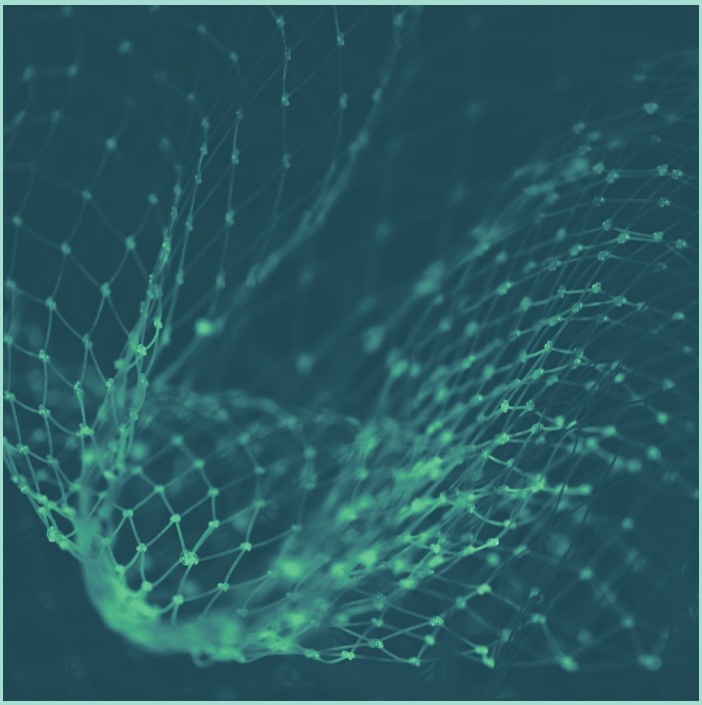
Abnormal

ABX: Abnormal Behavior Technology

/ Advanced Behavioral AI to Protect Your Cloud Communications



Executive Summary

Email has been the leading attack vector for cyberattacks for years, partially due to its ubiquity and partially because it is easy to infiltrate. Security organizations have responded by investing heavily in email security solutions to combat everything from commodity spam to ransomware hidden in attachments to credential phishing. And yet, losses continue to grow, despite an increase in tools and overall employee awareness.

Business email compromise (BEC) is one of the most pernicious threats for organizations today, with **$2.4 billion** lost in 2021 alone. The FBI Internet Crime Complaint Center (IC3) has reported that over 35% of all cybercrime losses in 2021 were to BEC—making it the most financially devastating cybercrime for the last five years running, with exposed losses of $43 billion.

To evade detection from traditional email security solutions, these increasingly sophisticated attacks use social engineering to bypass the secure email gateway and land in inboxes. Or, attackers enter through additional threat vectors like third-party apps connected to an email tenant. And as the most business-critical communications platform, the importance of email security cannot be understated.

Clearly, a new approach is needed to defend enterprises and to reclaim confidence and trust in email—the most critical business communication medium. Abnormal Behavior Technology (ABX) leverages a behavioral AI engine to provide a revolutionary approach to detecting email attacks. **ABX leverages identity, context, and risk awareness to detect threats in your inbound email and across the email platform.**

These three elements are what make Abnormal the most effective security platform on the market. Through an API integration, Abnormal ingests thousands of internal and external signals to make the platform **identity aware**. Leveraging knowledge bases of identities constructed and a baseline of their known-normal behaviors, Abnormal also analyzes the relationships between identities, making it **context aware**. And ABX analyzes the risk of each piece of content through NLP and NLU models to identify anomalies of an email, making it **risk aware**. Taken together, the robust ingestion of external and internal identities, their contextual relationships, and the content risk analysis allows ABX to arrive at high-confidence detection of the toughest socially-engineered email attacks.

And unlike other email security solutions, there is no need to perform any tuning to deliver or maintain this high degree of effectiveness. Deployment is fast and simple through an API integration into Microsoft 365 or Google Workspace.

35%

Business email compromise accounted for 35% of all cybercrime losses in 2021.

Abnormal™

Table of Contents

The Problem With Email Security

Socially-engineered attacks such as business email compromise evade traditional email security solutions because they lack the common threat signals that trigger a detection in most security solutions. These attacks do not have attachments carrying malware nor do they contain links leading to malicious websites. The content of the email is generally simple, and the attacks are typically customized for each individual target.

BEC attacks, by nature, represent a small portion of the total email attack vector. These attacks are nearly always hand-crafted and incorporate heavy elements of social engineering, and thus their fraction of all email threats is small—but these attacks disproportionately represent the greatest financial risk.

