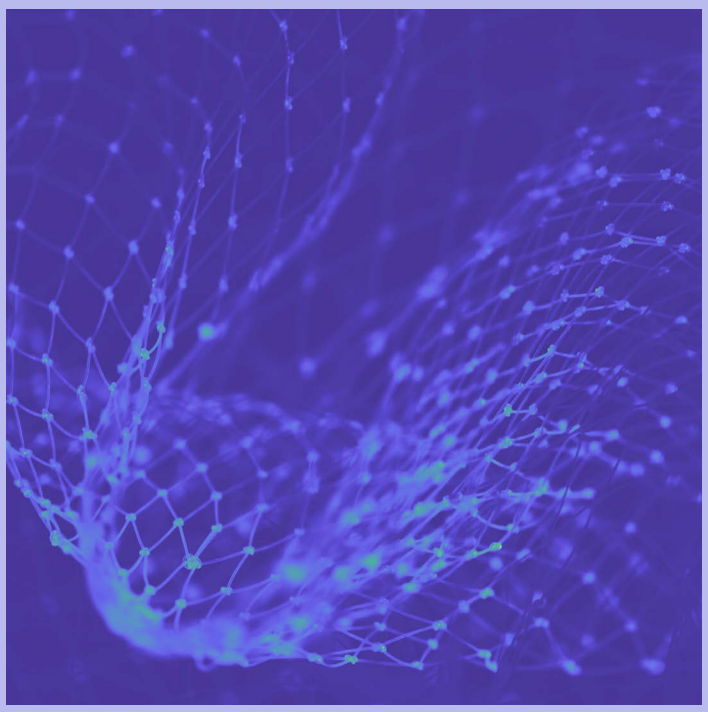
Abnormal

ABX: Abnormal Behavior Technology

/ Protecting Against Socially-Engineered Attacks



Executive Summary

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 35% of all cybercrime losses in 2021 were to BEC—making it the most financially devastating cybercrime for the last five years.

Email has been the leading attack vector for cyberattacks for years, partially due to its ubiquity and 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 in attachments to credential phishing. And yet, BEC losses continue to grow, despite an increase in tools and overall employee awareness.

To evade detection from traditional email security solutions, increasingly sophisticated attacks are often plain text and rely on social engineering to complete their schemes. This means the emails show few traditional indicators of compromise that a secure email gateway would detect. In addition, attacks are delivered from reliable domains (such as gmail.com) or via newly created infrastructure, thanks to the ease offered by cloud services, and thus bypass detection by reputation. 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 patent-pending techniques to provide a revolutionary approach to detecting targeted email attacks. This unique, data science-based approach allows ABX to arrive at high-confidence detection of the toughest socially-engineered email attacks. In addition, ABX learns from each customer environment, uniquely leveraging the broadest set of organization-specific data among all email security solutions to protect your enterprise.

By leveraging an API-based integration, deployment is fast and simple. And, unlike other email security solutions, there is no need for customers to perform any tuning to deliver or maintain the high degree of effectiveness.

