proofpoint.

2020 Stopping BEC and EAC

The Modern CISO's Guide to Protecting People with Proofpoint Email Security

Business email compromise (BEC) and email account compromise (EAC) are complex problems that require multi-layered defenses. Cyber attackers have countless ways of tricking your users, preying on their trust and exploiting their access to key data, systems and resources.

To succeed, attackers need to find just one tactic that works. That's why you must block all of them, not just some of them.

Here's a closer look at how Proofpoint Email Security safeguards your people from BEC and EAC attacks—and why it is the only solution that truly solves these growing problems.

Introduction

BEC and EAC are fast-growing problems with no easy solution.

That's because no two BEC or EAC scams are alike. While they all follow similar playbooks, each attack is as unique as the people they target, the personality traits they prey on, and the trust relationships they exploit.

They start with a seemingly routine email request from a boss, colleague or business partner. "Wire money to this account." "Send the payment here." "Attach employee files."

BEC and EAC defined

But in BEC and EAC attacks, the requests don't come from the person they appear to be from. Instead, they're from an impostor using a lookalike email address—or in some cases, the impersonated sender's own email account.

According to the FBI, BEC and EAC attacks have cost businesses upwards of **$26 billion** worldwide since 2016 in exposed (actual and potential) losses.[1] The average attack nets the attacker nearly **$130,000**.[2]

Gartner predicts that BEC attacks will double each year, totaling **$5 billion** in actual losses by 2023.[3]

EAC, also known as email account takeover, is often associated with BEC because compromised email accounts are used in a growing number of BEC-style scams. (EAC is also the basis of other kinds of cyber attacks). The FBI started to track them together in 2017.

The mounting toll

EAC is accelerating in an era of cloud-based infrastructure. A recent Proofpoint Threat Research study reveals that 40% of organizations using the cloud had at least one compromised account.

And even as organizations fend off inbound BEC attacks, cyber criminals may be using their trusted domain to launch outbound attacks against business partners and customers. These attacks can strain business relationships and leave respected brands tarnished.

Stopping BEC and EAC requires a multilayered defense that blocks every tactic attackers use—not just some of them.

Here's a closer look at how Proofpoint Email Security safeguards your people from BEC and EAC attacks—and why it is the only solution that truly solves these growing problems.

The average attack nets the attacker nearly

$130,000.

[1] FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.

[2] Darla Mercado (CNBC). "New online financial scam costs victims $130K per attack." February 2018.

[3] Gartner Research. "Protecting Against Business Email Compromise Phishing." March 2020.

Why BEC and EAC are so hard to stop

BEC attacks are difficult to detect because they don't use malware or malicious URLs that can be analyzed with standard cyber defenses. BEC attacks rely instead on impersonation and other social engineering techniques to trick people interacting on the attacker's behalf. That may include sending sensitive information, wiring money, diverting payroll and more.

Because of their targeted nature and use of social engineering, manually investigating and remediating these attacks is difficult and time consuming.

BEC attacks use a variety of impersonation techniques, such as:

- **Domain spoofing.** The attacker forges the sender address (the "MAIL FROM" or "return-path" field in an email) using a trusted domain. The recipient sees the forged address rather than the sender's actual domain.
- **Lookalike domains.** To get around domain-spoofing measures, attackers often register a domain that resembles the one they're trying to impersonate. The domain might use the numeral "0" instead of the letter "O," for example (y0urcompany.com).
- **Display-name spoofing.** Email senders can easily set their display name to anything they want. Many mobile email clients show only the display name by default, especially on mobile devices, making this a simple but effective technique. Most BEC attacks use display-name spoofing alongside other spoofing methods.

These attacks are effective because domain misuse is a complex problem. Stopping domain spoofing is hard enough—anticipating every potential lookalike domain is even harder. And that difficulty only multiplies with every domain of an outside partner that attackers can used in a BEC attack to exploit your users' trust.

In EAC, the attacker gains control of a legitimate email account, allowing them to launch similar attacks. But in these cases, the attacker isn't just trying to pose as someone—for all practical purposes, the attacker is that person.

Because BEC and EAC focus on human frailty rather than technical vulnerabilities, they require a people-centric defense that can prevent, detect and respond to a wide range of BEC and EAC techniques.

