training* (Gartner), but simulated phishing click-rates have dropped by only 1% from 2017 to 2018* (2019 Verizon DBIR).

In short, the current state of email security is shaky. Email security professionals need to be more vigilant as end-users are seeing more threats making their way to inboxes—25% more compared to last year. Keep reading to learn more about our findings, gain valuable insights, and see how your organization compares.

TRADITIONAL EMAIL SECURITY CAN'T KEEP UP

22% reported experiencing a **breach** due to an email-borne attack

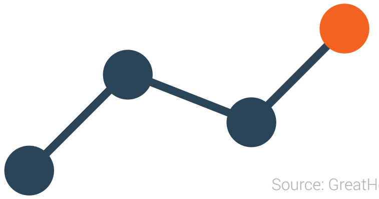
IN THE PAST 3 MONTHS

Defined as a compromised account, loss of confidential data/credentials, fraudulent financial transaction, etc.

Source: GreatHorn, "2019 Email Security Benchmark"

THE STATE OF SECURITY IS SHAKY

Respondents are seeing more threats making their way to inboxes



25% more compared to last year

Source: GreatHorn, "2019 Email Security Benchmark"

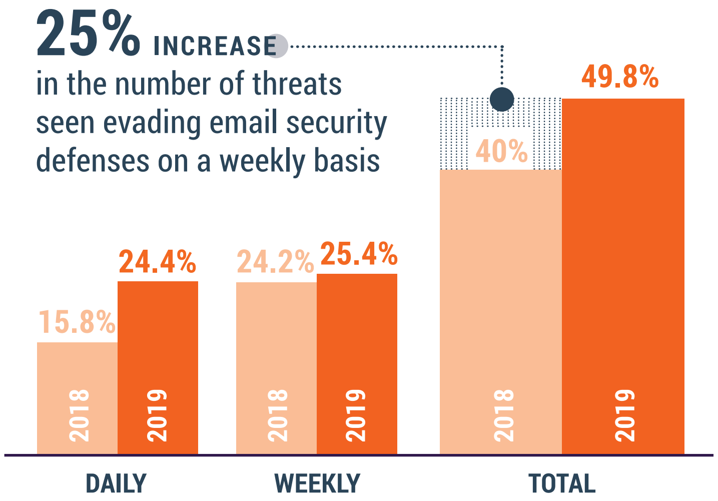
THREATS ON THE RISE

According to our research, email attacks are still on the rise and still keeping CISOs up at night. In general, the volume of email attacks is mounting as 24.4% of respondents indicated that despite existing email security measures, malicious messages (impersonations, wire transfer requests, W2 requests, payload attacks/malware, business services spoofing, and credential theft attempts) make their way to inboxes every day, with an additional 25.4% of respondents saying that they see email threats in their inboxes every week—a total of 49.8% seeing email threats at least every week (a 25% increase from last year).

When we separated our survey panel's responses into two groups: email security professionals and white-collar professionals, we found a stark contrast in the frequency of malicious email threats reported.

Approximately only 1 in 3 white-collar professionals (36.4%) report seeing email-based threats on at least a weekly basis. In contrast, a greater percentage of email security professionals (32.8%) report seeing threats every day, and an additional 27% report weekly, for a total of 59.8% seeing threats at least weekly. This marked difference in perception speaks to training and awareness gap that we'll explore in greater detail later in this report.

Alarmingly, 1 in 5 email security professionals reported that in the past three months they had experienced a breach (e.g. compromised accounts, loss of confidential data or credentials, fraudulent financial transaction, etc.) due to an email-borne threat. These same respondents also reported an average of 2.6 security products deployed to protect their email.



Source: GreatHorn, "2019 Email Security Benchmark"

RESPONDENTS WHO NOTICE MALICIOUS EMAIL THREATS WEEKLY, BY GROUP

36%
WHITE-COLLAR PROFESSIONALS

60%
EMAIL SECURITY PROFESSIONALS

Source: GreatHorn, "2019 Email Security Benchmark"

THREAT PREVALENCE

We found inconsistent replies when we asked respondents "what types of threats do you see in your inboxes" (i.e. those that do not get quarantined).

Only 30% of white-collar professionals see executive, internal, or external impersonations. But as we narrow our focus to email security professionals, we find that 56.7% of this population reports impersonations bypassing email security tools. Credential theft was the second most prevalent threat (33.9%), followed closely by wire transfers (33.3%), business services spoofing (32%), payload/malware (28.3%), and W2 requests (21.1%).

More than one-quarter of email security professionals report that payload attacks (e.g. malicious/suspicious attachments or links)—despite being the threats most heavily guarded against—are still making it through their cybersecurity defenses.

