2020 The Definitive Email Security Strategy Guide

A People-Centric Approach to Stopping Malware, Phishing, and Email Fraud

EXECUTIVE SUMMARY

Email is organisations' most essential business tool—and today's top malware delivery vector.[1] It has become fertile ground for the most damaging cyber threats and all kinds of fraud,[2] the channel where cyber attackers are most likely to compromise their targets. They trick users into clicking on an unsafe link, giving away their credentials, or even unwittingly carrying out attacks themselves (such as wiring money or sending sensitive files).

The threats have changed. Yet much of the cybersecurity sector remains stuck in old threat models, struggling to graft minor improvements onto old strategies that grow less and less effective by the day.

It's time for a new approach. In today's threat landscape, an effective cybersecurity programme focuses on people first.

Measuring, surfacing and reporting user risk

The first step to protecting users is identifying which ones are most at risk. While every organisation may weigh various risk factors differently, all should comprise some combination of vulnerability, attacks and privilege.

Vulnerability is a way of determining who's most likely to fall victim to a threat. An attack analysis can reveal who in your organisation is being targeted, to what extent, and by whom. And privilege can help predict how harmful a successful attack would be to the organisation.

We call users who represent a higher-than-normal risk based on any combination of these factors VAPs, or Very Attacked People™. They should be quickly identified in a way that security teams can use and report to others throughout the organisation when needed.

[1] Verizon. "2019 Data Breach Investigations Report." July 2019.
[2] Proofpoint. "Human Factor Report 2019." September 2019.

Vulnerability: how people work and what they click

Assessing vulnerability that stems from how people work starts with knowing what tools, platforms and apps they use. These may include what cloud apps they use and whether their devices are secure.

The second part of measuring vulnerability is figuring out how susceptible your users are to phishing and other cyber attacks.

Security-awareness training can offer insight into which users are the least prepared to recognise, resist and report cyber threats. In general, users who score poorly on training exercises—or haven't completed them—are more vulnerable than high scorers.

But the true test of users' resilience is how they fare against real-world attack techniques. Simulated attacks, especially those that mimic real-world techniques, can help identify who's susceptible and what tactics they fall for.

Attacks: how people are targeted

Every cyber attack is potentially harmful. But some are more dangerous, targeted or sophisticated than others. That's why measuring this aspect of risk might be trickier than it seems.

Indiscriminate "commodity" threats might be more numerous than other kinds of threats. But they're well understood and more easily blocked.

Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

Knowing the difference is critical to identifying users who are a higher risk. Rich threat intelligence and timely insight are the keys to quantifying who is being targeted and how heavily.

Privilege: what people have access to

Measuring user privilege starts with taking an inventory of all the potentially valuable things people have access to: data, financial authority, key relationships and more.

The user's position in the org chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one.

An administrative assistant might make a more appealing target than a mid-level manager for corporate espionage because the assistant has access to the CEO's calendar. In the same way, a hospital nurse with access to patient records might be a more useful target than the CEO for identify thieves.

Mitigating that risk

Identifying your VAPs is a critical foundation of email security. But it's only a first step. A people-centric approach keeps everyone protected by applying controls that correspond to their level of risk.

Base layer: security for everyone

Because email attacks come in many forms, you need a defence that stops the entire gamut of email threats, not just some of them. Here are the most essential steps to an email defence built for modern threats:

- Stop malware attachments and malicious URLs before they reach users' inbox.
- Stop non-malware impostor threats such as business email compromise (BEC) and other scams, including those coming from compromised email accounts within your own organisation.
- Secure users' web browsing and personal email with web and personal email isolation.
- Make users more resilient with security awareness training.
- Protect data from breaches and insider threats.

VAP layer: adaptive controls for those need more

An effective email security strategy protects everyone. But people-centered protection recognises that some users, your VAPs, need additional security layers and controls. These VAPs may be more vulnerable to falling victim to attacks. They may be more heavily targeted in attacks. They may have high user privileges to sensitive data and systems. Or they may have any combination of the three that results in higher overall risk.

Here are essential controls for users identified as VAPs:

- Targeted security awareness training
- Adaptive, risk-based protections such as step-up authentication, web and URL isolation
- Compromise (takeover) protections for cloud-based accounts

Response: taking effective action when something gets through

When an attack gets through, how quickly you can contain and remediate the damage can mean the difference between a short-lived incident and long-lasting impairment.