35%

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

Abnormal™

Table of Contents

The Problem With Email Security

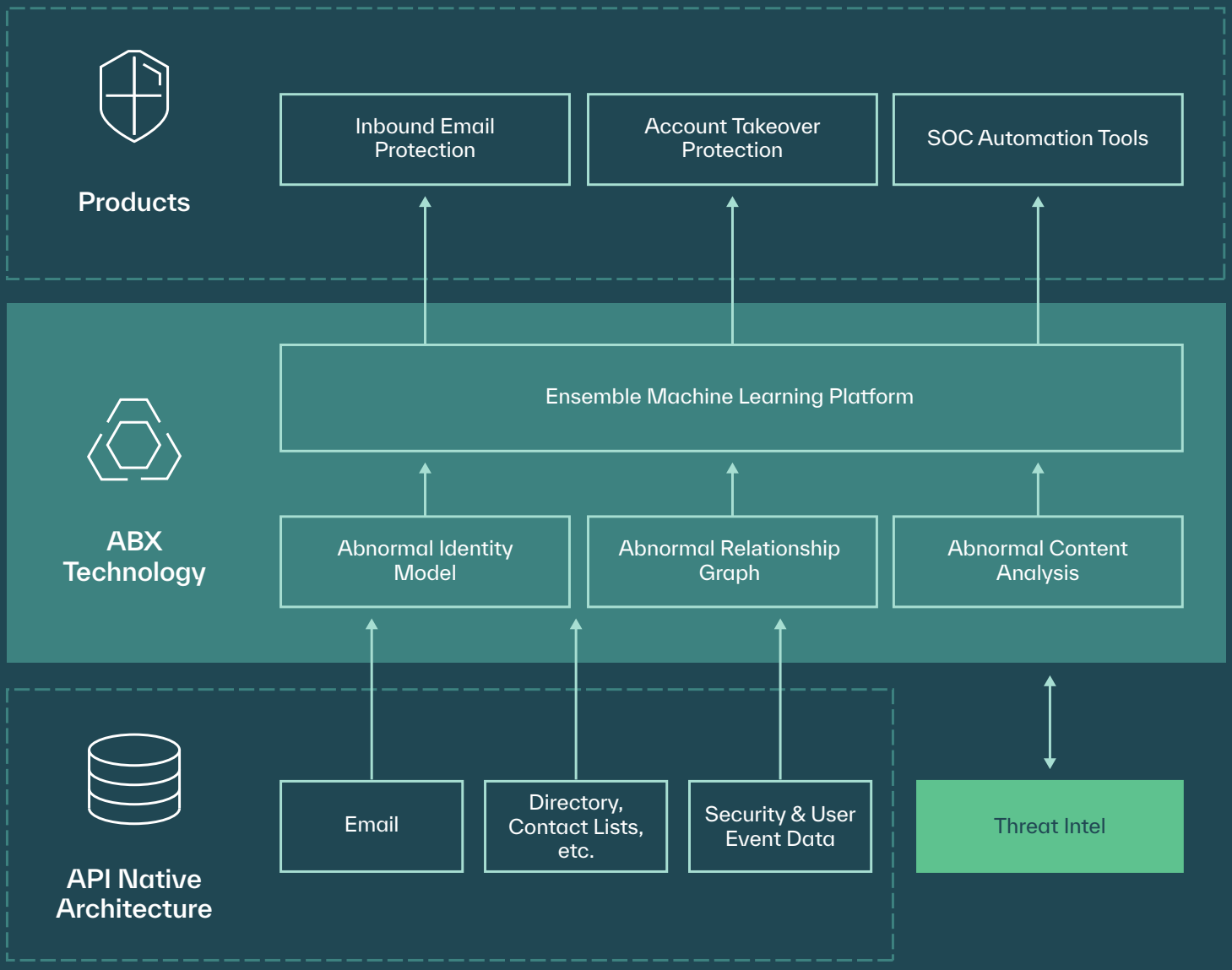
Socially-engineered attacks such as business email compromise evade traditional email security solutions because they lack the common threat signals to trigger a detection. These attacks do not have attachments carrying malware nor do they contain links leading to malicious websites. The content of the 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 resultingly tiny. As such, email security vendors who miss these attacks can still maintain claims of high efficacy rates due to the sheer volume of unwanted spam and malware campaigns they stop. That said, while a small percentage by comparison, business email compromise disproportionately represents the greatest financial risk and thus must be stopped.

The foundation of Abnormal Behavior Technology is rooted in decades of experience in advertising technology focused on understanding user behaviors with large-scale data science platforms.

The Attack Framework

Abnormal Security has developed the following framework to break down the different types of socially-engineered email attacks.



