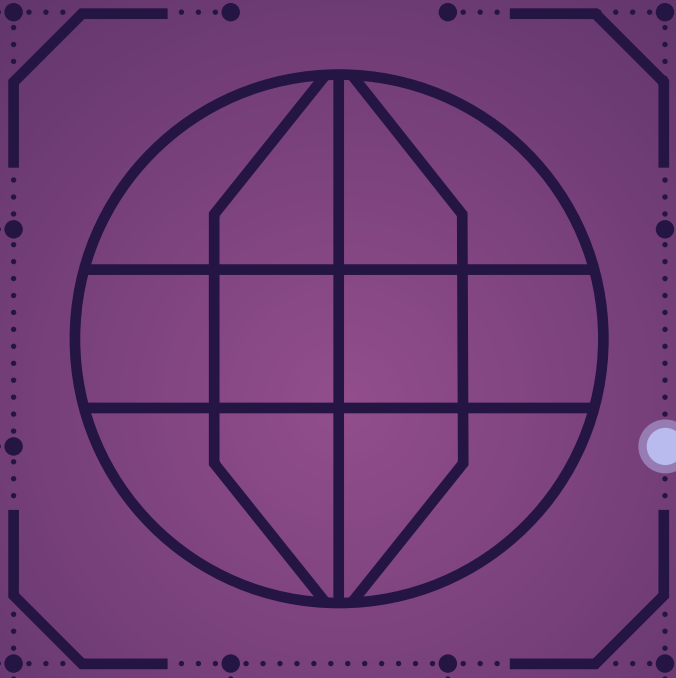
Abnormal



# Preventing Nation-State Email Attacks:

## A Federal Security Challenge

How to Combat Advanced Threats With AI

# Executive Summary

Nation-state actors are launching increasingly sophisticated email-based attacks against federal agencies, creating a persistent and complex cybersecurity challenge. From phishing and spear phishing to email account takeovers, these attacks exploit vulnerabilities in legacy security systems, placing significant strain on security operations centers (SOCs). Federal security teams grapple with alert fatigue, time-intensive investigations, and limited resources—all while adapting to rapidly evolving threats driven by advanced technologies like generative AI.

Historic breaches—including the OPM breach, Russian interference in the 2016 U.S. elections, the SolarWinds hack, and the Storm-0558 incident—underscore the stakes of email-borne threats. These attacks compromise sensitive government data, disrupt critical operations, and jeopardize national security. With the advent of generative AI, nation-state actors now have the tools to create highly targeted, automated phishing campaigns that evade detection by traditional solutions.

Legacy email security measures, such as secure email gateways (SEGs), can no longer keep pace with these advanced threats. To effectively defend against nation-state actors, federal agencies need AI-driven, behavior-based email security solutions. By analyzing communication patterns, identifying anomalies, and automating threat response, these tools empower federal SOCs to detect and mitigate email threats in real time.

This white paper explores:

- Key challenges federal security teams face when defending against nation-state email threats.
- Real-world breaches that reveal vulnerabilities in traditional security approaches.
- The growing risks of generative AI and email account takeovers in federal cybersecurity.
- How AI-powered solutions, like Abnormal Security, redefine email threat detection and response.

With the right strategies and innovative tools, federal agencies can stay ahead of adversaries, protect critical assets, and secure the nation's most sensitive information.

# Table of Contents

# Nation-State Email Attacks: Challenges and Historic Breaches

Nation-state actors using email-based attacks impose a heavy burden on federal security teams. These attacks create operational challenges related to alert overload, time-consuming investigations, advanced threat detection, and resource allocation. Security teams must constantly evolve, requiring more personnel, advanced tools, and cross-agency collaboration to defend against the sophisticated and persistent nature of these email-borne threats.

