

BEC



Generate

DECODING BEC IN THE AGE OF CHATGPT

WHITEPAPER

*Sincerely,
GenAI*

Overview

Business Email Compromise or BEC is a type of cyber attack delivered via email where threat actors impersonate or access an account (ATO) of a high-ranking executive, a colleague or a trusted vendor with the aim of tricking the recipient into transferring money, sharing sensitive information, or executing some action that benefits the threat actor. These attacks can be highly sophisticated, often bypassing both traditional and “next-gen” security measures due to their personalized and seemingly legitimate nature.

Imagine receiving an urgent email that looks like it’s from your manager, or from a service provider you’ve worked with for years; it could even be your own personal accountant. The message is personalized to you, contextually relevant, and grammatically perfect. It’s convincing. Except it’s not exactly real. It’s a product of Generative Artificial Intelligence (GenAI) chatbot like ChatGPT, meticulously crafted by adversaries to manipulate emotions, build false trust, and ultimately, to “social engineer” you, the end user in an organization into falling for a scam, disclosing confidential documents, and even transferring funds.

In this paper, we delve into the world of BEC attacks, a threat that has seen a significant rise in recent years and is now positioned as the costliest among cyber attacks (FBI IC3 report). We will explore how these attacks work, the role of GenAI in enhancing these threats, their impact on organizations, and how security leaders can protect their organizations against BEC.



It’s important to understand that BEC attacks, facilitated by generative AI tools, can manifest in various ways. These attacks may be components of broader strategies such as lateral movement or account takeover schemes, leading to severe consequences for both employees and their organizations.

The BEC Threat Landscape

Email security and the cyber threat landscape are constantly evolving, with adversaries employing increasingly advanced techniques to bypass security solutions and exploit the weakest link in the organization, us humans. BEC also known as “Pretexting”, is a prominent form of social engineering-based threat that has seen a significant rise in recent years. According to Verizon’s [Data Breach Investigations Report \(DBIR\) 2023](#), BEC attempts on organizations have nearly doubled, accounting for over 50% of incidents involving social engineering techniques in 2022 (with phishing as the runner-up). Perception Point’s 2023 Annual Report on Threats & Trends highlights an alarming 83% growth in BEC attack attempts over 2022.

These findings are in line with the observations made in Gartner’s Market Guide for Email Security 2023 that impersonation and account takeover attacks via BEC are increasing and causing direct financial loss, as users place too much trust in the identities associated with email, which is inherently vulnerable to deception.

83%

Annual growth in BEC attempts
[Perception Point](#)

Over 50%

of social engineering breaches
were BEC attacks
[Verizon DBIR 2023](#)

By 2025

Generative Artificial
Intelligence will be responsible
for creating 10% of all data
Gartner

The exponential surge in BEC attacks is a clear indicator of the growing level of sophistication of threat actors and the innovative tools they have at their disposal. One such tool that is proving to be a game-changer in the realms of social engineering and impersonation threats is Generative AI (GenAI). Attacks are now being “supercharged” with the power of AI and Large Language Models (LLMs), allowing cyber criminals to work faster, and on a much larger scale than ever before. Previously time-consuming preparation work, such as target research and reconnaissance, “copywriting”, and design, can now be done within minutes by using well-crafted prompts. In their GenAI paper for CISOs, Gartner noted that “GenAI can help attackers create more attacks through upskilling, automation, scalability, and plausibility”.

In this rapidly evolving threat landscape of low-risk, high-reward ways to siphon large amounts of cash from victims, it's crucial for organizations to stay informed and take proactive measures to protect themselves. In the following sections, we will delve deeper into the mechanics of BEC attacks, the role of GenAI in revolutionizing these threats, and the impact they have on businesses internationally.



Common BEC Attacks in 2023



CEO Fraud

The attacker impersonates a high-ranking executive, often the CEO, and requests an urgent money transfer (e.g. the notorious “gift card scam”) or sensitive information. Potential Targets: financial department, executive assistants.



Vendor Email Compromise or Supplier Swindle

The attacker impersonates a trusted vendor or supplier of the company and requests payment for a fake invoice or notifies a change in bank account details to siphon future payments. Potential Targets: procurement, accounts payable.