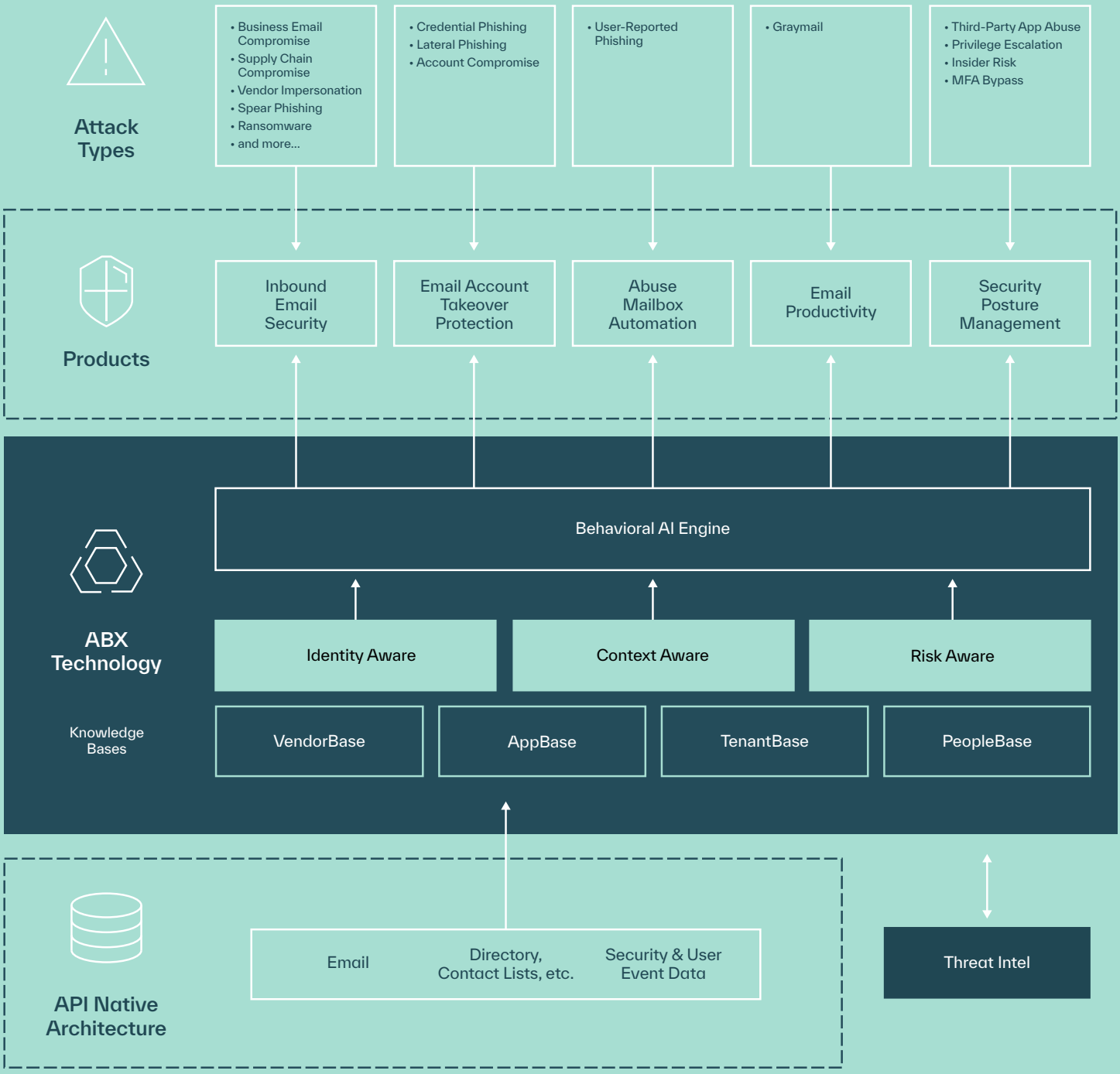
And unfortunately, cybercriminals are not stopping at BEC as they look for other ways to infiltrate email. Comprehensive cloud email security must go beyond inbound email security and fortify other entry points into the email platform to avoid account takeovers and the resulting internal attacks that can wreak havoc on an organization.

As a result, organizations must take a holistic approach to identify and remediate not only the business email compromise attacks of today, but also the costly email platform attacks that will continue to emerge in the future.

Abnormal Behavior Technology is rooted in decades of experience in machine learning focused on understanding user behaviors with large-scale data science platforms. That experience is now put toward understanding behaviors, context, and risk of every event in your cloud email environment, to detect and prevent even the most sophisticated attacks.

The Attack Framework

Abnormal Security has developed the following framework to provide insight into how ABX identifies and addresses socially-engineered email attacks.