Traditional email security measures, such as secure email gateways no longer provide sufficient protection for the federal government, as evidenced by some of the most prolific hacks in recent years:

### OPM Breach (2015)

Chinese nation-state actors used spear-phishing tactics to infiltrate the Office of Personnel Management (OPM), compromising over 22 million sensitive records, including security clearance information. Source

### Russian Interference in U.S. Elections (2016)

Russian operatives conducted spear-phishing campaigns targeting political organizations, including the Democratic National Committee (DNC). These efforts demonstrated how nation-states leverage email-based attacks to infiltrate high-profile entities and influence governmental functions. Source

### SolarWinds Breach (2020)

One of the most significant breaches in U.S. history, the SolarWinds attack primarily exploited vulnerabilities in software. However, email spear-phishing was also a key vector in the adversary's multi-pronged approach, targeting federal agencies and exposing critical data. Source

### Storm-0558 (2023)

In May 2023, Chinese hackers from the Storm-0558 group breached Microsoft's cloud-based Exchange email platform. This attack compromised 22 organizations, including U.S. State Department email accounts, resulting in the theft of at least 60,000 unclassified emails. The attackers targeted officials working on Indo-Pacific diplomacy, exposing sensitive information and highlighting vulnerabilities in unclassified email systems. Source

These breaches underscore the critical need for robust email security solutions to protect sensitive government information from sophisticated cyber threats.

# Generative AI and Account Takeovers Escalate Federal Cybersecurity Risks

**32,000**
cybersecurity incidents reported by U.S. federal agencies in 2023—a nearly 10% increase from the previous year.

*Statista*

**83%**
of security leaders report their organization experienced an account takeover attack in the last year.

*Abnormal Security Data*

**$4.88M**
average cost of a data breach.

*IBM Cost of a Data Breach 2024*

Generative AI amplifies the effectiveness of nation-state actors' email-based attacks on federal agencies by enabling more sophisticated phishing campaigns, enhancing social engineering, automating attack processes, and evading detection systems. These AI-driven techniques make it easier for attackers to compromise federal systems, steal sensitive data, and disrupt operations. As generative AI technology continues to evolve, federal security teams will need to adopt advanced cybersecurity measures to defend against these increasingly sophisticated threats.

Email account takeovers remain a persistent and serious threat to federal government systems. These breaches, often executed through spear-phishing or social engineering, allow adversaries to steal sensitive data, spy on communications, and compromise national security. From the OPM breach to the SolarWinds hack, email account takeovers have demonstrated how vulnerable even the highest levels of government can be to sophisticated cyber-attacks.

# Rethinking Email Security: Why Legacy Solutions No Longer Work

Once the cornerstone of email security, secure email gateways (SEGs) are increasingly inadequate against the advanced, evolving tactics employed by nation-state actors. Their reliance on static detection methods, such as signature-based filtering and blocklists, makes them ill-equipped to handle the dynamic, adaptive nature of modern threats. Nation-state attackers often employ AI-driven techniques to craft highly targeted spear-phishing emails that bypass traditional filters, rendering SEG defenses obsolete.

Beyond their inability to detect advanced threats, SEGs also lack visibility into internal communications, a critical gap in protecting against email account takeovers and lateral phishing attacks. Once an attacker gains access to an email account, SEGs are powerless to detect or mitigate malicious activity within an organization's internal network. This blind spot is particularly dangerous when attackers exploit compromised accounts to infiltrate deeper into systems or launch social engineering campaigns that exploit trust among employees.

Nation-state actors increasingly leverage multi-vector attack strategies, combining phishing, credential theft, and malicious attachments to penetrate organizations. SEG architectures, designed for simpler, one-dimensional threats, cannot provide the comprehensive protection needed to combat today's sophisticated cybercriminals.

Clearly a new approach to email security is needed. To counter nation-state email attacks, organizations must adopt modern, AI-driven solutions. These tools leverage behavioral analysis, contextual awareness, and API-based integrations to detect and respond to threats in real time. By monitoring email traffic holistically—both incoming and internal—AI-native systems can identify anomalous behaviors and block advanced attacks before they succeed.

# How Abnormal AI Protects You From Nation-State Actors

As cyber threats grow more sophisticated, combatting them requires a shift from traditional, reactive defenses to proactive, intelligence-driven solutions. Nation-state actors deploy advanced tactics that bypass legacy systems, exploiting gaps in detection and response. To effectively protect against these evolving threats, organizations need a modern approach—one that leverages cutting-edge AI, behavioral analysis, and automation.