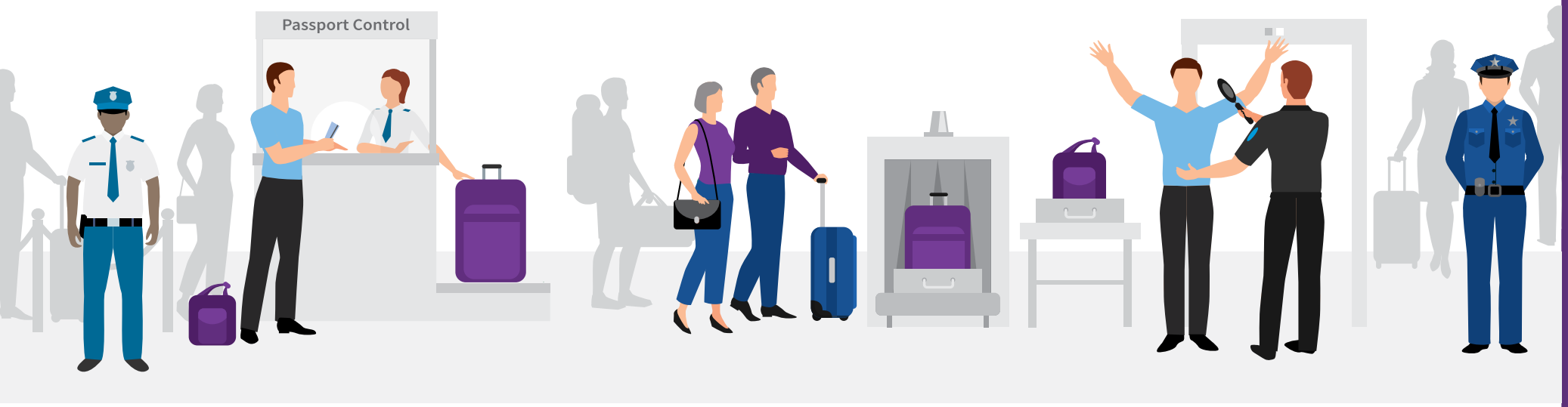
BEC and EAC focus on **human frailty** rather than **technical vulnerabilities**

Air Travel as an Analogy

Consider how airports manage a vast and changing mix of potential security issues. Most take a multipronged approach, each element featuring multiple checks and procedures.

- **Passport control.** Checks traveler's passport (or driver's license) and boarding pass to ensure they are 1) who they claim to be and 2) authorized to fly.
- **Screening.** Scans the luggage and passengers to ensure that nothing bad is getting on the plane—and that nothing's leaving that shouldn't be.
- **TSA agents.** Trained to spot and report suspicious traits and behavior.
- **Airport security.** Armed with the authority and means of physically stopping bad actors and separating them from anyone they might harm.
- **Law enforcement.** Aware of outside activity that may put travelers at risk, including identity theft, forged passports and coordinated criminal activity. Helps create no-fly lists, alerts airport security about potential threats and catches many criminals before they enter the airport.

At Proofpoint, we take a similar approach to securing your email. Here's how our email security solution secures every avenue an attacker might take in a BEC/EAC attack.



Authentication (passport control)

One of the first security measures travelers face when traveling internationally is having their identification and boarding passes checked. It's one of the most fundamental steps airport security can take to ensure that the traveler is who they say they are and are authorized to fly.

Many BEC attacks use email domain spoofing. The attacker piggybacks a trusted domain to pose as someone the recipient trusts. The impostor forges the email address of the person being impersonated so that the recipient—even those savvy enough to check the Return-path field in the email header—can't tell the difference.

That's why deploying an email authentication framework such as DMARC (Domain-based Message Authentication, Reporting and Conformance) is critical. With DMARC, you can protect your email domain from scammers looking to use it for spam, phishing and BEC attacks.

With our email authentication solution, we give you the visibility, tools, and services to authorize legitimate email and block fraudulent messages before they reach the inbox.

We help you:

- View all inbound impostor threats—such as display name spoofing and lookalike domain spoofing attacks—and block them at the Proofpoint gateway
- Enforce DMARC authentication quickly and confidently to block fraudulent emails that spoof trusted domains
- Automatically identify and flag lookalike domains that are registered by third parties and are outside of your control

Email gateway (screening)

At airports, passenger and luggage screening can feel like a major annoyance. But they're vital to keeping other passengers safe. With proper screening, airports can ensure that nothing unsafe is getting on the plane.