At many organisations, incident response can be a slow, labour-intensive process. That's where automation can help.

Effective response processes automate labour-intensive tasks such as correlating and analysing security alerts, verifying indicators of compromise (IOCs), and collecting forensic data. Automation can also help with remediation efforts such as updating firewall and email blocklists, pulling malicious email from inboxes, and restricting account access of affected users.

Used strategically, automation speeds up your incident response and frees up your security staff to focus on things people do best

The upshot

Email is today's most essential business tool—and cyber attackers' preferred threat vector. While email attacks come in varying forms, from diverse sources and with unique objectives, they all have one thing in common: people.

At their core, email attacks are all about getting people to do something that they shouldn't—open a malicious attachment, click an unsafe URL, send sensitive information or wire money to a fraudulent account. That's why securing email requires a people-centric approach.

With the right strategy, tools, insight and training, organisations can manage the risks inherent in email and safeguard their most critical business communications channel.

INTRODUCTION

Email is by far the top threat vector

Every day around the world, the battle for corporate data wages on in one of the most familiar and central features of modern work: the email inbox.

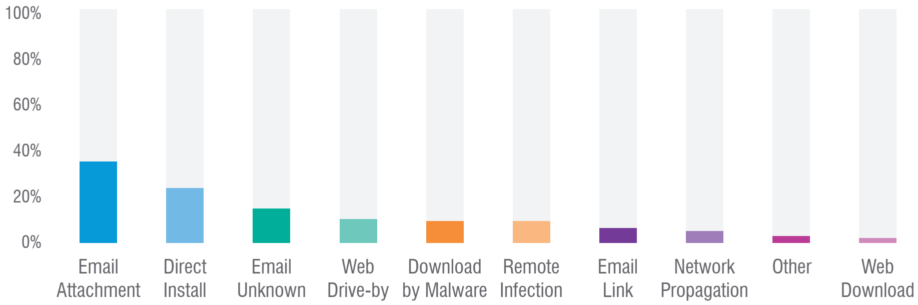
As the top malware delivery vector[3] and fertile ground for all kinds of fraud,[4] email is the channel where cyber attackers are most likely to compromise their targets. They trick users into clicking on an unsafe link, giving away their credentials, or even carrying out commands directly (such as wiring money or sending sensitive files).

It's not hard to see why attackers prefer email. It uses a decades-old architecture that wasn't designed with security in mind. It's universal. And unlike computer hardware and infrastructure, email attacks exploit vulnerabilities that can't be patched—people.

Organisations spend billions every year on security tools designed to harden the network perimeter, detect network intrusions and secure endpoints. But today's attacks hack human nature, not just technology. And email is the easiest way to reach them.

It's time for a new approach. Today's threat landscape calls for a fresh mindset and new strategy—one that focuses on protecting people rather than infrastructure.

Top Malware Vectors



Source: Verizon 2019 Data Breach Investigations Report

Consider this guide a starting point. You'll learn:

- Why email should be your No. 1 security priority
- What makes it so difficult to secure
- How people-centric security is more effective—and more cost-effective—than perimeter-based approaches that are out- of- step with today's people-focused threats.

FAST FACTS

94%

of external cyber threats start with email.[5]

27%

of external attacks resulting in an enterprise breach were carried out using stolen credentials—often obtained with a simple phishing email.[6]

$26 billion

Losses due to business email compromise (BEC) and email account compromise (EAC) scams have reached $26 billion in potential losses worldwide.[7]

90%

of detected malware arrives through email.[8]

47 email fraud attacks

Targeted organisations experienced 47 email fraud attacks on average in Q1 2019 alone.[9]

3X +

The median dollar amount stolen in business email compromise attacks (BEC), a type of email fraud, was $24,439—more than three times as much as the median data breach.[10]

[3] Verizon. *"2019 Data Breach Investigations Report."* July 2019.
[4] Proofpoint. *"Human Factor Report 2019."* September 2019.
[5] Verizon. *"2019 Data Breach Investigations Report."* July 2019
[6] Forrester Research. *"The Forrester Wave Enterprise Email Security, Q2 2019."* May 2019.
[7] FBI. *"Business Email Compromise: the $26 billion scam."* September 2019?
[8] Verizon. *"2019 Data Breach Investigations Report."* July 2019
[9] Proofpoint. *"Proofpoint Quarterly Threat Report Q1 2019."* May 2019.
[10] Verizon. *"2019 Data Breach Investigations Report."* July 2019

