proofpoint.

eBook

Reimagining Email Security

Protecting with People-Centric Email Security in the Cloud Era

Introduction

We send 102.6 trillion emails every year[1]. For organisations, it is the fundamental feature of modern business—and the number one threat vector. Everyday emails containing invoice payment requests from suppliers, communications with investors and other formal and informal correspondences outside of the network are all fertile ground for exploitation and fraud.

While email is a time-tested technology, the world and infrastructure around it has changed. And now, so should its protection.

As the great cloud migration continues, perimeter-based defences have become obsolete. The vast majority of threats aren't entering protected environments from breached firewalls. Instead, along with businesses, attackers have shifted to the cloud. And as employees work from anywhere and on any device, cyber criminals are blending both email and cloud vectors for financial gain.

In the changing landscape, security and risk management leaders like you must ensure that existing security solutions keep pace with fast-changing threats. It's clear that the defend-the-perimeter model of security hasn't worked for years and it's time to make a change—and today that means starting protection with people.

To help you reimagine email security in the context of modern threats, this e-book explains:

- The current state of business email
- How the shift to cloud has introduced new security challenges
- The top email threats businesses need to protect against
- Why a people-centric approach to email security is the key to protection

#1 Threat Vector:
More than 90% of cyber attacks start with email

[1] Statista. "Number of Sent and Received E-mails Per Day Worldwide from 2017 to 2025." February 2021

The Current State of Business Email

2020 saw a significant shift to remote workforces, which continued to fuel the adoption of cloud office systems.

New Security Challenges in the Cloud Era

71%
of companies use cloud or hybrid cloud email[2]

73%
of the time, cloud breaches involved an email or web application server[3]

77%
of those cloud breaches also involved breached credentials[4]

Massive Amounts of Malicious Messages in 2020

Attackers use the same cloud infrastructure as businesses to complete their attacks.

Proofpoint observed:

Nearly 60M
sent or hosted by Microsoft Office 365

>90M
sent or hosted by Google[5]

Compromising Cloud Accounts Give Attackers an Advantage

Because:

It is faster and easier to compromise users rather than infrastructure

They gain access to email

It is an entryway to: contacts, file repositories, calendars, and more

[2] Gartner. "Market Guide for Email Security." September 2020
[3] Verizon. "2020 Data Breach Investigations Report." 2020
[4] Verizon. "2020 Data Breach Investigations Report." 2020
[5] Proofpoint Research. 2020

The Ever-Evolving Threat Vector

The adoption of cloud office systems wasn't the only change in 2020. Mobile device prevalence was also on the upswing.

Cloud Isn't the Only Shift: Now More Email on Mobile Devices

The traditional 9-to-5 work schedule at an office desk is a thing of the past. To adjust to the free-flowing, time exempt nature of today's work, people are now power users of mobile email.

Mobile email presents new challenges for defenders:

- On a mobile native email client, a reporting button cannot be installed
- It has an inconsistent user experience
- It lacks user reinforcement
- Has less ability to warn users of malicious emails

Time to Rethink Protection

Past:

Protect Email

Present:

Protect Email AND Cloud

Protecting Against the Email Threat Trifecta

The popularity of cloud email continues to grow. Now we're at a critical tipping point as threats evade detection by common email security technologies that rely on standard antivirus and reputation. Because of this, a layered security approach is no longer optional if you want to be protected. However, it is often a challenge to source a technology that keeps pace with attackers, especially as they blend email and cloud attacks to increase chances of success:

Threat #1: Ransomware

Ransomware is a type of malicious software (malware) that threatens to publish or block access to data or a computer system, usually by encrypting it, unless the victim pays a ransom to the attacker.

While ransomware is an old tactic, it remains a top concern as the danger grows in scale. Instead of holding a single laptop or device for ransom, attackers now go after the entire organisation, bringing business to a halt. They deliver ransomware through a multi-stage attack with the first stage payload most often delivered through email.

Threat #2: Phishing

Phishing attacks deliver malicious emails designed to trick people revealing financial information, credentials or other sensitive data. Today, broad-based attacks continue to threaten organisation as attackers adopt themes related to the pandemic to dupe recipients.

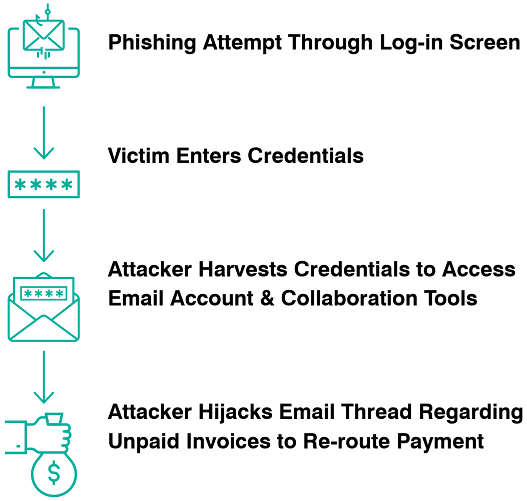
Threat #3: Business Email Compromise (BEC)

As one of the fastest growing email security threats, BEC is an attack that does not use malware or malicious links, but instead misleads a victim into diverting funds to the cyber criminal's account. Common types of BEC scams include supplier invoicing fraud, payroll re-directs and gift card scams. In 2019, there was nearly 100% increase in BEC attacks in 2019[8] and in 2020 BEC /Email Account Compromise (EAC) ranked as the top crime type for losses, equating to $1,866,642,107[9], or 44% of all business and consumer losses that year.