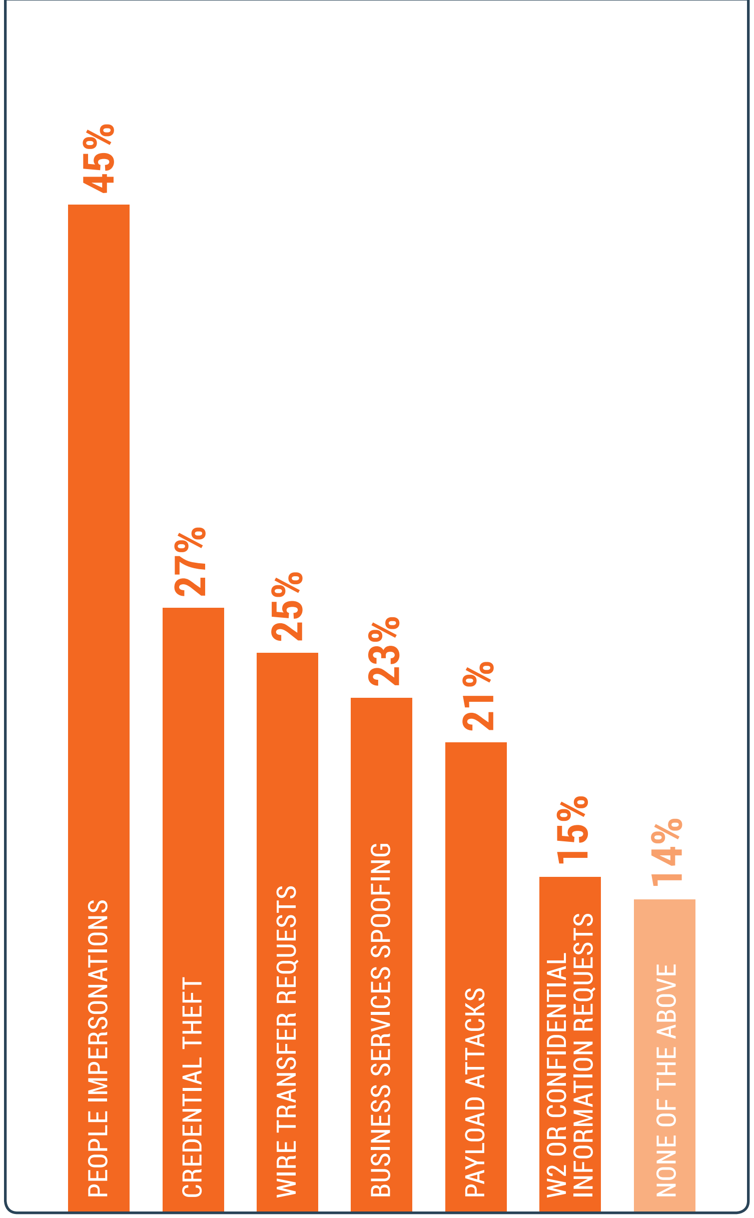
1/4 of email security professionals report that