Types of Attacks Stopped by Abnormal

Executive Impersonation

Pretext
Internal Employee

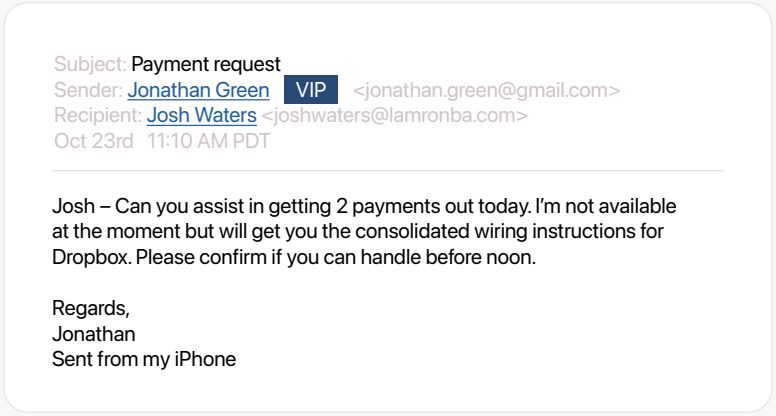
Approach
Impersonation

Delivery
No Payload

Executive impersonation is a common example of BEC and one of the easiest for attackers to execute. These attacks are very challenging to detect due to their simplicity and frankly, their elegance.

These emails often come from reliable and known webmail services such as Gmail. Due to the widespread use and general business need to communicate to individuals using these services, emails from those sending domains cannot be simply blocked.

Some enterprises implement rules for each executive by providing specific allowances for personal email addresses, but this is neither a foolproof nor a scalable solution. To better detect holistic anomalies indicating impersonation, tools need to baseline additional known-normal identity signals like location, IP, and time of day, as well as the tone, topic, and content of the email itself.


Subject: Payment request
Sender: Jonathan Green VIP <jonathan.green@gmail.com>
Recipient: Josh Waters <joshwaters@lamronba.com>
Oct 23rd 11:10 AM PDT

Josh – Can you assist in getting 2 payments out today. I'm not available at the moment but will get you the consolidated wiring instructions for Dropbox. Please confirm if you can handle before noon.

Regards,
Jonathan
Sent from my iPhone

Vendor Email Compromise

Pretext
External Partner

Approach
Compromised Account

Delivery
No Payload

When emails are sent from compromised vendor accounts, they are extremely difficult to identify because there are no traditional indicators that the email is malicious. The emails are sent from trusted sources and attackers may reply to an existing email thread to add further credibility. Context awareness of the typical relationship and risk awareness of the typical content between identities can stop this type of attack in its tracks. In order to stop these types of attacks, email security solutions must understand typical vendor-customer behavior and identify risk when signals, such as new banking information, associated with nefarious activity are included in an email.

Subject: Re: Payment status
Sender: Lucia Foreman <jluciaforeman@proliasystems.com>
Recipient: Renee West VIP <renee.west@lamronba.com>
Reply-to: Lucia Foreman <jluciaforeman@prolia-systems.com>
Oct 23rd 09:12 AM PDT

Hi Renee,
Update – we are moving to a new bank and will be requesting a change of payment information (new details in attachment). Please handle at your earliest convenience. Thanks

On Friday, Oct 01, 2022 at 08:58 AM Renee West <renee.west@lamronba.com> wrote:
Hi Lucia, thanks for confirming. Have a great weekend!
Cordially, Renee

On Friday, Oct 01, 2022 at 08:33 AM Lucia Foreman <luciaforeman@proliasystems.com> wrote:
Hi Renee,

Employee Compromise

Pretext
Internal Employee

Approach
Compromised Account

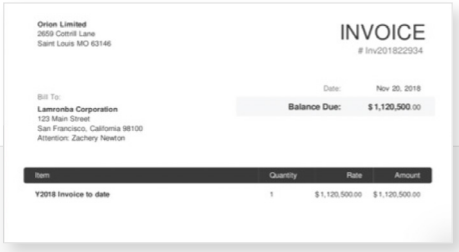
Delivery
No Payload

Like compromised vendor accounts, attacks from internally compromised accounts are also extremely difficult to identify. The emails come from trusted employees, may reference legitimate business information, and may bypass security tools that do not scan east-west mailflow. Once an attacker has gained access to an internal email account, he can use it to uncover information, move through connected applications, or send additional attacks to employees and customers, often for long periods of time without detection.

Subject: Orion Limited Invoice
Sender: Renee West VIP <renee.west@lamronba.com>
Recipient: Josh Waters <renee.west@lamronba.com>
Oct 23rd 02:46 PM PDT

Zachary and Josh,
Please review the attached – I have approved this wire transfer and it should be prepared for immediate release.