Abnormal Security stands out as a leader in this new era of email security, offering unique capabilities designed to counter nation-state-level threats. Here's how Abnormal's AI-powered platform safeguards federal agencies and other organizations against some of the most sophisticated attackers:

## Behavioral-Based Detection

Unique Capability: Abnormal Security excels at detecting **anomalous behaviors** in email communication. Rather than relying solely on traditional signature-based or rule-based security methods, Abnormal builds a baseline of normal behavior for every user, system, and email communication within an organization. It then identifies deviations from this baseline, which can be indicative of email account takeovers or phishing attacks.

Federal Agency Impact: This behavior-based approach is crucial for detecting sophisticated threats, such as nation-state actors using stolen credentials or compromised accounts, even when the email content appears legitimate. Federal security teams can benefit from this high-fidelity detection, which would reduce the chances of attackers moving laterally within the agency or exploiting compromised email accounts.

## Advanced AI and Machine Learning

Unique Capability: Abnormal Security's AI-driven platform uses machine learning to analyze vast amounts of data to detect subtle anomalies in email patterns, communication flows, and user behavior. This enables the platform to spot **highly targeted phishing, spear-phishing, and business email compromise (BEC)** attacks that traditional tools may miss.

Federal Agency Impact: Nation-state actors often craft **highly personalized** and **sophisticated** phishing campaigns aimed at key government officials or military personnel. Abnormal's AI capabilities ensure that even highly tailored attacks, which evade traditional security filters, can be detected before a breach occurs. This is particularly important for protecting high-profile targets in the federal space, such as those with access to classified information.

## Account Takeover (ATO) Protection

Unique Capability: Abnormal Security's platform specializes in detecting ATOs by monitoring for suspicious login activity, unauthorized access attempts, and unusual internal or external email behaviors that could indicate a compromised account.

Federal Agency Impact: Account takeovers are a common entry point for adversaries, especially those from nation-state groups. Once an account is compromised, attackers can conduct espionage, steal sensitive data, or spread malware throughout the network. Through its ATO protection, Abnormal can quickly detect when an email account has been compromised and alert security teams, allowing them to take immediate action to mitigate the threat before attackers can escalate their privileges.

## Automated Remediation

Unique Capability: Abnormal Security offers **automated response and remediation** to threats. When a suspicious email is detected, the platform can automatically remove the email from inboxes, quarantine the threat, and alert security teams, minimizing the time an attacker has to act.

Federal Agency Impact: For federal security teams that are constantly dealing with limited resources and high volumes of alerts, Abnormal's automated remediation helps reduce the burden on human analysts. This automation helps contain and resolve threats quickly, which is crucial in preventing email-borne attacks from spreading across large, interconnected federal networks.

## Comprehensive Protection Against Advanced Social Engineering

Unique Capability: Abnormal Security excels in detecting and blocking **social engineering attacks**, such as BECs and phishing campaigns, by analyzing the intent and context of email communication, rather than just scanning for known malicious indicators. Through the use of natural language processing (NLP), the platform is capable of recognizing subtle indicators of fraudulent requests, such as fake payment demands, unauthorized data access requests, or impersonation attempts.

Federal Agency Impact: Nation-state actors often rely on social engineering to manipulate federal employees into divulging sensitive information or carrying out unauthorized actions. Abnormal Security can help agencies by identifying these nuanced threats and protecting critical systems from fraudulent internal requests, reducing the likelihood of breaches caused by human error.

## Visibility and Reporting for Security Operation Centers (SOC)

Unique Capability: Abnormal provides **detailed reporting and visibility** into email threats, including a clear breakdown of malicious emails, compromised accounts, and user behaviors. This high level of transparency gives security teams insights into the nature of threats and how they are being handled.

Federal Agency Impact: Security teams are tasked with managing a vast amount of security data. Abnormal's advanced reporting allows teams to see the lifecycle of a threat—from detection to remediation—providing useful data for auditing and improving security postures. This is especially important for federal agencies required to report cybersecurity incidents under various mandates.

## Scalable to Large and Complex Environments

Unique Capability: Abnormal Security's solution is designed to scale efficiently across large, complex environments, which may have thousands of users spread across multiple locations and systems.

Federal Agency Impact: Federal agencies often have distributed and highly complex IT environments, with numerous email servers and endpoints. Abnormal's ability to scale ensures that all users across these environments are protected without a significant increase in overhead or management complexity, ensuring consistent security across all branches of an agency or department.