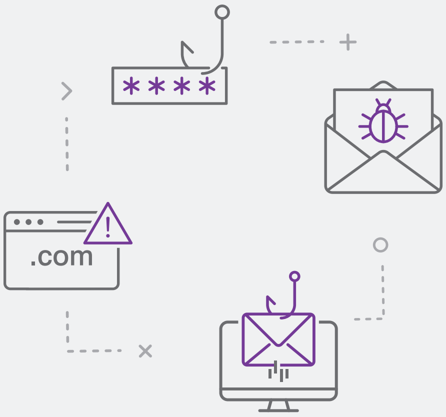
Email attacks are evolving faster than defences

Safeguarding email is the key to protecting the enterprise. But it's a complex challenge.

That's because email threats are numerous and wide-ranging. Attack techniques are constantly evolving. And human nature—the weak link in every organisation—is a perpetual target.

It's no wonder that solutions built for fighting the attacks of just two to three years ago are struggling to keep up.

Tools of the email attack trade



Here are some of the ways cyber attackers target people through email.

Malware: malicious code that infects PCs and servers. It can come as a file attachment, malicious URL link or secondary download by malware already installed on infected systems.

Phishing: malicious emails designed to trick people into doing something the attacker wants. This can include entering account login credentials, sending sensitive information or even wiring money (see "Email fraud" below).

Email fraud: type of phishing designed to trick people into wiring money or sending sensitive information to the attacker. Email fraud doesn't usually involve malware. Instead, it relies on social engineering to persuade the target to act on the attacker's behalf. These attacks typically use misleading display names, domain spoofing or lookalike domains to fool recipients into trusting the sender.

Internal phishing: phishing that uses a compromised email account to target users on the same email domain, typically colleagues. This form of phishing is effective because most organisations don't look for threats originating from their own domain. And recipients assume that email from their colleagues can be trusted.

Personal webmail phishng: attacks that target users through their personal webmail accounts. Many people access their personal email while at work, exposing their employer to threats from this often unprotected vector.

Why you need a people-centric approach

Cyber attackers have shifted their focus from infrastructure to people. The change has rendered the old perimeter-focused approach to cybersecurity—if it ever worked at all—hopelessly obsolete.

That's because there's no longer a perimeter to defend. People are mobile, accessing corporate data from everywhere on all sorts of devices, networks and platforms outside of the traditional corporate network.

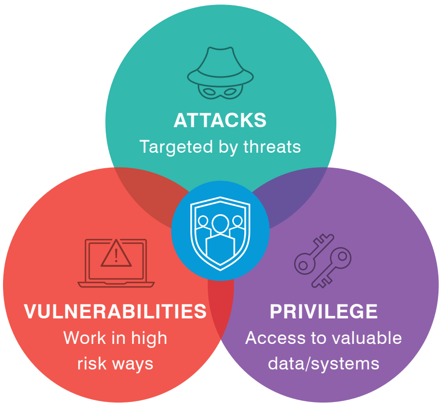
Widespread adoption of the cloud has only accelerated the trend. Even if your cloud infrastructure is secure, the people who use it are only human.

That's why any effective cybersecurity focuses on people first.

The VAP (Vulnerability, Attack, Privilege) model

Just as people are unique, so is their value to cyber attackers and risk to employers. They have distinct digital habits and weak spots. They're targeted by attackers in diverse ways and with varying intensity. And they have unique professional contacts and privileged access to data on the network and in the cloud.

Together, these factors make up a user's overall risk in what we call the VAP Index (measuring vulnerability, attacks and privilege).



Vulnerability

Users' vulnerability starts with their digital behaviour—how they work and what they click. They may access company email through unmanaged personal devices. They may use cloud-based file storage and install third-party add-ons to their cloud apps. Or they may be especially receptive to attackers' email phishing tactics.

Attacks

Today's cyber attacks are unrelenting, come in many forms, and are always changing. It's critical to understand not just who in your organisation is being targeted, but how, by whom and whether the attack is part of a larger campaign. A user targeted by a few highly advanced threats, for example, can pose more of a risk than someone on the receiving end of a broad, indiscriminate attack campaign.