Account Takeover Compromise

An employee or a vendor’s email account is hacked and used to request payments or sensitive data from other employees or business partners. This subtype of BEC is particularly dangerous because the attackers have already gained access to sensitive data that they can leverage and their messages originate from a legitimate account, making them harder to detect and more likely to be trusted by the recipient. Potential Targets: any employee, particularly those with access to sensitive data or financial authority.



Thread Hijacking

An ongoing email conversation or thread is taken over by an attacker, who then attempts to trick the victim into transferring money or sharing sensitive information. Potential Targets: any employee involved in externally facing email conversations with sensitive content or financial implications.



Attorney Impersonation

The attacker impersonates a lawyer or legal advisor who is supposedly handling confidential or time-sensitive matters, pressuring the victim into transferring funds or sharing information. Potential Targets: executives, general counsel, legal department.



HR Data Theft

Employees in Human Resources or bookkeeping are targeted to obtain sensitive data, such as employee tax information (e.g. W-2 report). This data can be used for further attacks or identity theft.



Everyone's a Target

It's worth noting that the process of identifying potential targets within an organization has become increasingly easy for threat actors. Social media platforms like LinkedIn, company websites, and basic OSINT techniques provide a wealth of data that can be used for reconnaissance. This highlights the importance of being mindful of the information shared publicly and implementing robust security awareness training across the workforce.

Unpacking BEC Tricks & Techniques

BEC attacks are intricate schemes that employ a blend of psychological manipulation and technical subterfuge to deceive unsuspecting employees into carrying out actions that serve the attacker's interests. To effectively guard against these threats, it's crucial to first comprehend their inner workings. The examples below detail some prevalent strategies threat actors use in BEC attacks:

Deceptive Email Practices

Adversaries frequently tamper with email headers or display names to give the impression that the email originates from a reliable source a.k.a Domain Spoofing. This could involve using a domain that closely resembles the legitimate one or adopting the identity of an actual employee or executive.

Creating a Sense of Urgency

Threat actors often employ psychological tactics to instill a sense of urgency or pressure to prompt swift action from the recipient, bypassing the usual checks and balances. This could involve asserting that the request is time-sensitive or crucial for business continuity.

Lateral Movement

In some instances, attackers have already infiltrated one email account or more before navigating their way to other users and executing a BEC attack. This could involve compromising a lower-level employee's account and then using that account to send deceptive emails to higher-level employees, financial departments or to other organizations with previous business relations.

Absence of External Verification

BEC scams often involve requests that are difficult to validate through external sources or third parties. This increases their stealth and the likelihood of the recipient complying with the request.

Trust Exploitation

Attackers often take advantage of the trust established between the impersonated individual or organization and the recipient. For instance, an employee is less likely to scrutinize a request appearing to come from their supervisor or a trusted vendor.

Multi-channel Approach

While the term "Business Email Compromise" suggests that these attacks are confined to email, this is no longer the case. Today's BEC attacks can originate from various business communication channels. Attackers are increasingly exploiting platforms like Slack, WhatsApp, and Microsoft Teams, where informal and rapid communication often occurs. This multi-channel approach broadens the attack surface and presents additional challenges for detection and prevention.

By understanding these strategies and techniques, organizations can better identify potential BEC attacks and respond effectively. In the subsequent section, we'll explore the role of AI in amplifying these threats.

How GenAI is Revolutionizing BEC Attacks

Anyone who has spent some time online or has read the news in recent months has likely felt the undercurrents of a seismic shift - the “Rise of Machine Learning.”. Popular Generative Artificial Intelligence (GenAI) platforms like OpenAI’s ChatGPT and Google Bard have been changing the digital landscape ever since their release.

With the power of Large Language Models at its core, GenAI is opening up a world where machines don't just compute - they create. Computers are crafting original content, from text to images, music to code, that is so human-like it blurs the line between man and machine.

The ripple effects of this technology are vast, touching almost every corner of our lives. It's a tool for good, sparking new ideas for artists, authors and coders, revolutionizing training for pilots and doctors, and even taking the hassle out of planning a vacation via travel agents. The potential applications of GenAI are as diverse as they are numerous, transforming the way we live and work.

But like many other innovations, the power of GenAI proves to be a double-edged sword. As it becomes more and more accessible, the risks it poses also escalate. Threat actors are exploiting GenAI tools to “supercharge” their malicious activities and enhance the effectiveness of malware, phishing, and social engineering attacks. This allows them to work faster, and on a much larger scale than ever before. Previously “laborious” tasks can now be executed within seconds by using text prompts on ChatGPT. This means more potential victims and an increased likelihood of successful attacks.