Examples of Emails That Bypass Traditional Solutions

Executive Impersonation

Pretext
Internal Employee

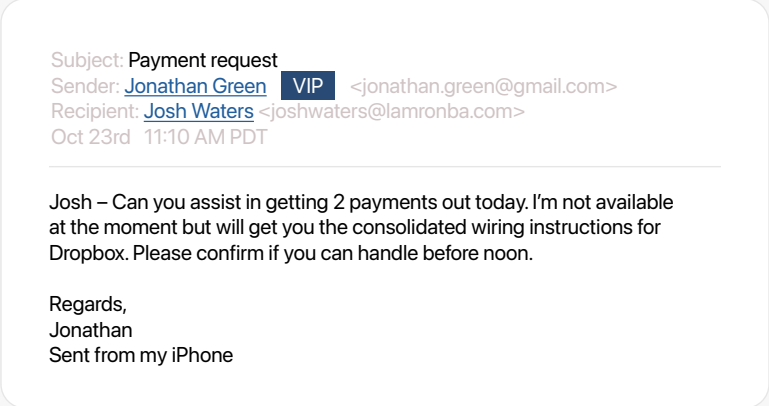
Approach
Impersonation

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.

Emails may be coming from reliable and known email 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 simply be 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.



Vendor Email Compromise

Pretext
External Partner

Approach
Compromised Account

Delivery
No Payload

Compromised vendor accounts are an extremely difficult attack to identify because there are no traditional indicators that the email is malicious. The emails come from trusted sources, and attackers may reply to an existing email thread to add further credibility.

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, 2021 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, 2021 at 08:33 AM Lucia Foreman <luciaforeman@proliasystems.com> wrote:
Hi Renee,

Employee Compromise

Pretext
Internal Employee

Approach
Compromised Account

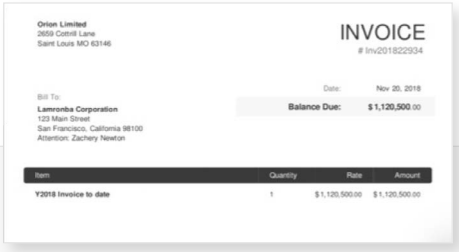
Delivery
No Payload

Like compromised vendor accounts, attacks from compromised internal accounts are also extremely difficult to identify. The emails come from trusted employees and may reference legitimate business information. Additionally, internal-to-internal correspondence (east-west domain mail flow) is not commonly scanned by traditional email security solutions. Once an attacker has gained access to an internal email account, he can use it to execute additional attacks, 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


Orion Limited
2659 Cottrill Lane
Saint Louis MO 63146

INVOICE
Inv201822934

Bill To:
Lamronba Corporation
123 Main Street
San Francisco, California 98100
Attention: Zachery Newton

Date: Nov 20, 2018
Balance Due: $ 1,120,500.00

Item	Quantity	Rate	Amount
Y2018 Invoice to date	1	$ 1,120,500.00	$ 1,120,500.00

Abnormal™

Credential Phishing

Pretext
Brand

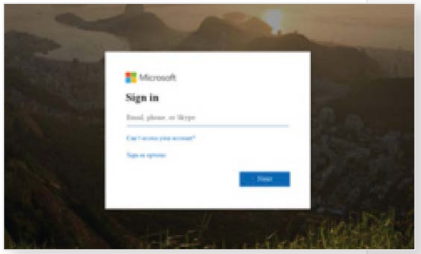
Approach
Impersonation

Delivery
Link to Credential Phishing Website

Most credential phishing attempts use content impersonating a known brand (such as Microsoft, Amazon, FedEx, Google, or another large organization) that the recipient is likely to recognize. While some email security solutions may detect these attacks (particularly if they use high entropy URLs or previously seen URLs), these attacks are still difficult to reliably catch—especially if they are new. The fact 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 2021.