Thanks,
Renee West
Treasurer
www.lamronba.com



Abnormal™

Credential Phishing

Pretext
Brand

Approach
Impersonation

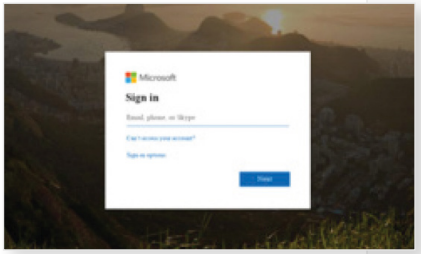
Delivery
Link to Credential Phishing Website

Most credential phishing attempts use impersonation of a known brand, such as Microsoft, Amazon, LinkedIn, Google, or another large organization that the recipient is likely to recognize. And once the recipient has entered their credentials, the attacker can use them to gain access to the account and all associated information.

While some email security solutions may detect these attacks, particularly if they use high entropy or previously seen URLs, these attacks are difficult to reliably catch without the risk awareness and known-normal identity baselines. The fact that credential phishing sites typically do not contain malware makes typical sandboxing approaches ineffective.

Subject: Microsoft365 password expiry notice!!!
Sender: Acme Microsoft Support <microsoft@acme.com>
Recipient: Adam Smith <Asmith@acme.com>
Nov 24th 05:30 PM PST

Password expiry notice!!!



User name: asmith@acme.com

Here's what to do next:

- Click the link below.
- Use the button below to re-confirm and continue with the same password.

Re-activate Password

If this issue isn't resolved, your subscription and any data you may have stored in it will be permanently deleted on 31 November 2022.

Sincerely,
The Acme Microsoft Support Team

MFA Bypass

Pretext
Internal Employee

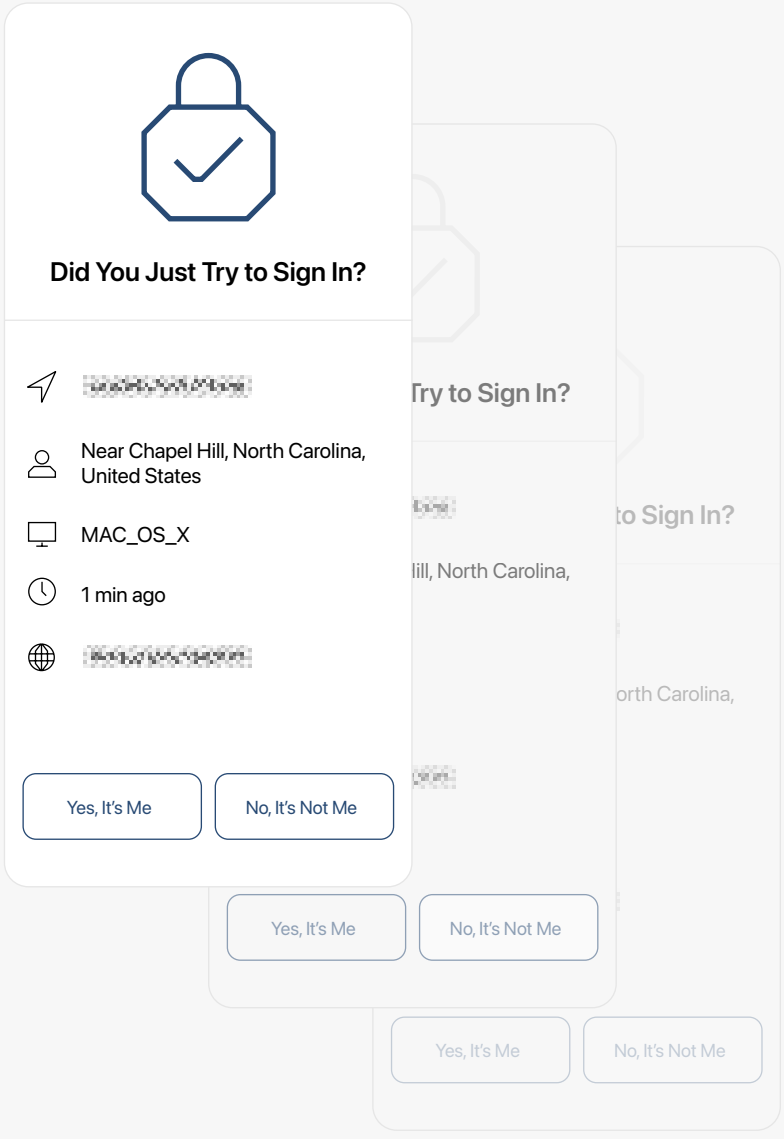
Approach
Exploiting Conditional Access Misconfiguration; Brute Force

Delivery
Legacy Authentication Exploitation; Push Notification Spam

In some instances, attackers may choose to access the account itself versus sending an inbound email attack. When multi-factor authentication is enabled, they must determine how to bypass that added security functionality, which can be done in a variety of ways.

