Why Proofpoint Offers the Only Effective Solution for Combatting BEC and EAC Attacks

FAST FACTS

- Through 2023, BEC attacks will continue to double each year to over $5 billion and lead to large financial losses for enterprises[1].
- Losses due to BEC and EAC scams have reached $26 billion worldwide (potential and actual losses)[2].
- Nearly 90% of organizations faced BEC and spear-phishing attacks in 2019[3].
- The average loss from a bank robbery is about $3,000. The average loss from a successful BEC attack is nearly $130,000[4].

Email fraud leads to two main threats: business email compromise (BEC), in which attackers pretend to be you, and email account compromise (EAC), in which attackers essentially **become** you.

BEC and EAC are complex, multi-faceted problems that are hard to prevent. Cyber criminals use a wide variety of tactics and channels to conduct these types of attacks. They target your employees' corporate and personal email, cloud apps and even your supply chain.

Get the Best Defense with Proofpoint

Because BEC and EAC are intertwined, you must address them at the same time with comprehensive security. If you're addressing BEC but not EAC, your organization is still exposed.

Proofpoint is the only vendor that can provide you with an integrated, end-to-end solution to effectively stop BEC and EAC attacks. We offer the most effective threat protection and we address all the methods cyber criminals use in these attacks.

With our unique, comprehensive solution, you can:

- Detect and block imposter and phishing emails and prevent fraudulent use of your domains.
- Gain deep visibility into your human attack surface. Find out which users are being attacked with impostor and phishing emails and who is vulnerable to these threats.
- Deploy adaptive controls for risky users, to mitigate BEC/EAC risk.
- Teach your users to spot identity deception tactics with proven security awareness training.
- Respond to threats faster and Improve your operational effectiveness. We automate threat detection and response, saving you time and money.

Stop More Threats, Faster

Our advanced solution provides better security effectiveness in stopping BEC and EAC attacks. Most other vendors rely on methods like static rules matching, which requires a lot of manual tuning, causing more work for you. We take it to the next level with machine

1 "Protecting Against Business Email Compromise," Gartner, 2020
2 Public Service Announcement, FBI, 2019
3 "State of the Phish report," Proofpoint, 2019
4 U.S. Secret Service, 2019

learning that dynamically classifies and detects impostor and phishing emails that don't always have malicious payloads. With multiple detection techniques, we accurately detect and block more email threats that others miss, so you can stay ahead of changing attacker tactics. We are the only company that can deliver comprehensive email security that:

- Detects and blocks BEC/EAC threats before they enter your organization
- Provides actionable insights into your human attack surface
- Authenticates email with DMARC and prevents fraudulent use of your trusted domains
- Identifies suspicious cloud activities, such as failed logins, brute-force attacks and compromised cloud accounts
- Enables adaptive controls such as browser isolation to ensure safe access to personal web email, and security awareness training

Gain Unmatched Visibility

BEC and EAC attacks both focus on people, rather than vulnerabilities in your critical infrastructure. To better understand your BEC and EAC risks, you need to understand your human attack surface.

To mount the best defense, you need to know about your people. To start, we give you unmatched visibility into which users are being attacked with impostor and phishing threats, who your Very Attacked People (VAP) are, and who is posing risk to your organization. None of our competitors can provide people-centric visibility to their customers.

You also need to know if anything suspicious is happening with your email traffic or cloud accounts. We give you visibility into both B2B and B2C email traffic, as well as all emails being sent using your domains. This includes trusted third-party senders.

What's more, you can see any suspicious cloud account activities from a single management interface. These include multiple login attempts and other actions that are considered early signs of email account compromise. We also correlate threat activities across email and cloud, connecting the dots between credential phishing email attacks and suspicious logins. For added security, we also report on fraudulent lookalike domain registrations so you can proactively prevent these impostor threats.

Improve Operational Effectiveness

Proofpoint cuts operational costs by preventing most threats from getting through in the first place. If a threat does slip through, we give you the context you need to respond and automate the investigation and remediation process.

- **Preventing threats:** We catch more threats than our competitors do. In just one example, we helped a Fortune 250 global manufacturer cut the number of security incidents that required further investigation 81%—and that was within the first three months of deploying our solution.
- **Providing context:** We give you actionable visibility across security control points and threat intelligence. We make it easy to consume, saving you time that would have been wasted if you had to compile it manually. That's insight our competitors simply do not provide. Their customers have to manually score their own threats and look through their people and distribution lists to try to figure out who requires additional protection.
- **Automating detection and response:** Our products are tightly integrated so that you can automate threat detection and remediation processes. Plus, we connect the dots across different control points, including email, cloud apps and users for better protection. You can quickly contain the spread of threats by automating responses. Actions include:
  - Rewriting embedded URLs to direct users to web isolation
  - Enforcing DMARC authentication
  - Automatically finding and removing malicious emails that contain URLs poisoned post-delivery
  - Suspending compromised cloud accounts.

This tight integration helps you accelerate threat response by reducing manual work and consolidating multiple security point products.

Find Out How We Can Help You

Learn more about how our integrated, end-to-end email security solution can help you effectively combat BEC and EAC. Ready to evaluate your options? Contact us for a free assessment of your current security environment. We'll have you set up within 24 hours with minimal configuration.

Sign up here: proofpoint.com/us/free-trial-request.

LEARN MORE

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