BEC stands out as one of the most prevalent cyber threats amplified by the use of GenAI:

Making Attacks More Convincing

GenAI can generate contextually relevant and coherent emails that are more convincing to recipients. GenAI-powered BEC attacks no longer have the tell-tale signs of a scam such as poor spelling, bad grammar, and lack of context.

By analyzing previous communications and learning the style and tone of the impersonated individual, GenAI can easily create emails that closely mimic legitimate communication, increasing the likelihood of the recipient falling for the scam. Moreover, if fed enough data, for example by leveraging “thread hijacking” following an account takeover, tools like ChatGPT can easily simulate the impersonated individual behavior and writing style, continue existing conversations and further complicate detection.



Bypassing Detection Measures

GenAI-generated emails can bypass next-gen security measures, which often rely on detecting signatures, patterns or anomalies in the content of emails. Because GenAI can generate emails that closely resemble legitimate ones, these emails are less likely to be flagged as suspicious by security systems. Traditional email security solutions, designed to detect typical indicators of phishing or other malicious emails, are struggling to keep up. They are not designed to handle the sophistication and subtleties of GenAI-generated content. This in itself highlights the need for a new breed of detection capabilities specifically designed to counter GenAI attacks.



Adapting to Security Measures

As security measures evolve, so too can GenAI. By learning from past successes and failures, GenAI can adapt its strategies to bypass new security protocols. This adaptability makes it a persistent and evolving threat that can keep pace with, or even outpace, advancements in cybersecurity technology.



Exploiting Human Vulnerabilities

GenAI can be used to exploit human psychology more effectively. Not every hacker is a gifted “social engineer” with manipulation skills, but by analyzing data about a target, GenAI can tailor its approach to exploit the individual's specific vulnerabilities. For example, it can use urgency, authority, or affinity tactics more effectively, making the BEC attack more likely to succeed.



Multilingual Capabilities

GenAI can generate content in multiple languages, making it easier for threat actors to target individuals and organizations across different regions and countries. This can significantly expand the potential victim pool for BEC attacks.



What the "Hack" is Going on With BEC and GenAI?

You may ask yourselves, aren't companies like OpenAI and Google responsible enough to set limitations and prevent their platforms from helping malicious actors do bad things?

The short answer is yes but apparently not enough. Go test it yourself and ask ChatGPT to write a malicious code or to set up a phishing campaign for you. There is a pretty good chance you will be presented with a generic apologetic message saying "Sorry, but I can't assist with that." It begs the question: how do threat actors still abuse GenAI?

There are two main methods cybercriminals are utilizing to bypass GenAI platforms' native security and ethical usage restrictions to produce illicit content:



Leveraging "Unethical" Alternatives

"WormGPT" is an example of a dedicated "blackhat" GenAI platform that is being used by threat actors to conduct sophisticated phishing and BEC attacks. It allows even novices to launch large-scale, personalized attacks, exploiting existing LLM models like Bard and ChatGPT and sidestepping their anti-abuse measures. Hackers' forums and cybercriminals marketplaces across the darknet offer other ChatGPT alternatives that are not bound by any ethical restriction or usage policy.

Jailbreaking Popular GenAI Chatbots

ChatGPT Jailbreak or "Jailbreaking" is a method used by threat actors (and cyber defenders) to manipulate or circumvent OpenAI's restrictions and controls, which were put in place to prevent misuse. For example, ChatGPT has safeguards designed to prevent it from generating inappropriate content, malicious code, or revealing sensitive information. A jailbreak method would be an attempt to bypass these safeguards and coerce the model into generating output that it is typically programmed to avoid. Tools like ChatGPT, Bing Chat AI, and Google Bard were all jailbroken within minutes of their release, the internet is filled with dozens of guides and go-to prompts for jailbreaking.



The Impact BEC Has on Organizations

BEC attacks have ascended to become one of the costliest cyber threats in recent years, outperforming even ransomware. Their profound impact stems largely from how the adversaries are exploiting the organization's weakest link, the people, and circumventing security tools, resulting in considerable damage for organizations worldwide.