A pure MFA bypass attack often takes the form of an attacker downgrading their OS or using an older version of the mail application to take advantage of legacy authentication that was not configured to support MFA. By doing so, attackers can simply use an older version of Outlook to gain access to an organization's cloud email platform by inputting stolen credentials—no additional authentication required.

However, if legacy authentication is disabled, attackers may take a more direct approach by targeting the users whose credentials have been stolen with a deluge of MFA push notifications—wearing the user down until they simply accept the authentication attempt and provide the attacker with access. Ensuring that security teams know when MFA has been bypassed is essential to keeping accounts secure.



Abnormal™

Malicious or Over-Permissioned Third-Party Applications

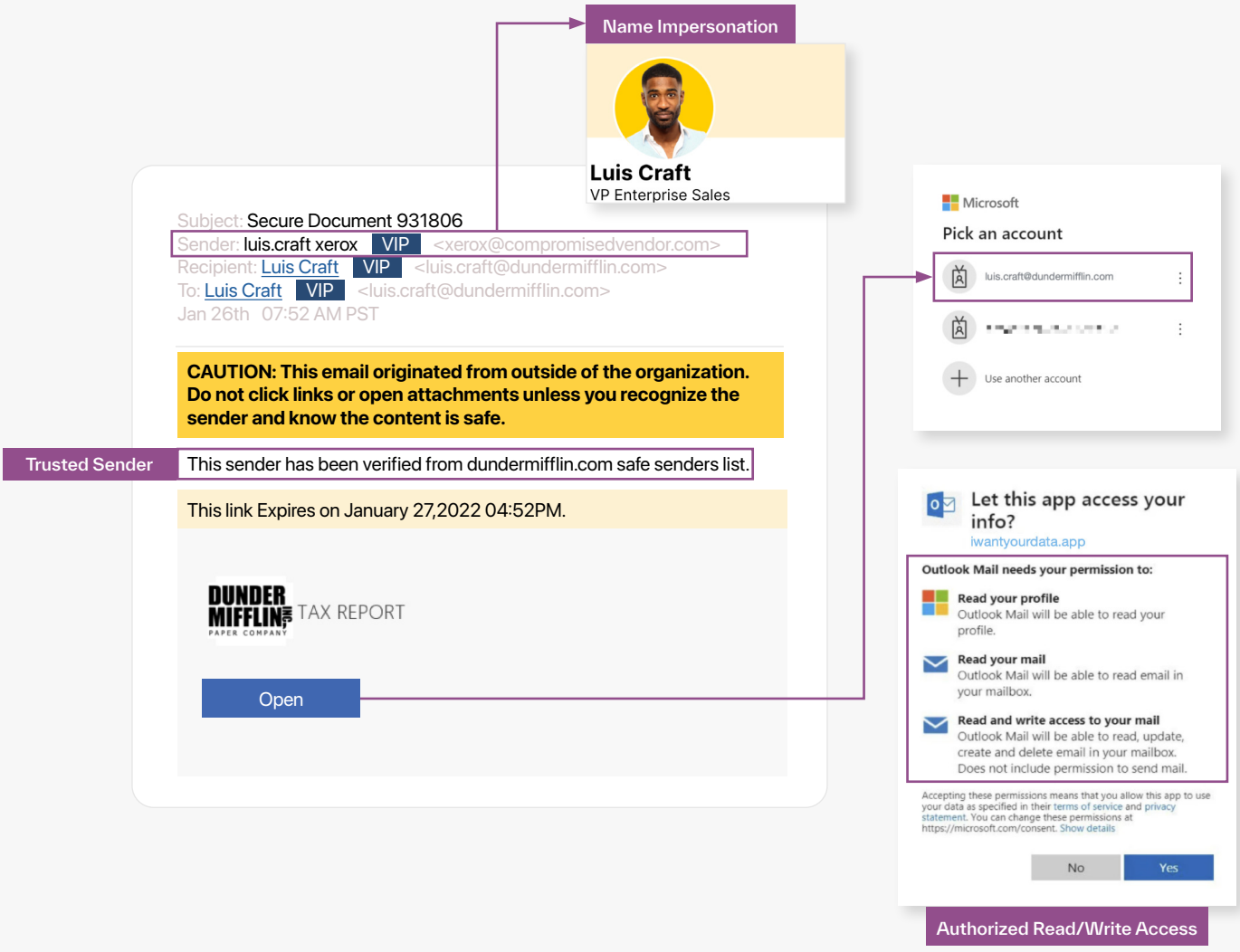
Pretext
Internal Employee

Approach
Updating App Permissions

Delivery
API Integration

As with most attacks, third-party application attacks tend to begin with phishing emails. However, rather than asking the target to sign in to a service, these attacks ask recipients to authenticate new third-party applications. These applications often grant read/write permissions—giving attackers unfettered access to an organization's calendars and mailboxes. Alternatively, attackers can also infiltrate legitimate applications, such as those used to spellcheck emails or simplify calendars, and use that access to complete their attack on the email platform.