Sincerely,
The Acme Microsoft Support Team

Looking Beyond the Email Itself

In the wake of successful BEC attacks, investigations from security teams expand beyond the scope of just the email. Examples of investigative activities stemming from a successful BEC attack include the following:

- Looking to identify the sender and whom they were impersonating.
- Contacting an executive to verify personal email accounts to confirm an executive impersonation.
- Contacting an impersonated vendor to verify bank account information, especially if the attacker had posed as a vendor and changed account information.
- Reviewing logs of internal accounts for evidence of a compromised account.

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

ABX learns from each customer environment, uniquely leveraging the broadest set of organization-specific data among all email security solutions to protect your enterprise.

Abnormal™

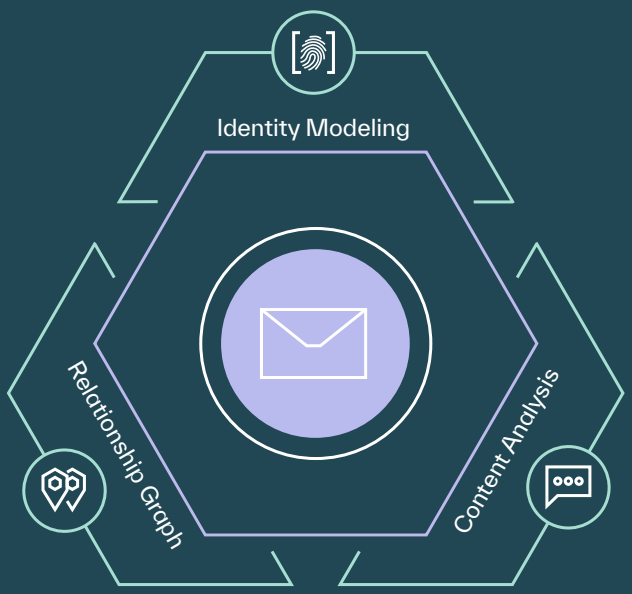
Abnormal Behavior Technology (ABX)

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. This enables ABX to arrive at high-confidence decisions to block targeted email attacks.

The roots of ABX derive from experience within the advertising technology space, where data scientists honed their craft by analyzing user behaviors. With expanded datasets available via email platform APIs from Microsoft 365 and Google Workspace, organization-specific inputs can now be leveraged to identify email attacks.

ABX analyzes the rich data from dozens of data sources to profile communications across three distinct perspectives:

- **Abnormal Identity Model**
- **Abnormal Relationship Graph**
- **Abnormal Content Analysis**



The results of the analysis are then consolidated by an ensemble of machine learning algorithms to ensure a high-confidence verdict. This minimizes the false positives that plague traditional machine learning algorithms.

Abnormal™

01. Abnormal Identity Model

The Abnormal Identity Model is a stateful model of both internal and external identities.

For employees, ABX takes inputs from the directory and analyzes user events as well as email communications, resulting in models for each employee. The attributes for each internal identity include the following:

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

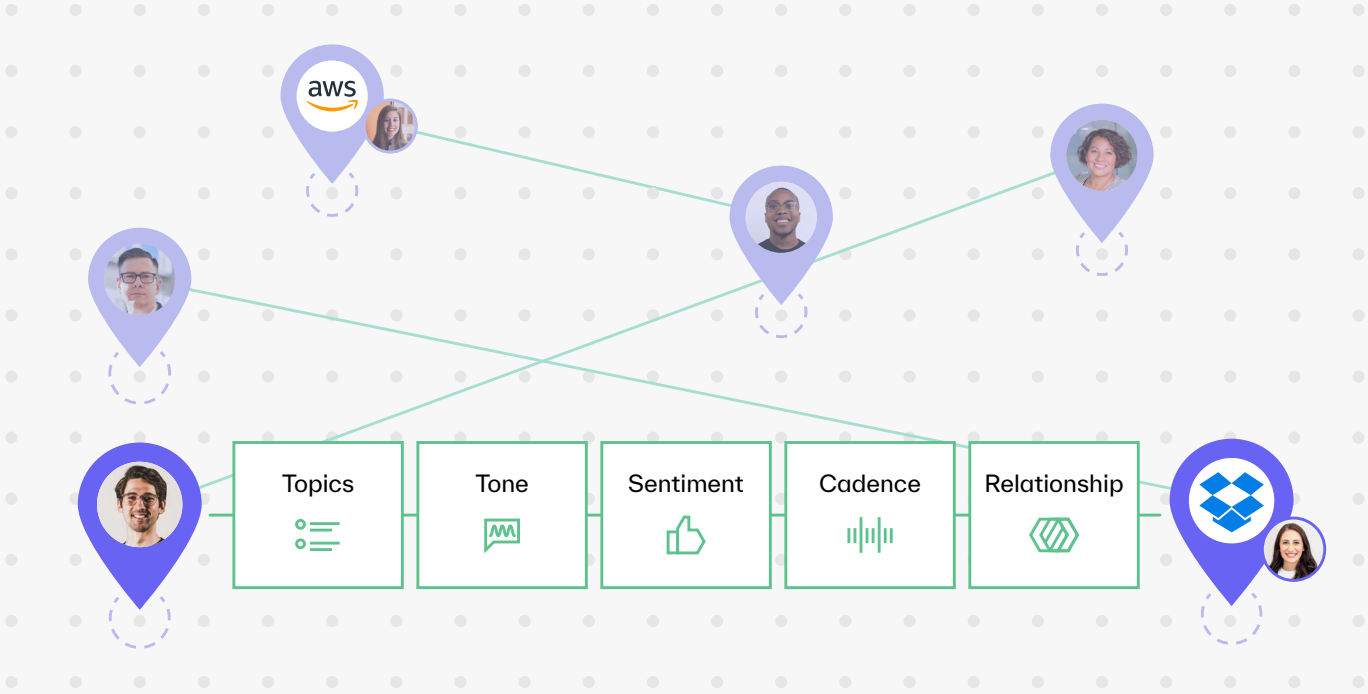
Customer Name	Customer Emails	Key Customer Contacts
Key Internal Contacts	Mailing Address	Verified Email FQDN
Phone	Invoice Frequency	Last Contacted
Years of Relationship	Communication Cadence	

ABX incorporates more sources of data than any other email security solution today.

02. Abnormal Relationship Graph

ABX profiles the communication patterns between individuals, departments, and organizations to create the Abnormal Relationship Graph, which is continually updated. The Abnormal Relationship Graph 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 may have abnormal topics and/or sentiment to indicate suspicious activity.



To understand the strength of each connection, ABX analyzes the frequency of communication along with the topic and tone of each email.

Abnormal™

03. Abnormal Content Analysis

ABX analyzes email content using a variety of techniques, including the following:

Deep URL Analysis

Link chains are followed to the final destination to ensure a complete and thorough analysis of what an end-user would be exposed to when clicking the link. URLs contained within attachments are also analyzed.

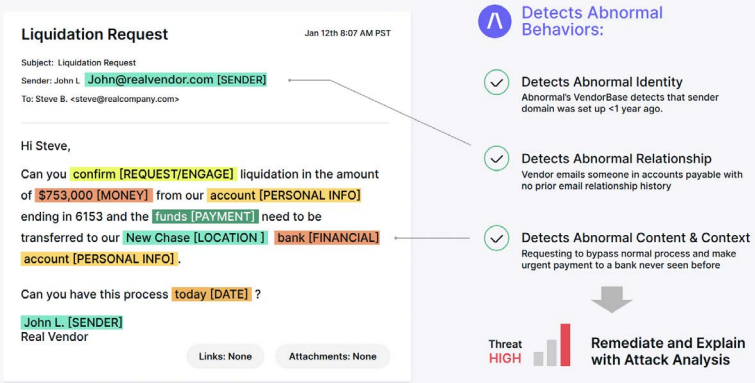
Computer Vision Techniques

Computer vision algorithms analyze URL landing pages to identify brand and form layouts. Attachments are also analyzed using these techniques to identify logos as well as extract information contained within the document.