PAYLOAD ATTACKS ARE STILL GETTING THROUGH

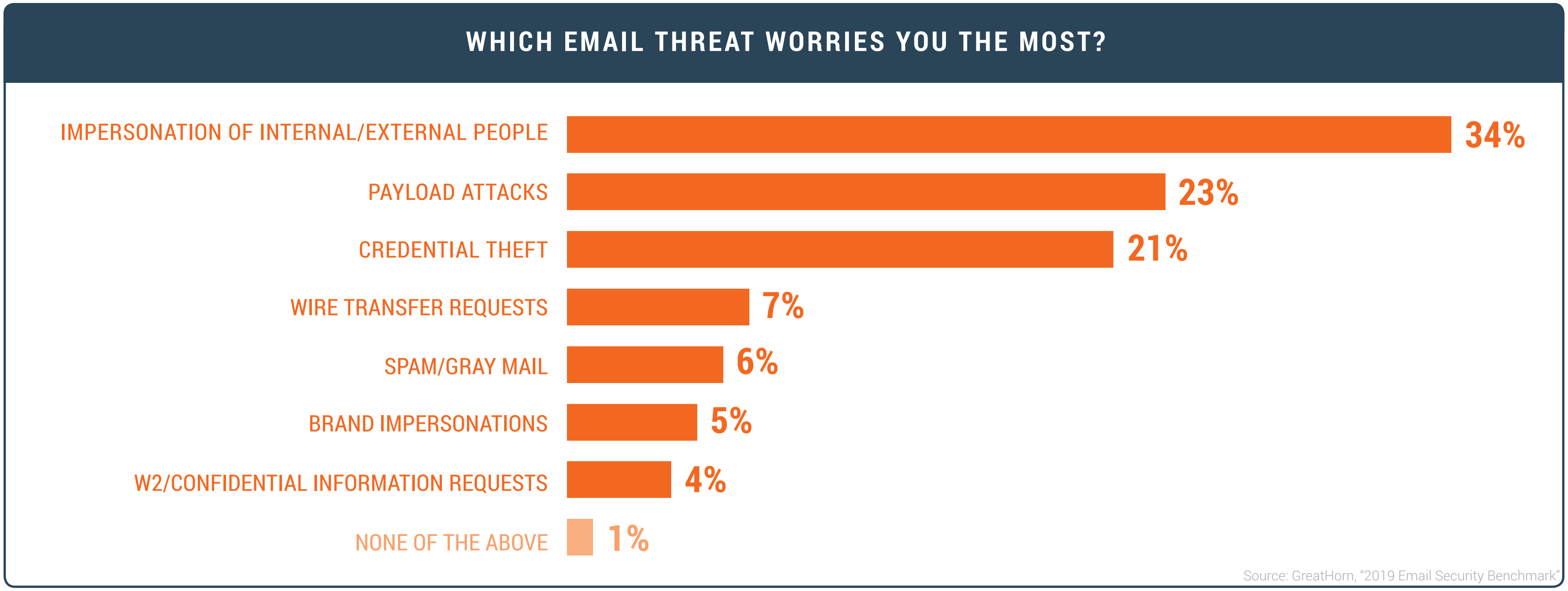
Source: GreatHorn, "2019 Email Security Benchmark"

When breaking down the data by company size, we find the prevalence of threats to be roughly the same (within ~ five percentage points), with smaller companies (defined as fewer than 500 employees) seeing a slightly higher rate of most email attack types with the exception of credential theft attempts (39.8% large companies vs. 25.6% smaller companies).

WHAT TYPES OF THREATS DO YOU SEE IN YOUR INBOX?



Source: GreatHorn, "2019 Email Security Benchmark"



WHICH EMAIL THREAT WORRIES YOU THE MOST?

Source: GreatHorn, "2019 Email Security Benchmark"

There was minimal correlation between the prevalence of a given type of attack and the importance assigned to it. When asked "Which email-based threat worries you the most," email security professionals consistently ranked three threats at the top, regardless of organization size: impersonations (34.3%), payload-based attacks (23.3%), and credential theft (20.5%).

In contrast, W2 or confidential information requests was consistently the least cause of concern (4.2%). Less than 1% of respondents expressed that they had no concerns about email-based threats.

Not surprisingly, people who indicated themselves as "dissatisfied" or "very dissatisfied" with their email security solution were much more likely to see threats reach inboxes, with 39.5% reporting business services spoofing, 37.2% payload-based threats, 37.2% credential theft attempts, 38.3% wire transfer requests, and 72.1% impersonations.

People who indicated themselves as "dissatisfied" or "very dissatisfied" with their email security solution were **much more likely to see threats reach inboxes**

Source: GreatHorn, "2019 Email Security Benchmark"

POPULAR PREVENTION MEASURES

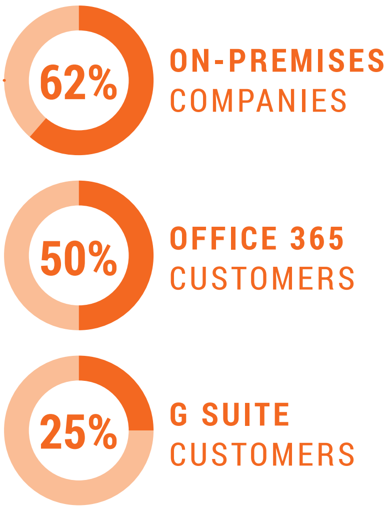
When we compare different groups against their use of specific strategies, we find some remarkable differences. For example, 61.6% of on-premises companies use secure email gateways compared to half (50%) Office 365 customers, and just a quarter (25.3%) of G Suite customers.

On-premises companies were also more likely to use stand-alone anti-virus/anti-spam solutions (47.3% vs. 41.7%) and firewalls (51.8% vs. 46.5%) than cloud-email companies. Adoption rates for computer-based training were consistent across both cloud and on-premises companies (35.7%).