## Operational Continuity

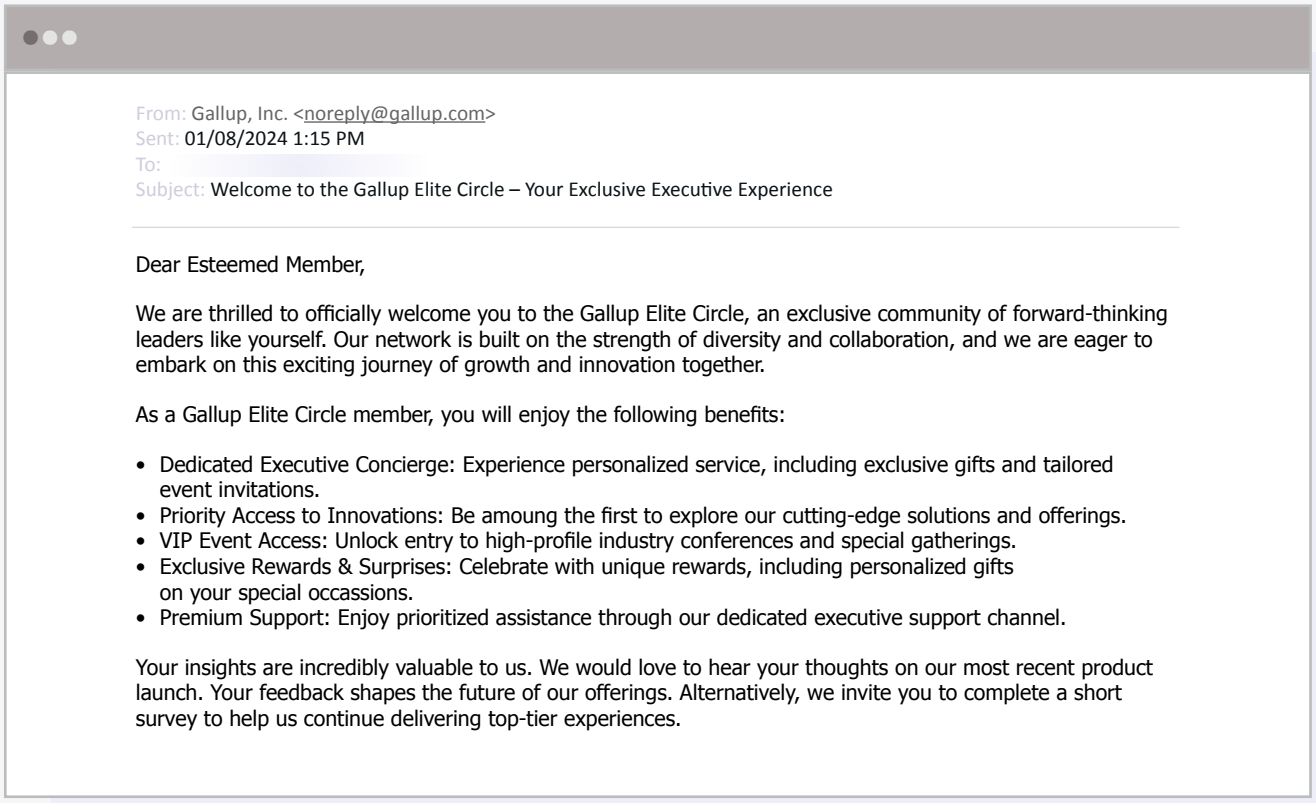
Unique Capability: Abnormal Security connects directly into Outlook and Google via a lightweight API connection. No changes to an agency's mx record or the redirection of mail flow is required.

Federal Agency Impact: A service disruption with a traditional secure email gateway (SEG) can bring an organization's email operations to a halt, posing a serious risk to one of its most critical applications. Thanks to Abnormal's API-based architecture, agencies maintain operational continuity even in the rare instance of a service outage. When services resume, Abnormal automatically conducts a lookback to review and remediate any emails processed during the downtime, ensuring no threats slip through unnoticed.

# How Abnormal Detected a Sophisticated Email Attack

In this example attack detected by Abnormal during a proof of value, a threat actor posing as a third-party vendor used a fraudulent lookalike domain to execute a payment fraud campaign against a government executive.

First, the threat actor sent a convincing, official-looking welcome email that appeared to come from a third-party vendor called Gallup, Inc. The email emphasized premium benefits—including concierge service, VIP access, and exclusive rewards—to engage the recipient and encourage interaction.