Email gateways perform a similar function in cybersecurity. Most gateways scan email in search of malware and unsafe URLs. This security layer is important for stopping account takeover in an EAC attack. But BEC and EAC also rely on social engineering, not malware and malicious links. So often, there's no attachment or URL to analyze.

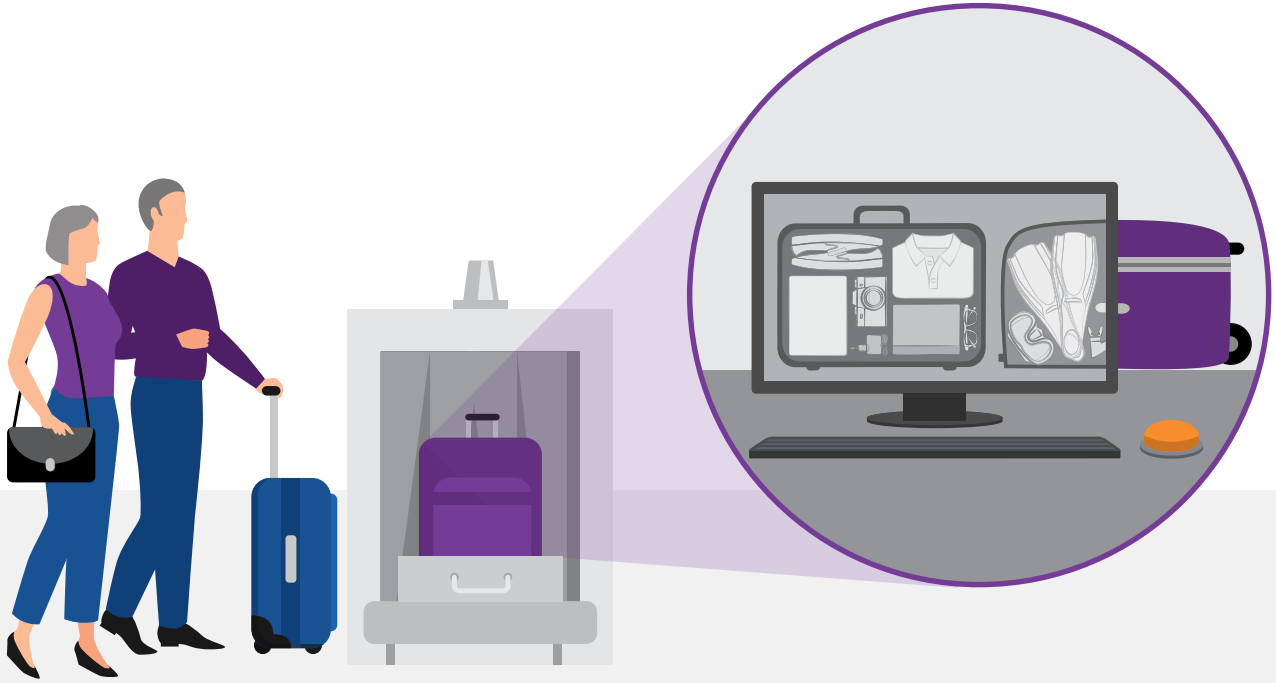
To stop BEC and EAC attacks, email gateways must go a step further and analyze the content and context of each email sent.

Our email security solution identifies malicious URLs and attachments that could lead to compromised accounts. We also scan incoming email to look for signs of social engineering and fraud. Our dynamic classification engine analyzes and manages email based on several factors, including:

- The email's content
- The sender's reputation (based on the IP address in the email header)

We typically look at several factors. Does the email come from a trusted sender—and does that sender have a good reputation? Does the email include a suspicious subject? Do the sender and the receiver have an existing email relationship? Does the body of the email look suspicious?

We score each email based on its level of riskiness. Then you can decide what to do with it according to that score—let it through, block it or route it to a quarantine folder.



Security-awareness training (TSA agents)

Airport body scanners, chemical detection, facial recognition and other technological improvements have made flying safer. But they all need well-trained people to operate the machines, interpret the results and know what to do with them.