It should come at no surprise that the most immediate and tangible impact of a BEC attack is often financial. According to the FBI's Internet Crime Report, in 2022 alone, BEC attacks led to \$2.7 billion in losses. These losses are not only from the direct theft of funds but also from the costs associated with responding to the attack, and potential fines or lawsuits resulting from the breach and the further disruption of the business continuity. Additional consequences of a successful BEC attack include:



Reputational Damage

Beyond the financial implications, BEC attacks can inflict significant reputational harm. If stakeholders, partners, or customers lose faith in an organization's ability to safeguard its data and financial resources, they may opt to take their business elsewhere. This erosion of trust can have lingering effects on an organization's market standing and profitability.



Legal and Regulatory Consequences

Organizations that have fallen victim to BEC attacks may face legal and regulatory repercussions, particularly if the attack leads to the compromise of sensitive customer data. Depending on the jurisdiction and the nature of the data compromised, organizations may be obligated to notify affected individuals, regulatory bodies, and in some cases, the public. They may also face fines or other penalties.



Increased Security Costs

Following a BEC attack, organizations are often required to invest in bolstered cybersecurity measures to prevent future attacks. These measures can include enhanced email security, employee training, and potentially costly system upgrades.

The impact of BEC attacks is far-reaching and often long-lasting, affecting not just the financial health of companies but also their operational efficiency, reputation, and legal standing. It underscores the importance of robust and proactive measures to prevent them in the first place.



Mitigating the BEC Risk: A Two-Pronged Approach

In the face of the rising tide of GenAI-powered BEC attacks, a two-pronged paradigm that focuses on both user education and robust security measures is crucial. This recommended approach empowers employees to recognize potential BEC attempts while equipping the security teams with the tools and strategies they need to detect and protect their organizations against these attacks.

Part 1: Best Practices for CISOs and Security Teams

With BEC, prevention is the best kind of protection you can have for your end users. If the fraudulent email never reaches your employee's inboxes in the first place, you have already neutralized your weakest security link that the threat actors are targeting - the human element.

Implementing a multi-layered defense with robust security measures is crucial in protecting the organization against GenAI-powered BEC. Here are some best practices:

AI-Powered Email Security

Implementing advanced threat detection solutions can prevent BEC emails from reaching end users. Look for a solution that uses machine learning and AI which is used to analyze email content, sender behavior, and other factors to identify and block BEC attempts. These technologies can adapt to evolving threats like GenAI-based threats and provide a proactive defense against BEC. With the line between machine and human generated content already blurred for us humans - "it takes one to know one."

Secure Your Own Domains

Prevent potential Domain Spoofing by registering different domain names similar to your organization's. This relatively inexpensive solution will go far in protecting against the email spoofing at the heart of successful BEC attacks.

Incident Response Plan

Having a well-defined and practiced incident response plan can help your organization respond quickly and effectively to a BEC attack, minimizing potential damage.

Implement DMARC, SPF, and DKIM

These email authentication protocols help prevent spoofing and impersonation by verifying that incoming emails are from a trusted source and have not been modified during transit.

Vendor Risk Management

Implementing a robust vendor risk management process can help ensure that your vendors are also following best practices to prevent BEC attacks.



Force Multi-Factor Authentication

Implementing multi-factor authentication makes it difficult for threat actors to access employees' email accounts (ATO) even if they have their credentials, making it harder to launch a BEC attack.

Monitor and Audit Email Systems

Regular monitoring and auditing of email systems can help identify suspicious activities early. This includes monitoring for unusual login activities, changes in email rules, and sudden increases in email forwarding. Organizations should employ internal email traffic scanning to quickly identify compromised accounts.

Part 2: User Awareness & Education - Recognizing BEC Attacks

Because 100% protection does not exist (yet), your second line of defense against machine generated or human-written attacks often lies with the end users themselves. Regular training and awareness programs can empower your employees to recognize and respond appropriately to BEC attacks.

Here are some key indicators your end users can learn to identify a potential BEC attempt:

Urgency

BEC emails often create a false sense of urgency to prompt swift action from the recipient, bypassing the usual checks and balances.

Unusual Language

Look out for unexpected language or requests that seem out of character for the person supposedly sending the email.

Domain Changes

Double-check the sender's email address. A spoofed address will often have an extension similar to your organization or vendor's legitimate email.

Asking for Sensitive Information

Be wary of any emails asking for sensitive information, especially if it's related to financial transactions.

Unexpected Emails







If you receive an email from someone you don't usually communicate with, or if the email is about a topic not typically discussed, it could be a BEC attack.