In 2020, **2/3** of organisations experienced a ransomware attack.[6]

Phishing and credentials are threat actors' currency: **57%** of organisations experienced a successful phishing attack in 2020, up from **55%** in 2019.[7]

Visualising Blended Attacks



Phishing Attempt Through Log-in Screen

Victim Enters Credentials

Attacker Harvests Credentials to Access Email Account & Collaboration Tools

Attacker Hijacks Email Thread Regarding Unpaid Invoices to Re-route Payment

[6] Proofpoint. "2021 State of the Phish Report." January 2021
[7] Proofpoint. "2021 State of the Phish Report." January 2021
[8] Gartner. "Protecting Against Business Email Compromise Phishing." March 2020
[9] FBI. "2020 Internet Crime Report." 2020

People are the New Perimeter

Cyber attackers shifted their focus from infrastructure to a more profitable option at the same time the cloud-enabled workforce rendered perimeter security obsolete. Because of these converging trends, the new model of cybersecurity starts with a new perimeter—people.

It's people that ransomware, phishing, and BEC attacks all have in common. Adversaries know that when businesses shift to secure cloud infrastructures, the one thing that doesn't change is our human nature. With people often the most vulnerable, cyber criminals use attacks that rely on employees opening a weaponised document, clicking a malicious link, entering their credentials or even carrying out demands like wiring money.

More than **99%** of today's cyber attacks are human-activated.[10]

Defending Your Critical Security Layer

To protect against attacks targeting people, you need to first start with visibility into your human attack surface so you know who is posing a risk to your organisation.

Do you know:

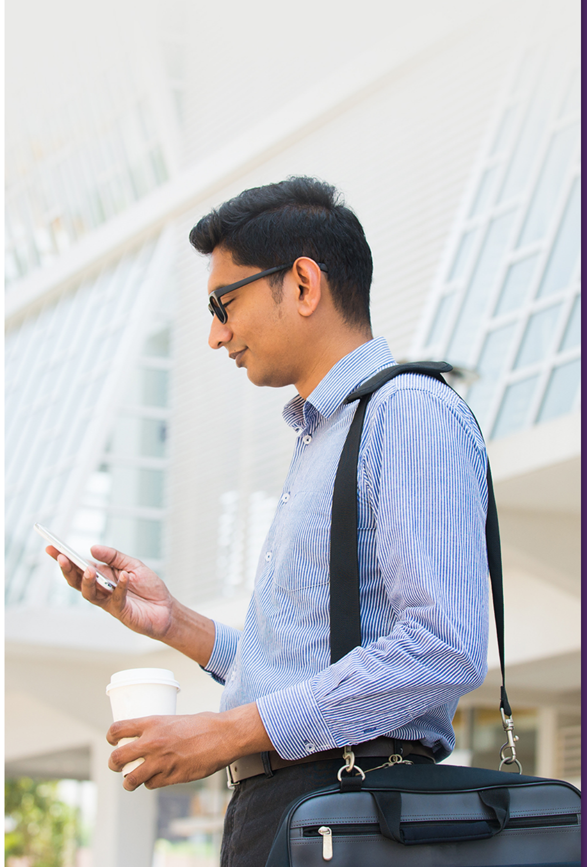
- Who your Very Attacked People™ (VAPs) are?
- How they are being targeted?
- Who are vulnerable to these threats?

Along with actionable visibility, effective email security uses a cohesive, synchronous approach that encompasses all layers that attackers use to exploit:

- Email – detect and remediate email threats
- Cloud – detect and remediate compromised employee accounts
- Users – train and engage based on threats they receive
- Suppliers – detect compromised supplier accounts that might be sending your people threats

Why People?

- People are much easier to compromise with deception and social engineering
- People have a difficult time spotting malicious emails given the chameleon nature of attacks
- People place too much trust in the identities of incoming emails



[10] Proofpoint. "The Human Factor Report." 2019

Reimagine Siloed Defence Into An Integrated Threat Protection Platform

In light of modern email threats that employ multiple tactics and combinations of impersonation and account compromise, defending against one or two tactics alone leaves businesses vulnerable to attacks that exact a heavy toll. You have to take a fundamentally different approach to how you view threats and design your protections to stop them.

The only way to safeguard people from the social engineering tactics targeting them, or to defend your organisation from threats, is to secure with an integrated threat protection platform.

The Proofpoint Threat Protection Platform is the robust, people-centric solution that your business needs to defend against and respond to threats quickly and effectively when something goes wrong. By analysing billions of messages and millions of cloud accounts each day, Proofpoint is always monitoring more threats—allowing us to assess, learn and adapt our defences against emerging threats and even hard-to-detect malwareless threats, such as BEC.

We have always advocated for people-centric security that protects your people from the threats that target them. With Proofpoint you can fill your cybersecurity gap and:

- Stop the vast majority of threats, including phishing, ransomware, and BEC/email fraud before they arrive in your user's inbox
- Gain visibility into your most attacked people, with actionable insights and forensics details of an attack
- Educate users with threat-intel driven training so they're less vulnerable to attacks
- Automated remediation of email threats and cloud account takeover

Take the next steps to securing your organisation from the number one threat vector.

Learn more

proofpoint.