HUNTRESS

Battling Business Email Compromise with Huntress Managed Identity Threat Detection & Response (ITDR)

Executive Summary

The growing reliance on cloud-based technologies has introduced unparalleled efficiency for modern businesses. However, this shift has also exposed organizations, especially small and medium-sized businesses (SMBs), to a rising wave of cyber threats.

This white paper will explore the increasing threat of business email compromise (BEC) attacks, emphasizing the critical need for SMBs to safeguard employee identities and Microsoft 365 environments. We will also delve into how Huntress Managed ITDR (formerly MDR for Microsoft 365) offers a reliable solution to these challenges, providing 24/7 monitoring, intelligent threat detection, and expert remediation guidance to thwart BEC attacks and ensure uninterrupted business operations.

The Menace of Business Email Compromise

In today's cloud-centric business landscape, safeguarding sensitive data and critical operations from cyberattacks is of paramount importance. While the rapid adoption of cloud-based infrastructures has brought immense benefits to modern businesses, it has also introduced new avenues for cyberattacks, with business email compromise (BEC) at the forefront.

Email is a cornerstone for business communication, collaboration, and data exchange. However, it is also a favored vector for cybercriminals to execute BEC attacks. Attackers often exploit stolen credentials or use other methods to compromise accounts, infiltrating cloud environments and launching devastating cyberattacks.

The FBI's 2022 Congressional Report underscores the severity of this issue, revealing that BEC consistently ranks as the largest dollar loss by victim crime typology, with staggering financial repercussions. The report highlights that in the calendar year 2021, BEC led to over $2.4 billion in adjusted gross losses[1], overshadowing other forms of cybercrime by a substantial margin.

The key to minimizing damage lies in early threat detection and response. Huntress Managed ITDR addresses this critical need by providing comprehensive around-the-clock protection, intelligent threat detection, and expert incident response to defend user identities against new and ongoing cyber threats.

The threats of today and tomorrow are becoming increasingly more sophisticated over time, and with the addition of generative AI tools that can be used to help malicious threat actors more efficiently execute BEC attacks, there is a high probability that every business will experience an attempted compromise in the next few years.

Some of the most common BEC attacks that organizations face globally are:

Invoice Fraud

Attackers compromise the email account of a legitimate vendor or supplier and use their email to send fake invoices to the targeted organization. The invoices contain payment details that will result in any funds paid being transferred to the attacker's account instead of the legitimate vendor's account.

Invoice Interception

Similar to invoice fraud, Invoice Interception targets the vendor's email account. Attackers compromise the vendor's email account, then intercept outgoing emails with legitimate invoices, but change the payment details in the invoice prior to sending the invoice. This type of attack leverages the trust established between the vendor and their customer as well as the fact that the customer is expecting an invoice for a specific amount already.

Employee Payroll Diversion

Attackers compromise an employee's email account, then contact HR or finance to change the direct deposit information for the employee's paycheck. This results in the employee's salary being redirected to the attacker's account.

Executive Impersonation

The threat actor compromises the email account for a high-level executive in the company, then emails other employees from that account asking them to urgently purchase gift cards or another kind of easily laundered asset. The stated reason for the purchase is that they need it for a last-minute company award, or to give out at a convention.

IT Administrator Compromise

Threat actors breach the IT administrator's account, which can globally administer the company's Microsoft 365 instance. This enables them to read and edit the emails of any employees, add more admin users to maintain their access, and even set up new cloud resources they can use to launch further attacks against the targeted company or other businesses.

Legal Intimidation

The attacker compromises the account for a member of a legal firm, then uses that account to solicit payments for legal services or to pressure a victim into transferring funds to avoid a lawsuit.

HUNTRESS

Trends in BEC and Social Engineering

97% of CISOs and other high-level security leaders have been targeted by email-based phishing attacks[2].

BEC led to over **$2.4 billion** in adjusted gross losses in 2021[5].

Organizations with fewer than **500** employees reported an increase in the average monetary impact of a data breach, up from **$2.92M** in 2022 to **$3.31M** in 2023[3].