One of the most effective ways to counter BEC attacks is to instill a culture of verification. Advise employees to double-check and report any unusual or unexpected requests, even if they appear to come from a trusted source.



How to Prevent BEC Attacks Generated by AI

In the face of high-volume and growing sophistication of BEC email attacks, it's crucial for security and risk management leaders to carefully evaluate and select the right email security solution for their organization. Below is our checklist for cybersecurity decision makers:

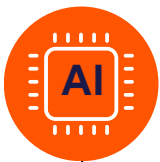
-  *The right solution should not only be capable of detecting and blocking traditional threats but also be equipped to handle the evolving landscape of BEC and social engineering, especially those enhanced by GenAI.*
-  *It should be able to learn and adapt to the ever-changing tactics and tools of threat actors “on-the-fly.”*
-  *It leverages advanced machine learning and AI models to continuously update its understanding of threats and improve its detection. Including capabilities to analyze and understand the context and subtleties of an email, rather than just looking for known signatures or obvious anomalies.*
-  *It should provide comprehensive visibility and control over the organization's email environment. This includes features like detailed threat intelligence reports, customizable policies, and easy integration with other security tools in the organization's security stack.*
-  *It should be user-friendly and not add unnecessary complexity to your organization's existing processes. It should provide clear and actionable alerts to quickly respond to threats and have intuitive interfaces for both end-users and administrators.*
-  *The solution should also extend its protection to other channels through which BEC threats can reach the end users, such as messaging apps, SaaS applications, and collaboration tools. This multi-channel protection is crucial in today's interconnected digital workspace, where threats are not confined to email alone.*

Selecting the right security solution is one of the most critical steps in mitigating BEC attacks. It requires a careful evaluation of the solution's capabilities, adaptability, integration, and usability. By choosing the right security product, organizations can significantly enhance their defense against BEC and other email-based threats.

Perception Point's Solution for GenAI Threats

Advanced Email Security by Perception Point is a leading Integrated Cloud Email Security (ICES) solution recognized by Gartner 4 times in a row (2019, 2020, 2021 and 2023). Combining the highest detection accuracy on the market powered by patented anti-evasion technology and enriched with an all-included managed Incident Response service, the solution delivers enterprise-grade protection against any modern cyber threat.

The AI-powered threat prevention platform, utilizes unique combination of human insight with proprietary machine learning models and AI algorithms:



NLP and GenAI

Models that deeply understand the organization's relationships and communication patterns.



Computer Vision

Algorithms that see through BEC attacks, phishing and other spoofing attempts



Anomaly Detection & Content Analysis

Recognize suspicious behaviors and unfold evasion techniques



24/7 Human Insight

The all-included team of cybersecurity experts constantly optimize detection, analyze incidents, create new AI/ML algorithms on the fly, proactively hunt for false positives, and offer rapid remediation when necessary



Anti-BEC: AI-Powered Detection Models



GenAI Decoder™

LLM-based model utilizes transformers to recognize the patterns in AI-generated text and detects malicious social engineering attempts

Learn more:

["An AI for an AI: LLM-Based Detection of GPT-Generated BEC Attacks."](#)



Thread Hijack Protection

Domain-spoofing correlation algorithm prevents conversation hijacking and vendor impersonation attempts



Supply-Chain Recognition

Analyzes business communication to automatically identify domains of the organization's business partners, vendors, VIP users etc.



Anomaly Detection

Identifies changes in sender's tone and sentiment, analyzes the message content and compares to metadata to find deviations, topic modeling for subject and email body and more



Anti-Textual-Obfuscation

Detects evasion attempts that conceal the malicious text by replacing certain characters with other visually similar ones, invisible ones, etc.



Content Analysis

A myriad of NLP models extract sensitive content like personally identifiable information (PII), identify names of entities (NER), analyze textual metadata and more

Customer Case Study: VEC Attack on US-Based Food & Beverage Distributor

At Perception Point, we recently encountered a classic instance of a Vendor Email Compromise (VEC), also known as "Supplier Swindle," targeting one of our customers, a food and beverage distributor based in the United States. This is a threat that almost cost our client quarter million dollars.