Privilege

Privilege measures all the potentially valuable things people have access to, such as data, financial authority, key relationships and more. Measuring this aspect of risk is key because it reflects the potential payoff for attackers—and harm to organisations if compromised.

Measuring, surfacing and reporting user risk

The first step to protecting users is identifying which ones are most at risk. While every organisation may weigh various risk factors differently, all should comprise some combination of vulnerability, attacks and privilege.

Vulnerability is a way of determining who's most likely to fall victim to a threat. An attack analysis can reveal who in your organisation is being targeted, how heavily and by whom. And privilege can help predict how harmful a successful attack would be to the organisation.

We call users who represent a higher-than-normal risk based on any combination of these factors VAPs. They should be quickly identified in a way that security teams can use—and report to others throughout the organisation when needed.

This level of visibility in all three areas is essential to people-centric security. Without it, organisations have no way of knowing who needs additional layers of security or how best to protect them.

Vulnerability: how people work and what they click

Quantifying vulnerability isn't easy with traditional technology-focused security tools. But with a people-centric approach, you can measure: how they work and what they click.

How they work encompasses the tools, systems and platforms they use to do their job. What they click is a measure of their security awareness and propensity to fall for likely threat tactics.

How your people work

Assessing vulnerability that stems from how people work starts with knowing what tools, platforms and apps they use. These include:

- What cloud apps they use
- How many and what devices they use to access email
- Whether those devices are secure
- Whether the user practices good digital hygiene
- Whether they use multifactor authentication consistently

The more granular your visibility, the better.

What your people click

The second part of measuring vulnerability is figuring out how susceptible your users are to phishing and other cyber attacks.

Security-awareness training, an essential part of any effective security strategy, can offer insight into which users are the least prepared to recognise, resist and report cyber threats. In general, users who score poorly on training exercises—or haven't completed them—are more vulnerable than high scorers.

But the true test of users' resilience is how they fare against real-world attack techniques.

Short of letting attackers in and seeing who opens a malware file or wires money to an attacker (not ideal for obvious reasons), phishing simulations are the best way to gauge this aspect of vulnerability.

Simulated attacks, especially those that mimic real-world techniques, can help identify who's susceptible and to which tactics. Someone who opens a simulated phishing email and opens the attachment might be the most vulnerable. A user who ignores it would rank somewhat lower. And users who report the email to the security team or email administrator would be deemed the least vulnerable.

Attacks: how people are targeted

Every cyber attack is potentially harmful. But some are more dangerous, targeted or sophisticated than others. That's why measuring this aspect of risk might be trickier than it seems.

Indiscriminate "commodity" threats might be more numerous than other kinds of threats. But they're well understood and more easily blocked.

Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

Knowing the difference is critical to identifying users who are a higher risk. Rich threat intelligence and timely insight are the keys to quantifying who is being targeted and how heavily.

The factors that should weigh most heavily in each users' assessment include:

- The cyber criminal's sophistication
- The spread and focus of attacks
- The attack type
- Overall attack volume

You should also weigh these factors in context of what departments, groups or divisions the individual user belongs to.

For instance, some users might seem not at risk based on the volume or type of malicious email sent to them directly. But they may actually represent a higher risk because they work in a highly attacked department—and are therefore more likely to be a key target in the future.

Privilege: what people have access to

Measuring user privilege starts with taking an inventory of all the potentially valuable things people have access to: data, financial authority, key relationships and more.

Users with access to critical systems or proprietary intellectual property, for instance, might need extra protection, even if they aren't especially vulnerable or aren't yet on attackers' radars.

The user's position in the org chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one.

An administrative assistant might make a more appealing target than a mid-level manager for corporate espionage because the assistant has access to the CEO's calendar. In the same way, a hospital nurse with access to patient records might be more useful target than the CEO for identify thieves.

For attackers, a valuable target can be anyone who serves as a means to their end.

I know who my VAPs are—now what? People-centric security in action

Identifying your VAPs is a critical foundation of email security. But it's only a first step. A people-centric approach keeps everyone protected by applying controls that correspond to their level of risk.