The role of people is even more acute in cybersecurity, especially in BEC and EAC. That's because these attacks target people. They exploit human frailties. And they don't work if people don't fall for them.

With security-awareness training, we help turn your users into a strong last line of defense by:

- Teaching users to recognize, reject and report suspicious emails
- Revealing user vulnerabilities, showing which users are most vulnerable and the BEC/EAC tactics they're most likely to fall for
- Targeting training to those who need it based on where they're most vulnerable, how they are being targeted in attacks, and their access privileges to key data, systems and resources

Our security awareness training modules are informed by rich, timely threat intelligence, so they reflect the latest real-world attack tactics and techniques. And reporting BEC/EAC attempts is easy with our PhishAlarm button for Microsoft Outlook users and PhishAlarm analyzer for security teams. Both tools are part of suspicious email reporting system that helps streamline both BEC/EAC reporting and remediation.

Threat response (airport security)

Even with the most advanced tools and best-trained people, things can go wrong. That's why most airports have on-site security. These armed officers help deescalate high-risk situations, arrest anyone who poses a threat, and detain or remove them from the premises.

Our threat-response automation capabilities serve a similar role in combating BEC and EAC by orchestrating and automating key parts of the incident response process. Here just a few of the actions you can set to happen automatically when a BEC or EAC attempt reaches a users' inbox:

- Pull phishing emails that contain URLs that become unsafe after being delivered—along with any copies that have been forwarded to other users
- Remove unwanted email from internal accounts that have been compromised
- Quarantine potential impostor emails reported by users
- Force password resets
- Suspend compromised accounts
- Revoke any active user's session
- Enforce risk-based authentication

We help you quickly contain and remediate BEC and EAC threats to avoid the worst effects of a successful attack.

Cloud-account defense (law enforcement)

Sometimes, stopping threats to air travel requires insight that extends beyond the airport boundaries. That's where outside law enforcement comes in. Local police, the FBI, U.S. Department of Homeland Security and other agencies can stop the threat and alert airport officials of criminal activity that occurs outside of the airport that could hurt traveler safety.

The same is true of EAC attacks. In EAC, the cyber criminal takes over the account of a legitimate user. Because the account is real, recognizing it as a threat is difficult for even the best-trained users and most advanced email gateways—assuming that the organization is scanning internal email at all.

Our cloud security is a police force for EAC attacks. It detects when a cloud-based email account has been compromised. It alerts your security team. And it takes steps to remediate the account before the attacker has a chance to misuse it.

We use the latest threat intelligence and powerful forensics to correlate outside threats, account behavior and user context. It connects the dots between:

- Account activity—unusual actions such as suddenly BCCing emails in bulk or setting up calendar-forwarding rules
- Context—out-of-character logins from locations too far apart to be from a single user, on new devices, through unknown networks and at unusual times
- Threat intelligence—attack campaigns targeting specific roles or groups or using methods consistent with activity observed in a user account.

If something looks amiss, it applies risk-based controls such as suspending the account, asking the user to log in again or requiring multifactor authentication.

Putting the Pieces Together

Proofpoint Email Security address all attackers' tactics and secures all threat vectors, including corporate email, personal webmail, cloud apps to end-users. Our integrated, end-to-end solution:

- Reduces the risk of BEC and EAC by protecting across broad range of attacker tactics.
- Provides visibility into all the email sent using your domain, including trusted third-party senders, as well as compromised account risks from cloud apps
- Stops impostor email and fraudulent use of trusted domains and detects compromised cloud accounts and phishing
- Identifies who your most attacked people are, who's being attacked with credential phishing and impostor emails, and who's vulnerable to credential theft
- Enables you to apply adaptive controls, such as browser isolation and security awareness training, to your Very Attacked People™
- Trains your end users to become more resilient to BEC and EAC attacks

With deep visibility into all these areas, you can better understand the threat, communicate risks to the board and business peers and prioritize mitigation. We remove the complexity of managing different point solutions from different vendors. With this comprehensive approach, you can optimize resources to improve security and operational effectiveness.

Learn more about how Proofpoint's multilayered, people-centric approach can help you stop BEC and EAC threats at https://www.proofpoint.com/us/solutions/bec-and-eac-protection

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0501-002-01-02 8/21