Meanwhile, companies on cloud email were far more likely (10.9%) to either use “nothing” just “native cloud-email features,” compared to on-premises organizations (5.4%). Details on the “Other” indicate a variety of options, such as environmental segregation (on-premises) and newer cloud-native email security products.

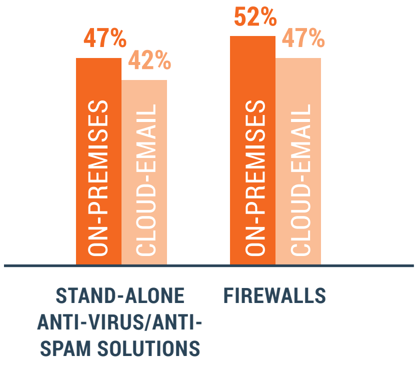
Microsoft Office 365, Google G Suite, and/or traditional email gateways often mark real, legitimate email messages as spam or junk mail, creating many false positives and a false sense of security. This dangerous combination can result in risky end-user behaviors. Not surprisingly, those individuals who expressed dissatisfaction with their existing email security tool for “negatively impacting business operations (e.g. too many false positives)” were even more likely to open email in their junk or spam filters (61.5% in the past month).

COMPANIES USING SECURE EMAIL GATEWAYS



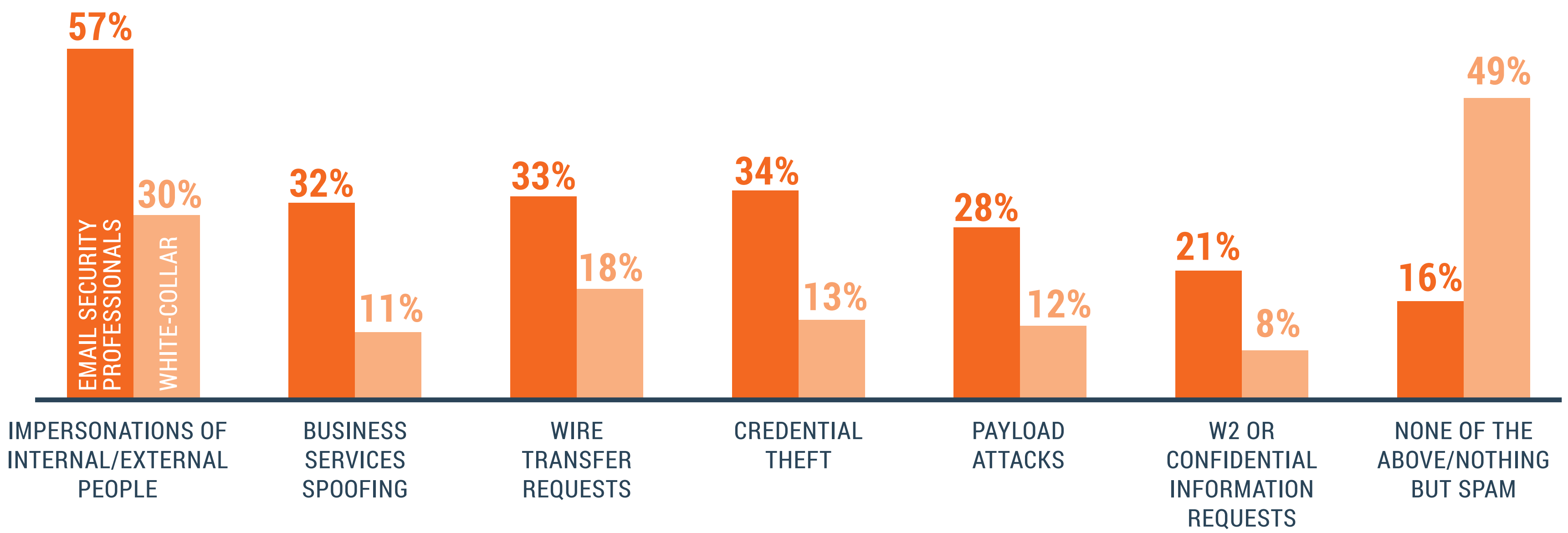
Source: GreatHorn, “2019 Email Security Benchmark”

On-premises companies are more likely to use other solutions over cloud-email companies:



Source: GreatHorn, “2019 Email Security Benchmark”

WHICH OF THE FOLLOWING TYPES OF EMAIL DO YOU/YOUR USERS SEE IN YOUR INBOXES (NOT WHAT GETS QUARANTINED)?



Source: GreatHorn, "2019 Email Security Benchmark"

We asked our survey panel, "Which of the following types of email do you/your users see in your inboxes (NOT what gets quarantined)?" As you can see in the graph above, it's not just the sophisticated and personalized phishing attacks that evade email security filters.