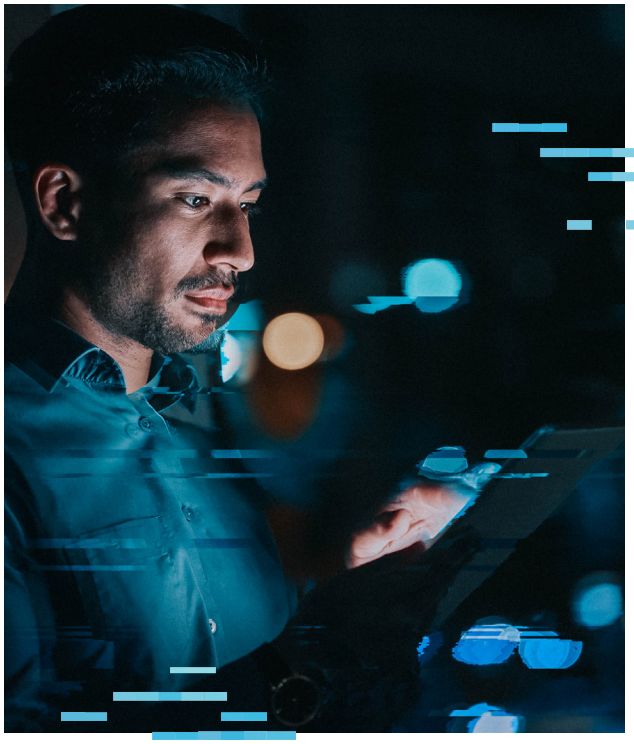
BEC attacks nearly **doubled** across all incidents in 2022. Those BEC attacks represent more than **50%** of social engineering attacks[6].

There has been a **34%** increase in vendor email compromise attacks over the last 12 months[4].

Employee training has been shown to reduce the average breach cost by **$232,8677**, which could be the entire valuation of a small business.

How to Defend Against BEC Attacks

Business email compromise attacks often involve social engineering and manipulation, so a multi-faceted approach is essential, consisting of technology, security best practices, and employee training. Below is a comprehensive guide on how to protect your organization against BEC attacks.



[2] Mimecast State of Email Security Report 2023
[3] IBM's 2023 Cost of a Data Breach Report
[4] Abnormal Security Email Threat Report for H2 2023
[5] FBI's 2022 Congressional Report on BEC and Real Estate Wire Fraud
[6] Verizon's 2023 Data Breach Investigations Report
[7] IBM's 2023 Cost of a Data Breach Report

HUNTRESS

Suspicious indicators to look out for in emails:

Spoofed Sender Information	Attackers manipulate the "From" field to display a sender's name or email address that appears legitimate, **even though it may not be.**
Urgent or Threatening Language	**Phishing emails** often create a sense of urgency or fear to encourage recipients to take immediate action without thinking.
Hyperlinks to Malicious Websites	Phishing emails contain links that direct recipients to **fraudulent websites** designed to collect **sensitive information, install malware,** or perform other **malicious activities.**
Malicious Attachments	Some phishing emails include attachments, such as infected documents or **compressed malware**. When opened, these attachments can infect the recipient's computer.
Fake Logos and Branding	Attackers replicate logos, branding, and visual elements of legitimate organizations to create a **false sense of authenticity.**
Grammar and Spelling Errors	While attackers are becoming more sophisticated, some phishing emails may still contain **language errors** that hint at their illegitimacy.
Request for Sensitive Information	Phishing emails often request recipients to provide confidential information like **passwords, credit card numbers,** or **Social Security numbers.**
Unusual Sender Requests	The email might request unusual actions, such as **transferring funds** to an unfamiliar account or providing **sensitive information** via email.

Best practices to prevent BEC:

Employee Training and Awareness

- Tools that focus on educating employees about threats and making them aware of suspicious indicators of phishing are key to success, such as Huntress Managed Security Awareness Training (SAT) product.
- Perform routine simulated phishing attacks, where suspicious emails using tactics of real attackers are sent out to employees. This can help employees apply knowledge gained via training and reinforce those concepts so they can avoid being compromised during a real attack.
- Send out regular bulletins that highlight the most recent phishing and BEC tactics seen so that employees can continue to build their knowledge.
- Implement written policies that help safeguard employees when faced with attacker scenarios. Examples include:
    - Any email requests for change in financial information must be verified by a phone call for transactions over a certain amount.
    - Gift card purchases may only be made by specific individuals who are pre-authorized in advance by the finance department.

Multi-Factor Authentication (MFA)

- By requiring more than one form of authentication, enforcing MFA will lessen the chance of malicious threat actors gaining access to a user's login credentials.
- MFA should still be coupled with a strong password policy and awareness training to prevent users from entering their credentials in fake phishing schemes.

Conditional Access Policies

- This Microsoft 365/Azure offering enforces that particular controls are satisfied before a user is granted access. For example, a user must sign in from a particular geo-location or must be using an onboarded device to gain access.
- Conditional access policies make it more difficult for a threat actor to log in, even if they manage to phish user credentials and convince the user to provide their MFA token for login on a fake site.