Base layer: security for everyone

Email security starts with robust protection for every user. Because email attacks come in many forms, you need a defence that stops the entire gamut of email threats, not just some of them. Here are the most essential steps to an email defence built for modern threats:

Stop malware attachments and malicious URLs before they reach users' inbox.

Most cyber attacks rely on the intended victim doing something—in many cases, opening an attachment or clicking a URL. But these human-activated attacks can't succeed if the intended victim never sees the message.

That's where a secure email gateway comes in. By stopping malware threats before they reach users' inbox, your gateway can protect organisations from a wide range of malware threats, including ransomware, banking Trojans, remote-access Trojans, information stealers, downloaders, botnets and more.

Stop non-malware impostor threats

Stopping malware threats is critical, but some of the most damaging email attacks don't use malware at all. Instead, they rely on social engineering.

Business email compromise (BEC), a type of wire-transfer fraud, is one example. BEC has led to more than $26 billion in potential losses since 2016, according to the FBI. The law-enforcement agency says BEC attacks been reported in all 50 states and 177 countries, with fraudulent transfers sent to at least 140 countries.[11]

In BEC and other non-malware attacks, the scammer impersonates someone the recipient can trust using a spoofed, compromised or lookalike email account. Under that false identity, the attacker asks the victim to do something on the attacker's behalf—say, wire money to an overseas bank account, send sensitive files and more.

Impostor threats are a complex problem with many facets. To stop them, you need a layered defence that secures inbound, outbound and internal email—and works in a holistic, cohesive way.

Along with user training and other security controls described in this this section, here are key elements of an impostor email defence.

RECENT BEC AND EAC SCAMS

Here are high-profile victims of recent BEC and EAC attacks.

"Shark Tank" host Barbara Corcoran:

$400,000

Government of Puerto Rico:

$4 million

Nikkei America:

$29 million

Red Kite Community Housing:

$1.2 million

Manor (Texas) Independent School District:

$2.3 million

Toyota Boshoku:

$37 million

Cabarrus County, N.C.:

$2.5 million

Ocala, Fla.:

$750,000

Rijksmuseum Twenthe (museum):

$3.1 million

[11] FBI. *"Business Email Compromise: the $26 Billion Scam."* September 2019.

DMARC

Deploy DMARC email authentication. DMARC is an internet-wide policy that validates that the email sender is who they say they are and that they're authorised to send on the organisation's behalf.

With DMARC, you get visibility into all the email being sent using your email domain, including trusted third-party senders such as Marketo, Salesforce or SurveyMonkey. With this visibility, you can authorise all valid senders trying to send email on your behalf—and block anyone using your trusted domains to steal money or hurt your brand.

Dynamic classification

While DMARC can help stop threats that spoof your domain, attackers use other techniques to trick users. That's why another critical component of stopping non-malware threats is dynamically analysing and classifying the content of the emails. This aspect of email security is all about parsing what's in the email, not just where it comes from. That's why you need email security can look for telltale signs of fraud and block or further study anything that looks unsafe. Dynamic classification analyses and manages email based on several factors, including:

- The email's content, header and IP address
- The sender's reputation
- The relationship between the sender and recipient

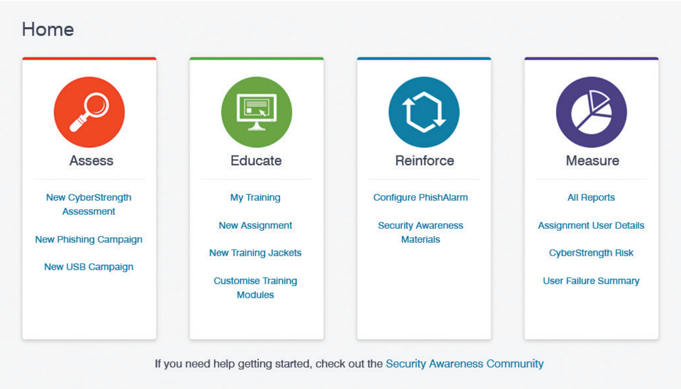
Internal email defence

In some cases, attackers don't try to disguise their email address at all—they just take over a legitimate account. Email account compromise (EAC) can be used in a wide range of attacks, but it's especially potent impostor tactic. That's because:

- Most organisations don't subject internal to the same levels of scrutiny and security controls as external email
- Most users inherently trust email from people they know
- Attackers who take control over an account have access to a trove of information about the compromised user—who they correspond with, what they discuss and even their writing style. These details make the impersonation especially convincing.