Surfacing changes in permission identities of third-party apps and their user permissions to monitor over-permissioned identities is crucial to closing these gaps in email platform security.



Stopping Attacks by Understanding Identity

In the wake of successful attacks, investigations from security teams expand beyond the scope of just the email. Examples of investigative activities may include:

- Looking to identify the sender and whom they were impersonating.
- Contacting an executive to verify personal email accounts and confirm an executive impersonation.
- Contacting an impersonated vendor to verify bank account information, especially if the attacker had posed as a vendor and requested a change to account information.
- Reviewing logs of internal accounts for evidence of a compromised account.
- Reviewing multi-factor authentication records to see if and how MFA was bypassed.
- Understanding the read-write access permissions of third-party apps with access to the email platform and verifying the legitimate business need for each application.

Unfortunately, none of the traditional email security solutions perform these activities while attempting to identify and block a socially-engineered inbound email attack or a targeted email platform attack.

In contrast, ABX learns from each customer environment, uniquely leveraging a broad set of organization-specific data to protect the enterprise. By doing so, Abnormal can detect and stop the attacks that other solutions miss.

A Deep Dive into Abnormal Behavior Technology

Abnormal Behavior Technology, or ABX, looks beyond email data and redefines the scope of behavioral analysis. **ABX takes a data science approach, analyzing dozens of data sources specific to each organization to arrive at high-confidence decisions** to block targeted inbound email attacks and email platform attacks.

The roots of ABX derive from experience within the advertising technology space, where data scientists honed their craft analyzing user behaviors. By understanding the identity of each user within the environment using data across Microsoft 365 and Google Workspace, organization-specific inputs can be leveraged to identify email attacks.

ABX ingests and analyzes the rich data from dozens of data sources to profile communications across three distinct categories to provide:

- ✓ Identity Awareness
- ✓ Context Awareness
- ✓ Risk Awareness

The results of the analysis across these three areas are then consolidated by an ensemble of machine learning algorithms to ensure a high-confidence verdict of whether a threat exists in the email platform—minimizing the false positives that plague traditional machine learning algorithms.

Abnormal™

01. Abnormal Identity Awareness

Abnormal Identity Awareness is a stateful model that ingests thousands of internal and external identities. For employees, ABX takes inputs from the directory, analyzes user events, and analyzes email communications, resulting in models for each employee. The attributes for each internal identity include:

Employee Identity Model

Name	Email	Role
Personal Email	Location	Sign-In Locations
Manager	Manager Location	Department
VIP Status	Office Address	Phone Number
Term at Company	Browsers Used	Devices Used
Usual Login Time	Mail Filter Configuration	Client Application Used
Mailing Address		

To create models for external entities, ABX evaluates the email communications in detail to extract identity attributes.

Vendor Identity Model

Vendor Name	Email Used for Communication	Key Vendor Contacts
Key Internal Contacts	Mailing Address	Verified Email FQDN
Phone	Invoicing Software	Invoicing Cadence
Key Vendor Contacts	Key Internal Contacts	Bank Information / Accounts
Invoicing Language	Last Contacted	Phone
Years of Relationship		

Customer Identity Model

Customer Name	Customer Emails	Key Customer Contacts
Key Internal Contacts	Mailing Address	Verified Email FQDN
Phone	Invoice Frequency	Last Contacted
Years of Relationship	Communication Cadence	

To create models to detect anomalous activity from third-party apps, ABX ingests and monitors the identities of each application to secure the organization's posture from malicious third-party apps.

Third-Party Application Model

Installed Application	Application Name	Release Date
Version	Read Access	Write Access
Number of Applications		

To create models that monitor changes and configuration risks that exist in the tenant, ABX ingests and baselines behaviors of the identities in each tenant.