Natural Language Processing

Natural language processing (NLP) 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.

NLP algorithms are also used to help establish the Abnormal Relationship Graph by understanding the communication (such as formal vs. informal) that are occurring between individuals, departments, and organizations.



Natural language processing (NLP) algorithms identify topic, tone, and sentiment.

Threat Intelligence

In addition, ABX leverages threat intelligence feeds to block known bad signals such as suspicious domains or malicious links.

Abnormal™

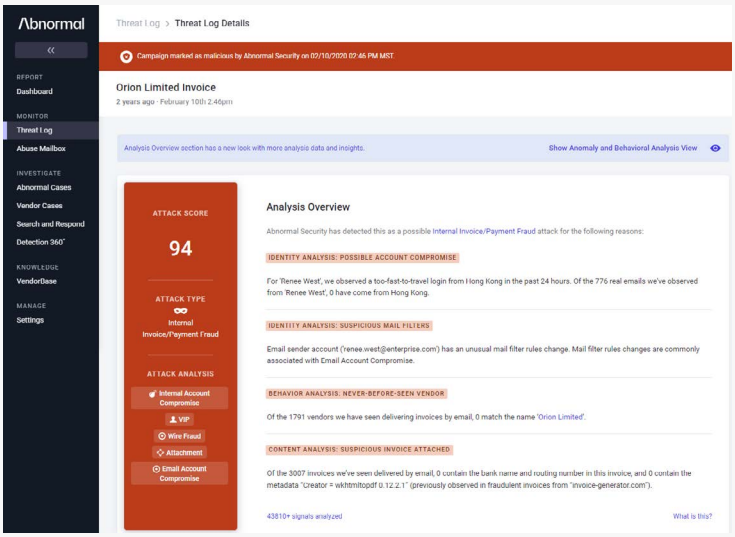
04. Composite Analysis: Ensemble Machine Learning Algorithms

An ensemble of machine learning algorithms evaluates the signals generated by the trio of perspectives from the Abnormal Identity Model, the Abnormal Relationship Graph, and the Abnormal Content Analysis. The algorithms identify specific types of attacks and techniques, which results in a final email analysis. This is delivered along with clear, concise, and explainable insights for the human analyst to review.

Explainable Insights

Most solutions that leverage machine learning technologies result in “black-box” outputs. Some results make sense; others may not. Either way, users have no mechanism of understanding why and how the algorithms reached a specific conclusion.

The Abnormal decision engine explains and summarizes the automated analysis of thousands of signals that were used to detect the attack. Users can view a full analysis overview with details on why the email was blocked or removed.



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

Abnormal™

The Abnormal Integrated Cloud Email Security Platform

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

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 attacks.

The Abnormal Integrated Cloud Email Security Platform provides three core capabilities:

01. Inbound Email Protection

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

02. Account Takeover Protection

Looks beyond email and analyzes hundreds of signals to accurately detect compromised accounts.

03. SOC Automation for Email Response

Assists security operations teams with automation and tools to respond quickly to email threats.

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

Integrating via API provides access to a broad set of data that enables ABX to analyze behaviors and monitor intra-domain email traffic. This includes internal traffic, which is generally a blind spot for traditional email security solutions. Additionally, the API-based architecture provides ease of integration and maintenance, with no mail exchange (MX) record or mail routing changes required.

Abnormal™

Conclusion

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

Combining the Identity Model, Relationship Graph, and Content Analysis to drive accurate detection of email attacks, Abnormal Behavior Technology looks beyond email data to protect your organization from the most dangerous threats.

Abnormal

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@abnormalsec