Fortifying Your Defenses Against BEC Attacks

In the ongoing battle against BEC attacks, the formula for success is clear: early detection and swift response. As the threat landscape evolves, businesses must fortify their defenses by investing in security solutions that offer continuous monitoring, real-time threat detection, and expert guidance for incident remediation.

Huntress has spent the last eight years curating the above elements for our partners and customers, using the people, process, and technology triad that's been proven to be an incredibly effective methodology in combating today's emerging threats. From constantly evolving our software and detections in the backend to the years of high-level government, military, and public sector knowledge that has been gathered by our incredible teams, Huntress is a unique partner in the fight against today's cybercriminals. We think like attackers so we know how to stop them, we are situated at the forefront of emerging tradecraft, and we have completely solidified our capabilities to hunt attackers down, wherever they try to hide.

HUNTRESS

Huntress by the Numbers

3800+
Partners

115k+
End Customers Protected

1M+
Identities Monitored

Battling Business Email Compromise with Huntress Managed ITDR

Huntress Managed Identity Threat Detection & Response (ITDR)

Huntress Managed ITDR (formerly MDR for Microsoft 365) continuously evaluates user activities and system logs to detect suspicious behavior and potential identity-related threats in real-time. Backed by a team of identity threat experts, detection engineers, and security operations specialists operating 24/7, Managed ITDR focuses on the most pervasive identity threats for Managed Service Providers (MSPs) and less-resourced organizations. Be it unwanted logins, shadow workflows, evasive behaviors, or rogue apps, Managed ITDR is the first line of defense against identity-focused tradecraft like credential theft, session hijacking, malicious inbox and forwarding rules, and account takeover and BEC.

While other MDR vendors focus their efforts on meeting the needs of large enterprises, Huntress is uniquely attuned to the needs of your SMB clients. By focusing on delivering high-power, low-noise security backed by a 24/7 SOC, Huntress provides effective, affordable security that doesn't cut corners or require enterprise-sized wallets.

Huntress Managed ITDR integrates seamlessly with your Microsoft Cloud environment, gathering user, tenant, and application data, and then enhancing it with insights from both internal and external threat feeds to provide details like geo-location and IP reputation. This contextualized information empowers the Huntress SOC to furnish precise and detailed incident reports, complete with mitigation steps to swiftly neutralize threat actors.

HUNTRESS

How Huntress' Managed ITDR works:

Collect

We continuously capture Microsoft event data, correlating user actions like policy changes, login events, and mail flow manipulation to jumpstart our detection efforts.

Detect

Our Security Operations Center (SOC) analysts and threat detection engineers use detection logic to review ingested data and make contextual insights quickly.

Escalate

Sometimes our analysts need more information to establish if something unknown is malicious. Escalations empower partners to tell Huntress (via Unwanted Access rules) if an activity is Expected or Unauthorized.

Analyze

Our analysts dig deep into the data and scrutinize Unwanted Access rules to identify real threats, cutting through the noise and false positives that clutter your ticketing queue.

Report

We send you an incident report that summarizes our findings and outlines any next steps you should take. These can be sent via email or directly to your ticketing system.

Remediate

In some cases, Huntress will automatically log out and disable an identity on your behalf when malicious activity is detected. If not, we provide clear, detailed instructions for any manual actions, ensuring even a junior tech can handle incidents confidently.

Huntress is recognized by cybersecurity insurance providers, which regularly enables businesses to check more boxes when applying for coverage due to 24/7 monitoring for threats and rapid isolation when an incident is detected. At the same time, Huntress is easily managed and deployed by a small IT team or even a single technical individual, making it accessible to small and mid-sized businesses who have limited IT budgets.