Tenant Model

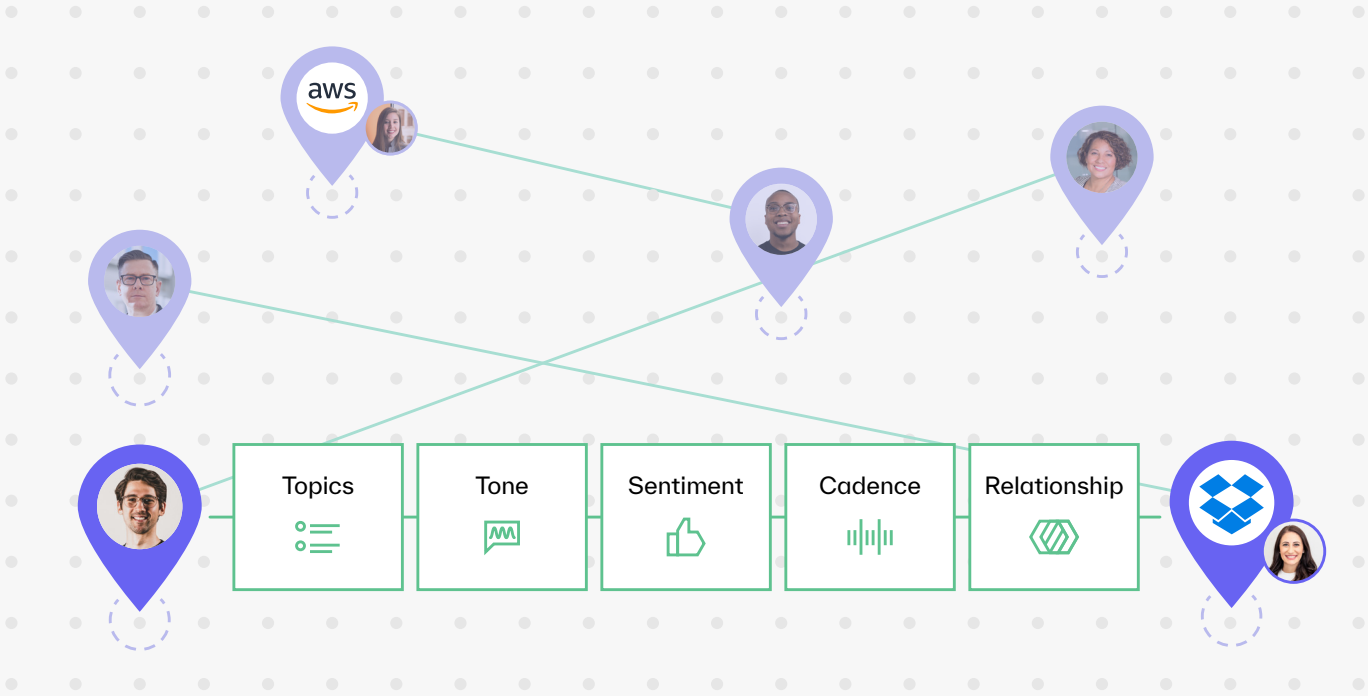
Number of Tenants	Name of Tenant/Platform
Permissions in Tenant	New Users Added
	Date of New Users Added

ABX ingests thousands of signals from both internal and external entities to build out baselines of the known normal behaviors of those identities, making it identity-aware.

02. Abnormal Context Awareness

Once ABX understands identity, the platform can profile the communication patterns between individuals, departments, and organizations to create a contextual relationship graph, which is continually updated. Abnormal Context Awareness provides an understanding of the strength of each connection by analyzing the frequency of communication along with the topic and tone of each email.

Unusual communications can be identified from rare or never-before-seen paths. Alternatively, normal communication paths that have abnormal topics and sentiment may indicate suspicious activity.



ABX understands the strength of each connection, the structure of the organization, and the frequency of communication among identities, along with the intent, sentiment, and tone of each email communication, making it context aware.

Abnormal™

03. Abnormal Risk Awareness

The risk of each event in the email platform is analyzed by ABX using a variety of techniques, including:

Deep URL Analysis

Abnormal does structural link analysis and follows links to see what an end user would be exposed to after clicking a link within an email. URLs contained within attachments are also analyzed.

Extraction Techniques

Abnormal scans and extracts text from within images and other attachments to inform the intent of the message. Attachments are also scanned for malware and the platform detects malicious signals such as macros, executables, javascript, and password protection associated with the files.

Natural Language Algorithms

Natural language understanding (NLU) algorithms identify topic, tone, and sentiment within all communications. Costly business email compromise attacks typically feature urgent requests on financial topics, so identifying these types of communications can assist in the accurate detection of attacks.

Natural language processing (NLP) algorithms are also used to help establish the contextual relationships that explain and score the types of communication, such as formal vs. informal, that are occurring between individuals, departments, and organizations.

Threat Intelligence

In addition, ABX leverages a threat intelligence API and extracts key traditional indicators of compromise including links, domains, and sender attributes. These signals provide additional insight into attacks to help ABX make a final decision on whether an email is malicious.