Nearly half (48.5%) of white-collar professionals reported "nothing but spam," but only 16.4% of email security professionals said the same. That means that two-thirds of white-collar professionals mischaracterize sophisticated email threats as "just spam." There is a clear nomenclature problem. Somewhere along the line, things got muddied. This convolution of spam mail and potentially dangerous email threats is too risky and can cause white-collar professionals to partake in risky behaviors (e.g. opening email from spam or junk mail folders).

REPORTING "NOTHING BUT SPAM"

49% WHITE-COLLAR PROFESSIONALS

16% EMAIL SECURITY PROFESSIONALS

Source: GreatHorn, "2019 Email Security Benchmark"

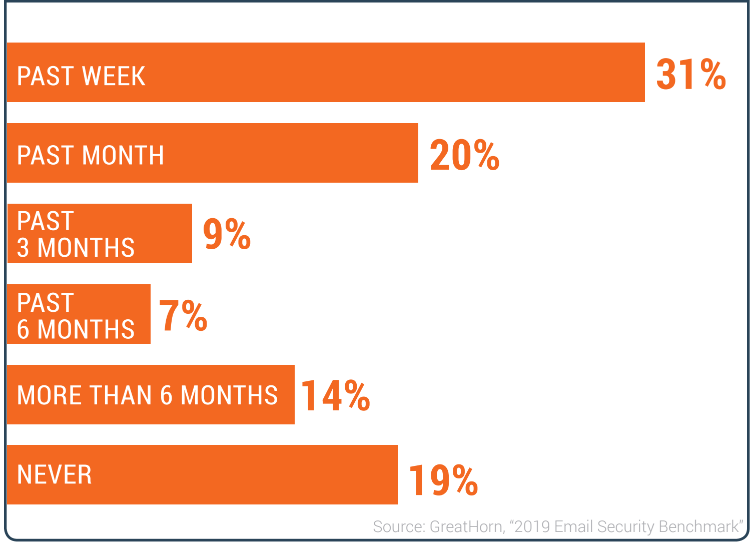
One of the more alarming findings is that in the past month, 51% of our panel had opened email messages in their junk and spam folders—31% did so in the past week.

Surprisingly, email security professionals (53.4%) were more likely to have opened messages in their junk and spam folders in the past month—compared to non-email security professionals (41.3%).

When we asked white-collar professionals, “What types of email threats do you see in your inboxes,” they are 3x more likely to say, “nothing but spam” (48.5% vs. 16.4% of email security professionals.)

As we stated in the beginning of this report, this misspeak illustrates a striking education gap—even though companies are spending a lot of resources on computer-based training and phishing simulations. Security awareness training alone is not enough. According to Gartner, since 2015 more than $1.2 billion has been spent on computer-based training, and simulated phishing click-rates have dropped by only 1% from 2017 to 2018.

WHEN DID YOU LAST OPEN AN EMAIL IN YOUR JUNK/SPAM FOLDER?



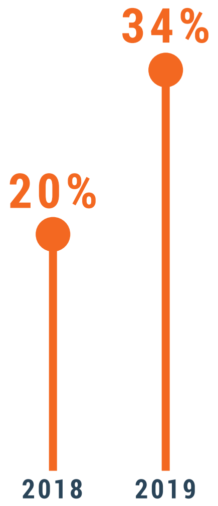
Source: GreatHorn, “2019 Email Security Benchmark”

INCIDENT RESPONSE RATES

In addition to understanding the frequency and types of threats professionals see, we asked respondents how often direct remediation and/or incident response actions are necessary (i.e. suspending compromised accounts, PowerShell scripting, resetting compromised third-party accounts, etc.).

Since last year, there’s been a steep rise in remediation rates from 20% of respondents needing to take direct email remediation actions every week to more than 34% this year.