Make users more resilient with security awareness training

Cyber attackers have grown ruthlessly effective at exploiting human nature with convincing spoofing techniques, attention-grabbing subject lines, and hard-to-resist calls to action. As we detail in our **2019 Human Factor** report, the most effective phishing emails were clicked 1.6 times—meaning some of the emails were clicked not just by the recipient but forwarded and clicked by others.[12]



If you need help getting started, check out the Security Awareness Community

Protect data from breaches and insider threats

No email defence can stop every threat. And even among the best-trained workforce, some users may fall for targeted social engineering attacks.

That's why every email defence should include data loss prevention (DLP) tools, including encryption. Even when something goes wrong, a fast response and DLP ensures that the attack doesn't spread and that attackers don't get your most sensitive data.

DLP is also a useful defence against insider threats. No one likes to think of their colleagues as a potential security foe. But insider threats—including workers who are careless, criminal or compromised—caused an average of $8.76 million in damage in 2018.[13]

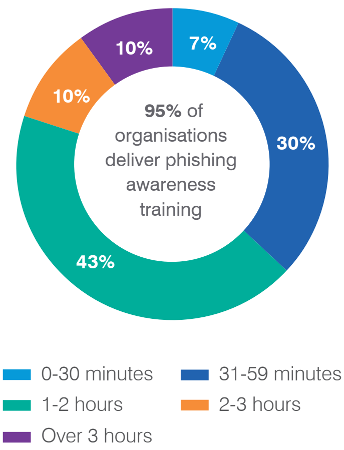
Whether data exits your environment through an external breach or insider attack, DLP helps keep it secure.

[12] Proofpoint. *"The Human Factor 2019."* September 2019.
[13] Ponemon Institute. *"2018 Cost of Insider Threats: Global."* April 2018.

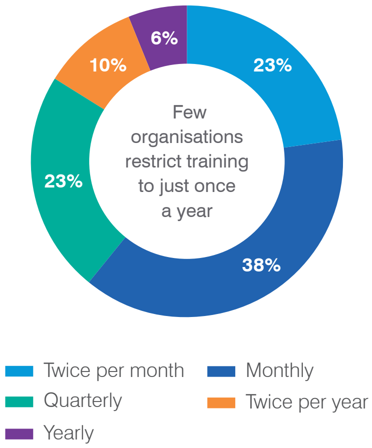
FOREWARNED AND FOREARMED

Here's how organisations are deploying security awareness training programmes.

Time Allocated to Security Awareness Training Each Year



Frequency of Security Awareness Training



Adaptive layer: controls for VAPs

An effective email security strategy protects everyone. But people-centered protection recognises that some users, your VAPs, need additional security layers and controls. These VAPs may be more vulnerable to falling victim to attacks, more heavily targeted in attacks, have high user privileges to sensitive data and systems—or any combination of the three.

Targeted security awareness training

Company-wide security awareness training is useful for revealing vulnerabilities and reducing your human attack surface. Beyond shoring up obvious gaps, targeted training can also be a helpful preventative measure for all VAPs, not just those who rank high on the vulnerability component.

Users identified as VAPs because of their attack profile, for instance, can get training on the very threats that are targeting them. And users with high privileges can get extra training related to attack campaigns targeting the data they have access to.

Adaptive, risk-based protections

Applying the most stringent security controls to all users all of the time just isn't practical for most organisations. It could even backfire. Needlessly tight controls can hinder users' productivity and might drive them to turn to security workarounds just to do their job.

But sometimes, that extra layer of security is necessary. A frontline worker might be especially prone to an attack making the rounds in your industry. A researcher might be targeted by an especially sophisticated attacker. Or a CEO, because of the nature of the job, might have access to the organisation's most sensitive data.

In some cases, you might step up authentication requirements. In other cases, you may need to use web isolation for any URLs the user clicks from email.

Whatever form they take, the key to adaptive protections is a having a timely picture of the VAP-related risk factors and applying controls that are proportional to those risks.

Account protections for cloud-based accounts

Email account compromise (EAC), especially for cloud-based accounts, is fast becoming a preferred attack vector. To a cyber criminal, a compromised account is practically a license to steal.