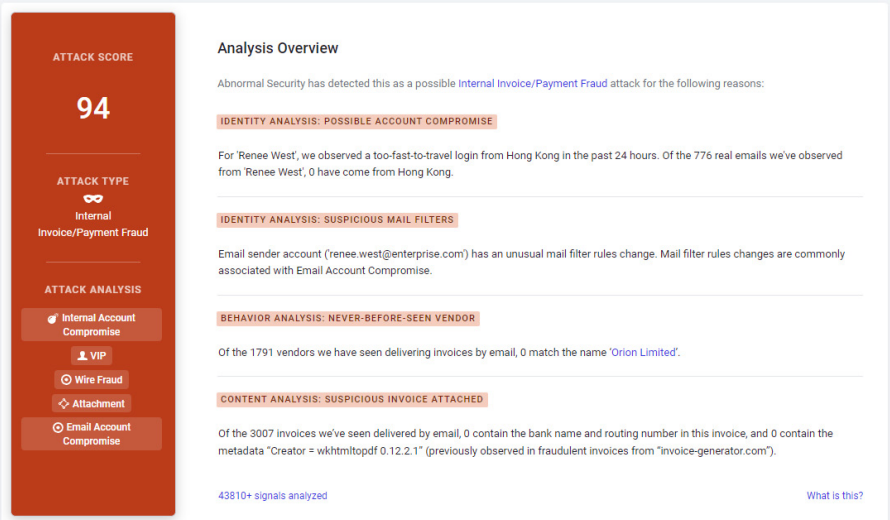
ABX leverages NLU to understand risks, NLP to explain its insights, and pairs threat intel with the analysis of each event in the email platform to determine the level of risk, making it risk aware.

04. Composite Analysis

An ensemble of machine learning algorithms evaluates the signals generated by the trio of perspectives from the pillars of Identity Awareness, Context Awareness, and Risk Awareness. By doing so, the algorithms identify specific types of attacks and techniques through multiple algorithms, which results in the delivery of a final email disposition alongside clear, concise, and explainable insights for the security analyst to review.

Most solutions that leverage machine learning technologies result in “black-box” outputs. Some results make sense. Others may not, but security analysts have no mechanism for understanding why and how the algorithms reached a specific conclusion.

In contrast, the Abnormal decision engine explains and summarizes the automated analysis of thousands of signals that were used to detect the attack, providing a full analysis overview with details on why the email was blocked or removed and summed up in an attack score.



Automated analysis and attack classification provide a clear overview to assist with next steps.

With these insights across identity, context, and risk, SOC analysts can more quickly take action to remediate attacks, address downstream impacts, and educate the organization in real-time about emerging attack types.

Abnormal™

Powering the Abnormal Cloud Email Security Platform

Abnormal Behavior Technology powers the Abnormal Security platform to protect organizations with complete cloud email security. The solution is designed to augment Microsoft 365 and Google Workspace to allow organizations to remove legacy security solutions that cannot stop modern attacks.

The native security capabilities of Microsoft 365 and Google Workspace handle the widespread threats, including broad spam and phishing campaigns, while Abnormal Security uses its unique behavioral approach to address the sophisticated, targeted inbound attacks and more advanced email platform attacks. Combined, the two platforms can stop the full spectrum of email threats.

The Abnormal Cloud Email Security platform provides five core capabilities:

01. Inbound Email Security
Stops the full range of email attacks, with a unique focus on modern social engineering attacks like business email compromise.

02. Email Account Takeover Protection
Looks beyond email and analyzes hundreds of signals to accurately detect and remediate compromised accounts.

03. Abuse Mailbox Automation
Assists security operations teams with automation and tools to respond quickly to email threats.

04. Email Productivity
Filters time-wasting emails from employee inboxes with an adaptive and policy-free approach.

05. Security Posture Management
Discovers and provides visibility into misconfiguration risks across the entire cloud environment.

Integrating via API provides access to a broad set of data to enable ABX to baseline and analyze a broader set of behaviors, as well as monitor intra-domain email traffic, including internal traffic, which traditional email security solutions are blind to. Additionally, the API-based architecture provides ease of integration and maintenance, with no MX record or mail routing changes required.

Powered by ABX, the Abnormal Cloud Email Security platform protects organizations with cloud-native email security designed to augment Microsoft 365 and Google Workspace.

Conclusion

Abnormal Behavior Technology uses a unique, data science-based approach to drive high-confidence detection of the toughest socially-engineered email attacks and vulnerabilities in the cloud email environment. ABX learns from each customer environment, uniquely leveraging a broad set of organization-specific data to protect your enterprise.

Combining identity awareness, context awareness, and risk awareness to drive accurate detection of email attacks, Abnormal Behavior Technology looks beyond email data to drive accurate detection of advanced inbound email and email platform attacks. As a result, Abnormal is uniquely equipped to protect email platforms from never-seen-before attacks that evade traditional email security solutions.