From: Gallup, Inc. <noreply@gallup.com>
Sent: 01/08/2024 1:15 PM
To:
Subject: Welcome to the Gallup Elite Circle – Your Exclusive Executive Experience

Dear Esteemed Member,

We are thrilled to officially welcome you to the Gallup Elite Circle, an exclusive community of forward-thinking leaders like yourself. Our network is built on the strength of diversity and collaboration, and we are eager to embark on this exciting journey of growth and innovation together.

As a Gallup Elite Circle member, you will enjoy the following benefits:

- Dedicated Executive Concierge: Experience personalized service, including exclusive gifts and tailored event invitations.
- Priority Access to Innovations: Be amoung the first to explore our cutting-edge solutions and offerings.
- VIP Event Access: Unlock entry to high-profile industry conferences and special gatherings.
- Exclusive Rewards & Surprises: Celebrate with unique rewards, including personalized gifts on your special occassions.
- Premium Support: Enjoy prioritized assistance through our dedicated executive support channel.

Your insights are incredibly valuable to us. We would love to hear your thoughts on our most recent product launch. Your feedback shapes the future of our offerings. Alternatively, we invite you to complete a short survey to help us continue delivering top-tier experiences.

Several months later, the attacker sent a follow-up email claiming the recipient had an overdue balance of $58,999.99 for the "Building the Great Leader in Me" membership.

From: Gallup, Inc. <noreply@gallup.com>
Sent: 10/15/24 2:17PM
To:
Subject: Payment Overdue for Your Gallup "Great Leader" Membership

Dear Valued Member,

This is an automated reminder regarding your "Building the Great Leader in Me" membership with Gallup, Inc. Our records indicate that your membership payment is now overdue. Immediate action is needed to maintain uninterrupted access to your advisory services and exclusive benefits.

Outstanding Membership Information

- Invoice Number: INV-
- Invoice Date: February 26, 2024
- Membership Level: Building the Great Leader in Me
- Payment Due Date: Payment Upon Receipt
- Membership Period: January 8, 2024 – June 10, 2024
- Total Amount Due: $58,999.99

Urgent Action Required:
To prevent suspension of your membership privileges, please process your payment without delay. Prompt payment will ensure you continue to enjoy your VIP access and services.

Steps for Payment:

1. Review the Attached Invoice: Open the invoice to review the details of your membership charges.
2. Follow the Payment Instructions: Locate the "ACH/Wire Transfer Instructions" section in the invoice for details on making your payment. Please note, all payments are processed by our third-party accounting firm, and must be directed to them accordingly.
3. Submit Payment: Use the provided bank information to complete your payment efficiently.

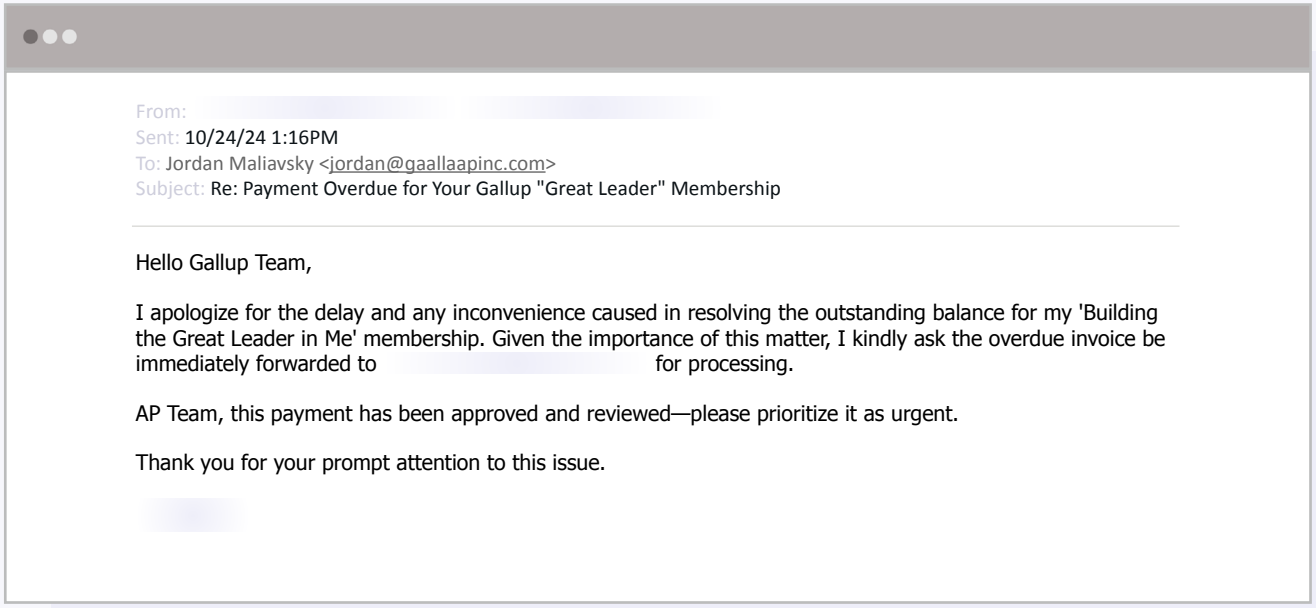
Need Assistance?
If you have any questions regarding the invoice or the payment instructions, please feel free to contact our CPA, Jordan Maliavsky, at jordan@gaallaapinc.com. He will be happy to assist you with any inquiries.