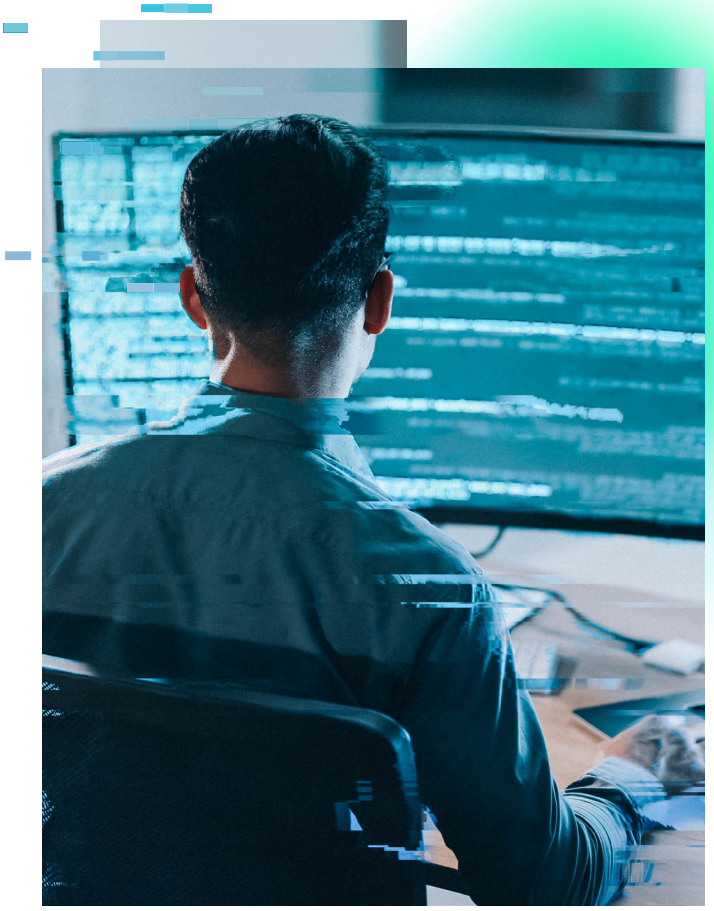
The Human Advantage of the Huntress SOC

Cybersecurity has changed drastically over the years, and businesses are looking to implement processes and technology that are capable of combating threat actors and their evolving attack tradecraft. While artificial intelligence and machine learning play a role, they lack a crucial element that's often exploited by attackers: the human element.

Enter the Huntress SOC, a formidable fusion of human expertise and cutting-edge technology that reshapes the battle against cyber threats.

The Huntress SOC embodies the union of human analysts and advanced technology. By embracing the attacker's mindset, our SOC analysts dissect attack possibilities and anticipate the end goals of today's threat actors.

They leverage years of experience in threat analysis to weed out obvious false positives that purely machine-based technology would forward as legitimate alerts. Huntress analysts are able to combine their expertise with a plethora of information gathered from thousands of reports and investigations they have access to. This blend has helped Huntress create one of the industry's least noisy and most accurate reporting methodologies out there.



From its inception, Huntress' philosophy is to be a low-noise, high-value security ally built for small and medium-sized businesses. Our dedicated detection engineering team builds targeted detectors based off of the most commonly observed attacker tradecraft to rapidly elevate malicious behaviors to the attention of SOC analysts.

They then hunt for and characterize unknown activity to ensure that new methods of evasion cannot escape detection. Every critical and high signal is then reviewed by a SOC analyst so that Huntress Managed ITDR customers will be the recipient of true positive malicious activities that have been validated by a human context.

Team	Their Function
Detection Engineers	Detection Engineers help create new detections, define logic, and create analytics to identify compromises in our partners' environments. They build targeted detectors that mimic attacker tradecraft to rapidly elevate malicioius behaviors to the attention of Huntress SOC Analysts.
SOC Analysts	SOC Analysts hunt and characterize unknown activity to detect new methods of evasion. Critical and high signals are then reviewed by SOC analysts and validated by a human context to help warn our customers of malicious activities.

This approach sets Huntress apart from other competitors in the cybersecurity space who forward every alert and expect their end customer to have the time and expertise to review alerts and determine which were true positives.

Identity-based intrusions and attacks are becoming a staple tool in the adversary's arsenal. At Huntress, we know that neutralizing a threat actor in the early parts of their campaign at the email perimeter can repudiate their entire operation, and ultimately evict and deny the attacker from returning to the network. Our SOC team filters out the lackluster, needless noise to focus on the cloud adversarial activity that could cost businesses millions while delivering consistent security value.

Huntress' commitment to simple yet powerful cybersecurity is recognized throughout the IT and security communities. Our SOC's proficiency in identifying attacker tradecraft isn't confined to our partners alone. Through technical blog posts and educational live webinars, we disseminate our knowledge and insights, elevating the cybersecurity prowess of all.

The Path Forward

As the BEC threat continues to evolve, SMBs face an uphill battle to protect their cloud environments and employee identities. The solution lies in proactive security measures that prioritize early detection, swift response, and ongoing vigilance.

Huntress Managed ITDR offers a robust defense for SMBs to mitigate the risks posed by BEC attacks and fortify their defenses in the modern digital age.

Want to learn more about Huntress Managed ITDR?

Take it for a test drive with our free trial.

Start Your Free Trial

HUNTRESS