A STEEP RISE IN REMEDIATION RATES IN THE PAST YEAR

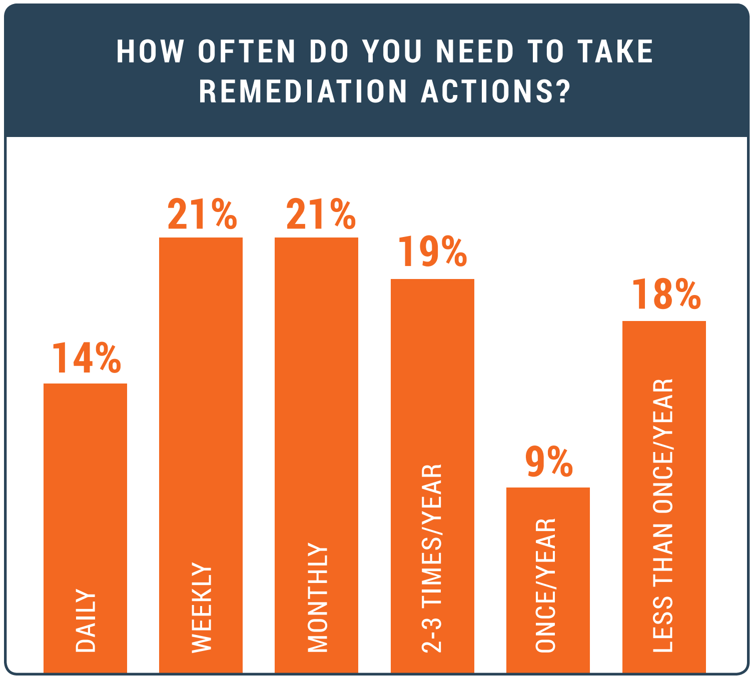


On average, one in three respondents needs to take such remediation actions on at least a weekly basis. An additional 20.7% need to do so at least monthly. Not surprisingly, the more often they reported seeing threats in their inboxes, the more likely they were to require daily or weekly remediation.

Of the respondents who see threats reach inboxes daily, 54.8% of them must take remediation actions on at least a weekly basis. Change that very slightly to look at respondents who report threats weekly, and the weekly remediation percentage drops to 44.2%. Only 6.4% of respondents who report monthly threats conduct weekly remediation.

Organizations that remediate "Daily" (38.5%) and "Weekly" (35.9%) have experienced a breach more frequently. 1 in 5 respondents reported that they have experienced a data breach (e.g. compromised accounts, loss of confidential information, credential theft, fraudulent financial transaction, etc.) due to an email-borne threat in the past three months.

Respondents who see email threats in their inboxes on at least a weekly basis were more likely to have experienced a data breach (25.6%). Also, very large enterprises (over 10,000 mailboxes) were more likely (31.3%). Email security teams that need to manually remediate Daily (38.5%) and Weekly (35.9%) have experienced a breach more frequently.



Source: GreatHorn, "2019 Email Security Benchmark"

1 IN 5

RESPONDENTS

reported that they have experienced a data breach due to an email-borne threat in the past three months

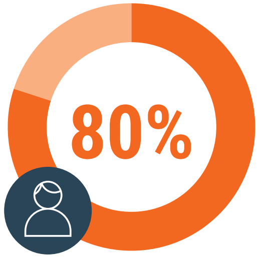
Source: GreatHorn, "2019 Email Security Benchmark"

CONCLUSION
GOOD ENOUGH IS JUST NOT GOOD ENOUGH

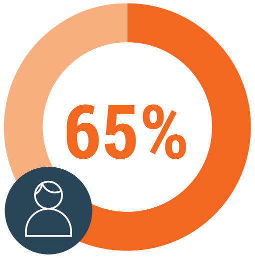
When asked, “Which of the following are problems for you despite your current email security solution? (Select all that apply),” 79.4% of all respondents indicated fundamental issues with their solution:

- **26.6%** say that their current solution “Doesn’t stop internal threats (e.g. if a user account is compromised)”
- **18.9%** say “Missing payload attacks (e.g. malicious attachments and/or links)”
- **21.2%** say “Missing payload-free attacks (e.g. impersonations, social engineering)”
- **34.2%** say “Challenges with remediation”
- **19.8%** express concern that their solution “Negatively impacts business operations (e.g. too many false positives)”

65% highlighted fundamental technical issues with their existing email security solution.