A compromised email account can be used in all sorts of malicious ways. By gaining control of the right account, the intruder can move laterally within your environment, steal data or dupe your business partners and customers. That's why protecting mail accounts, especially cloud-based accounts, is critical.

Compromising situation: how attackers take over cloud-based accounts

In email account compromise, the email account doesn't just *seem* legitimate—it's the real thing. Here are a few ways attacks can gain control over your users' account.

Brute-force attacks. The attacker, usually through an automated script, ttries a username/password combination across many accounts until one works.

Breach replay attack. It's a bad practice, but many people use the same password for multiple accounts. If one of those passwords is leaked in an unrelated data breach, any other account with the same username (often an email address) and password is at risk.

Phishing. Old-fashioned credential phishing remains an effect way to get a victim's password. Without additional controls such as multi-factor authentication (MFA), lost credentials can lead to compromised accounts.

Response: taking effective action when something gets through

Security incidents are inevitable. But they don't have to be catastrophic.

When an attack gets through, how quickly you can contain and remediate the damage can mean the difference between a short-lived incident and long-lasting impairment. That's why a vigorous response framework is a key part of every people-centric security posture.

At many organisations, incident response can be a slow, labour-intensive process that includes:

- Investigating and verifying the incident
- Containing the threat
- Determining the cause and scope
- Remediating infected systems

All of these steps are critical to an effective response. But as security leaders know all too well, performing them manually doesn't scale. That's where automation can help.

Effective response processes automate labour-intensive tasks such as correlating and analysing security alerts, verifying indicators of compromise (IOCs) and collecting forensic data. Automation can also help with remediation efforts such as updating firewall and email blocklists, pulling malicious email from inboxes, and restricting account access of affected users.

Used strategically, automation speeds up your incident response and frees up your security staff to focus on things people do best— understand, prioritise and respond to real security threats.

Checklist: what to look for in a security solution

The cybersecurity industry is slowly coming around to the idea that today's attacks target people, not technology. But people-centric security is more than a marketing buzzword—it's a fundamentally new way of looking at threats and how to stop them.

Here's a checklist of what to ask for in people-centric security solutions.

Effective email security for all users

The best way to thwart email attacks is stopping them before they reach the inbox. Look for a solution that can recognise and block a wide range of attacks and tactics, including:

- Malware-based attacks that use attachments and URLs
- Non-malware attacks such as BEC
- EAC and cloud-account takeovers

People play the biggest role in today's email attacks. That's why security awareness training should be a key part of your email security strategy. Make sure your training programme includes the following:

- Training based on proven methodologies and real-world attacks
- Phishing simulations informed by real-world campaigns to train users on the threats they're most likely to face
- Targeted follow-up training for users who exhibit critical gaps or vulnerabilities

To secure data that is stolen, mistakenly shared or maliciously exposed by an insider, encryption and other DLP measures are critical. Effective DLP can:

- Analyse email content in detail and, when needed, block parts of outgoing email and similar content from being sent.
- Identify and protect all standard forms of restricted content, such as PCI, HIPAA, FINRA and other regulated material
- Automatically reroute, encrypt or reject emails that violate security and other policies and alert the appropriate people within your organisation

Adaptive controls for VAPs

Higher-risk users—based on their vulnerability, attack profile and privilege—require additional security controls. A people-centric email security solution helps you identify those VAPs and protect them with extra layers of security. Look for a solution that:

- Gives you actionable visibility into your VAPs informed by rich, timely threat intelligence and deep insight into users' risk profile
- Offers reporting tools that makes it easy to surface and communicate users' vulnerability, attack profile and privilege, with departmental and industry comparisons
- Automatically responds to changing user risk profiles with step-up authentication, reduced privileges, URL isolation and more

Fast, effective response when something gets through

Automating key parts of the incident response process can help streamline critical labour-intensive tasks and free up responders for higher-level activities. Look for automated response tools that:

- Verify threats, identifies affected users, and collect forensics data and context around those users
- Enrich threat alerts with actionable intelligence
- Contain and remediate threats and re-authenticate accounts across the environment, in the cloud and on premises

Learn more

To learn more about how you can take a people-centric approach to email security, visit **www.proofpoint.com/uk/products/email-protection/email-security-and-protection**.

LEARN MORE

For more information, visit **proofpoint.com/uk**