The threat actor initiated the attack by infiltrating a local vending partner of our customer, the distributor. Our customer's partner, a small-to-medium-sized business (SMB), had not invested heavily in robust security measures, providing the attacker with an easy entry point. With minimal security barriers to overcome, the attacker successfully breached the email account of our customer's contact at the local vendor and began monitoring the email communications between the two parties. The attacker patiently awaited the opportune moment to strike, which presented itself when the vendor sent a legitimate invoice to the distributor's CFO, requesting a payment exceeding \$200,000.

From:
Sent:
To:
Subject: Re: PO #11768-DI

Thank you for your response.

We received a check payment for **\$213168.00** please kindly void the other check and have them processed via WIRE TRANSFER into our account to avoid any delay in receiving the payment. Let me know if I should forward you all necessary information for payment.

Await your positive response.

Seizing this opportunity, the attacker, who in the meantime purchased a similar domain to the vendor's and spoofed an email address using the vendor's name, hijacked the email thread and requested a change in payment details, redirecting the funds to their own account rather than the legitimate vendor's.

From: [Redacted]
Sent: Monday, [Redacted] 4:46 PM
To: [Redacted]
Cc: [Redacted]
Subject: Re: PO #11768-DI

Shon,

Trust you are well

Please can you confirm if payment for this invoice can be processed via ACH payment into our updated bank account due to some unforeseen issue with our previous bank. Let me know when you intend on making payment so I can forward all necessary information for ACH payment.

Apologize for any inconvenience.

Await your response.

[Redacted signature]



Our platform immediately caught this anomaly using AI algorithms together with advanced reputation and SPF/DKIM/DMARC checks. The email was detected and prevented from reaching the end user.

But this is where things get interesting with this particular BEC attack. The end user, the CFO, who was notified about the prevented incident assumed it was a false-positive since he did need to pay the pending invoice. He then contacted his IT administrator who promptly and unknowingly released the malicious email without checking the supporting evidence that deemed it malicious.



The Perception Point Incident Response team was alerted of the release and actively checked it. Upon confirming that the email was indeed malicious – the team immediately engaged with the administrator to block the money transfer and pull the email again!

This case study underscores the importance of robust and proactive security measures, even for SMBs, as they can often be the weakest link in a larger network of business relationships. It also highlights the sophistication and patience of threat actors in executing such attacks, further emphasizing the need for comprehensive security solutions that effectively combine state-of-the-art AI models with good old human insights.

Moreover, this incident illustrates the crucial value of a natively integrated IR service that can actively monitor and respond to threats, even when internal team members may mistakenly classify an incident as a false positive. This additional layer of security can be the difference between a successful BEC attack and a thwarted one, protecting the organization's financial resources and reputation.

Navigating the Future of BEC Attacks

The overall threat landscape, especially BEC attacks, is evolving at a rapid pace, with Generative Artificial Intelligence (GenAI) playing an increasingly significant role in enhancing these threats. As we've explored in this whitepaper, these attacks can be highly sophisticated, often bypassing traditional and next-gen security measures due to their personalized and seemingly legitimate nature.

In this ever-evolving threat landscape, it's crucial for organizations to stay informed and take proactive measures to protect themselves. This involves a two-pronged approach that focuses on both user education and robust security measures. By empowering employees to recognize potential BEC attempts and equipping security teams with the tools and strategies they need to detect and protect against these attacks, organizations can significantly enhance their defense against BEC and other email-based threats.

As we move forward, it's clear that the fight against BEC attacks is far from over. With the rise of GenAI and its increasing use in cyber attacks, the challenge will become even more complex. However, by staying informed, implementing robust security measures, and fostering a culture of security awareness, organizations can navigate this challenging landscape and protect their valuable assets.

Remember, in the face of BEC attacks, prevention is the best form of protection. By implementing a multi-layered defense with robust security measures and fostering a culture of verification and awareness among employees, organizations can significantly reduce their risk and ensure their continued success in the digital age.



About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection and response to all attacks across email, cloud collaboration channels, and web browsers. The solution's natively integrated incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights; providing proven best protection for all organizations.

Deployed in minutes, with no change to the enterprise's infrastructure, the patented, cloud-native and easy-to-use service replaces cumbersome legacy systems to prevent phishing, BEC, spam, malware, Zero-days, ATO, and other advanced attacks well before they reach end-users. Fortune 500 enterprises and organizations across the globe are preventing content-borne attacks across their email and cloud collaboration channels with Perception Point.

***INTERESTED IN PREVENTING BEC
ATTACKS GENERATED BY AI?***

[Request a Demo](#)

[Learn More](#)