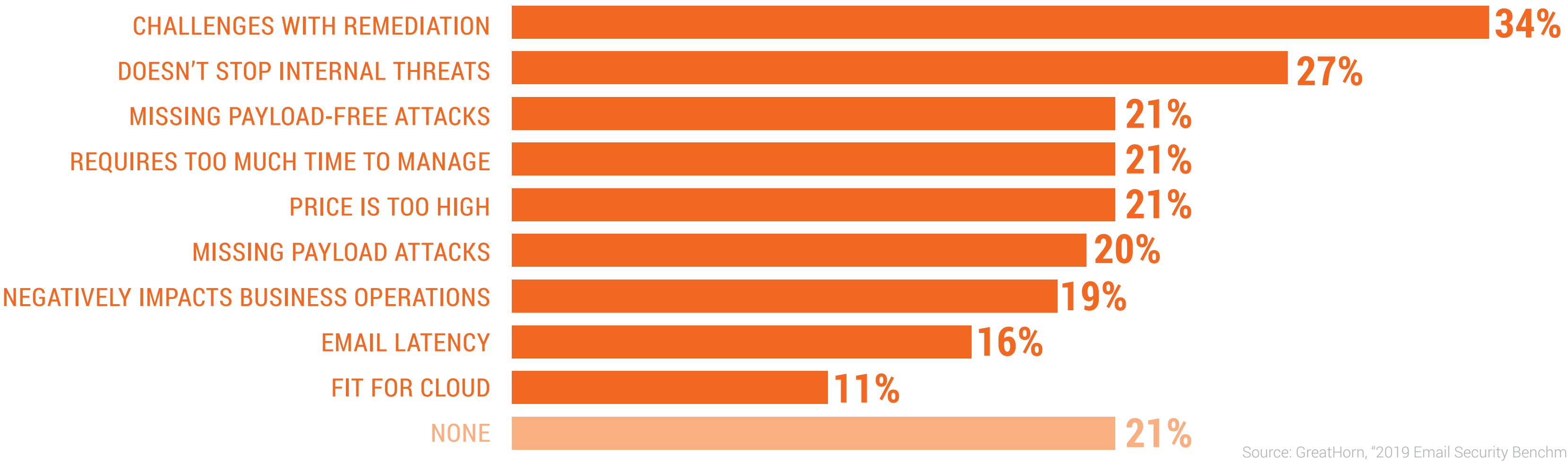
Indicated **fundamental issues** with their solution



Indicated **fundamental technical issues** with their solution

Source: GreatHorn, “2019 Email Security Benchmark”

WHICH OF THE FOLLOWING ARE PROBLEMS FOR YOU DESPITE YOUR CURRENT EMAIL SECURITY SOLUTION?



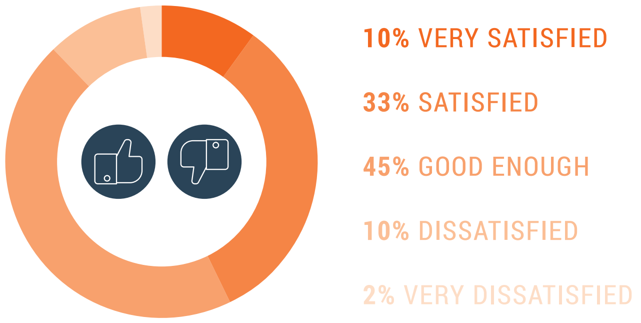
Source: GreatHorn, “2019 Email Security Benchmark”

Overall, nearly 3 out of 5 respondents reported that they were less than "satisfied" with their current email security solution, and only 10.4% were "very satisfied." Roughly a third (34.3%) indicated that their solution was "good enough."

G Suite/O365 customers were slightly more likely to be "Satisfied/Very Satisfied" (45.3%) with their solution as compared to on-premises companies (38.9%). Interestingly, however, when broken out by role, the more senior roles (technical decision maker, budget owner, and CISO), were much more likely to be either "dissatisfied" or "very dissatisfied" by their email security solution (15.4% compared to 12.0% in general).

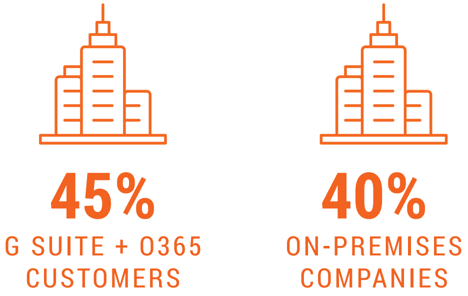
Based on our research, 1 in 5 professionals sees malicious email threats (at least) weekly, so the risk exposure is high. It's no secret that the bad actors are becoming more sophisticated. Even though tech stacks are catching up, information security and IT teams need to be vigilant about reevaluating their email security strategies — from the technologies, user-awareness strategies, and remediation plans—to ensure adequate and holistic protection from email threats.

HOW SATISFIED ARE YOU WITH YOUR CURRENT EMAIL SECURITY SOLUTION?