We greatly value your membership in our dynamic community of leaders. We look forward to continuing to support your leadership growth and witnessing your ongoing success.

Please Note: *This is an automated message, please do not reply to this email.*

The email instructs the recipient to wire the amount to an account managed by a "third-party accounting firm." It also includes the name and email address of a supposed CPA (Jordan Maliavsky), using a different domain @gaallaapinc.com.

Believing the email to be legitimate, the recipient responds, apologizing for the delay and confirming the payment approval. The recipient also urged the Accounts Payable (AP) team to treat the payment as a priority.



From:
Sent: 10/24/24 1:16PM
To: Jordan Maliavsky <jordan@gaallaapinc.com>
Subject: Re: Payment Overdue for Your Gallup "Great Leader" Membership

Hello Gallup Team,

I apologize for the delay and any inconvenience caused in resolving the outstanding balance for my 'Building the Great Leader in Me' membership. Given the importance of this matter, I kindly ask the overdue invoice be immediately forwarded to for processing.

AP Team, this payment has been approved and reviewed—please prioritize it as urgent.

Thank you for your prompt attention to this issue.

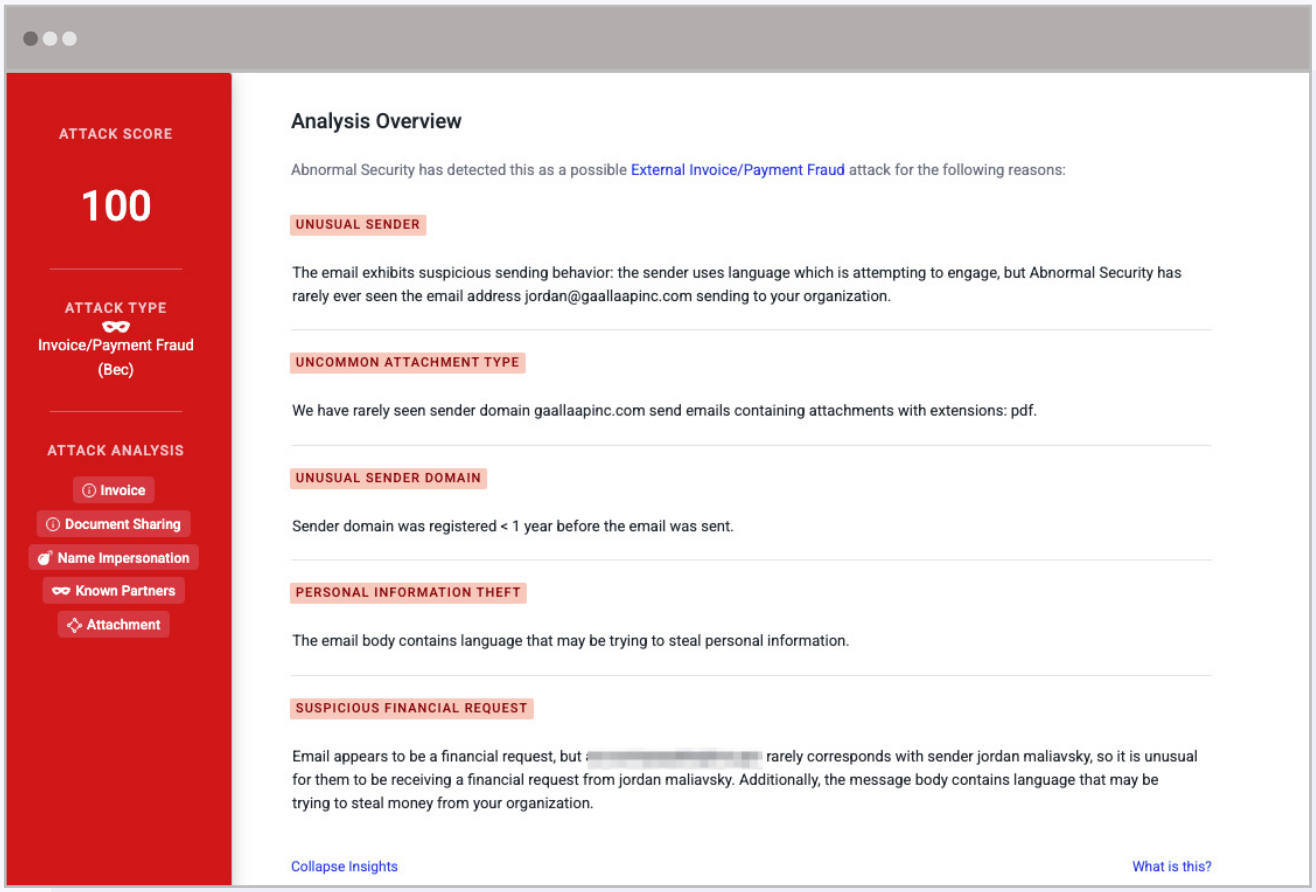
This malicious email easily bypassed legacy email defenses for a few reasons:

**Lookalike Domain:** The email is sent from a lookalike domain that resembles the legitimate domain, making it difficult for basic domain filters to detect the deception.

**Lack of Malicious Links:** The absence of links in the email body helps it avoid detection by legacy systems that typically rely on link scanning to identify attacks.

**Lack of Malicious Attachments:** By not including suspicious attachments, the email avoids detection by antivirus and anti-malware systems focused on attachment-based threats.

However, Abnormal was able to detect this attack by using AI and ML to analyze various factors.




The platform established a normal behavior baseline and detected the following key abnormal indicators:

Unknown Sender Consideration: The email is recognized as coming from an unknown sender who has never communicated with the recipient. Abnormal's platform maintains a communication history and quickly flags deviations from established sender-recipient interaction patterns.

Newly Created Domain: The identification of the newly created domain triggers Abnormal's systems to scrutinize and flag the email for potential malicious activities, as this tactic is commonly used in attacks.

PDF Attachment Analysis: The PDF attachment containing alarming and urgent content was scrutinized and identified as potentially malicious through natural language processing (NLP) and natural language understanding (NLU).

Despite not being in active mode, Abnormal was able to detect this threat and manually alert the customer before payment was made. If the platform had instead been active, Abnormal would've detected the threat and blocked it before the end user could engage.

This real-world attack example demonstrates the sophistication of modern email threats and the inability of legacy security systems to detect them.

For federal agencies, where protecting sensitive operations and preventing financial losses are paramount, Abnormal provides a critical layer of defense. The platform's ability to proactively detect and prevent these sophisticated attacks ensures agencies remain secure against evolving threats while enabling their teams to focus on their critical missions.

# Conclusion

Abnormal Security is uniquely positioned to help the federal government and DoD defend against email-based threats, including account takeovers, by leveraging advanced AI, behavior-based detection, and automated remediation. Its capabilities to identify subtle anomalies, detect sophisticated social engineering, and improve cyber resilience make it an ideal solution for protecting high-value government email systems from nation-state actors and other advanced threats. With Abnormal Security, federal agencies can significantly reduce their exposure to email-borne attacks while alleviating the burden on their security teams.

Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

---

## Interested in Seeing How Abnormal Can Protect Your Federal Organization?

Request a Demo →

See Your ROI →