Source: GreatHorn, "2019 Email Security Benchmark"

SATISFIED/VERY SATISFIED WITH THEIR SOLUTION

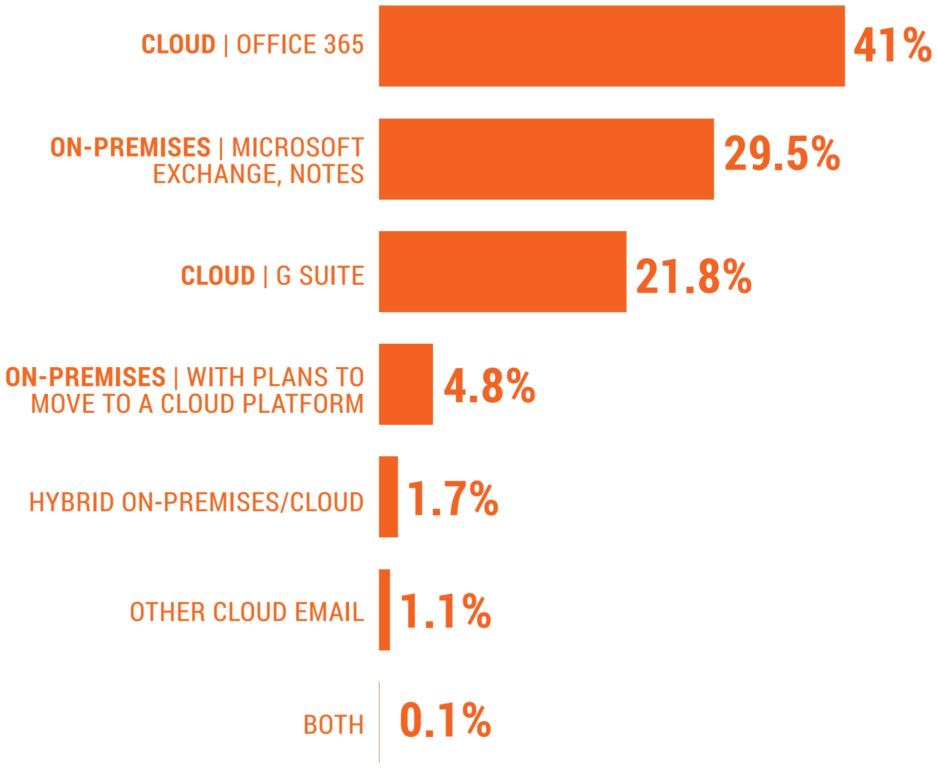


Source: GreatHorn, "2019 Email Security Benchmark"

2019 SURVEY PANEL DETAILS

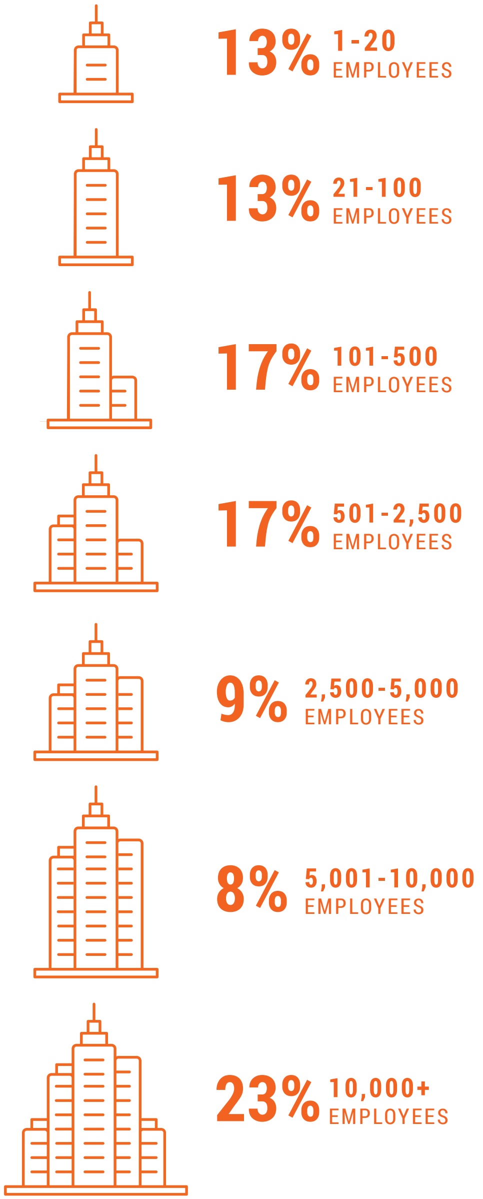
Survey responses from 1,021 professionals were gathered through both offline sources (2019 RSA Conference and the 2019 Gartner Security & Risk Management Summit) as well as online (two panels, one security-focused and one IT-focused, from two different sources). Data was collected between March and June of this year. Respondents were predominantly from North America.

EMAIL PLATFORM



Source: GreatHorn, "2019 Email Security Benchmark"

COMPANY SIZE



Source: GreatHorn, "2019 Email Security Benchmark"

GreatHorn