Enterprise Strategy Group by TechTarget

Technical Validation

Abnormal Cloud Email Security

Behavioral AI to Protect Business Email

By Justin Boyer, Validation Analyst;
and Tony Palmer, Principal Validation Analyst

January 2023

Introduction

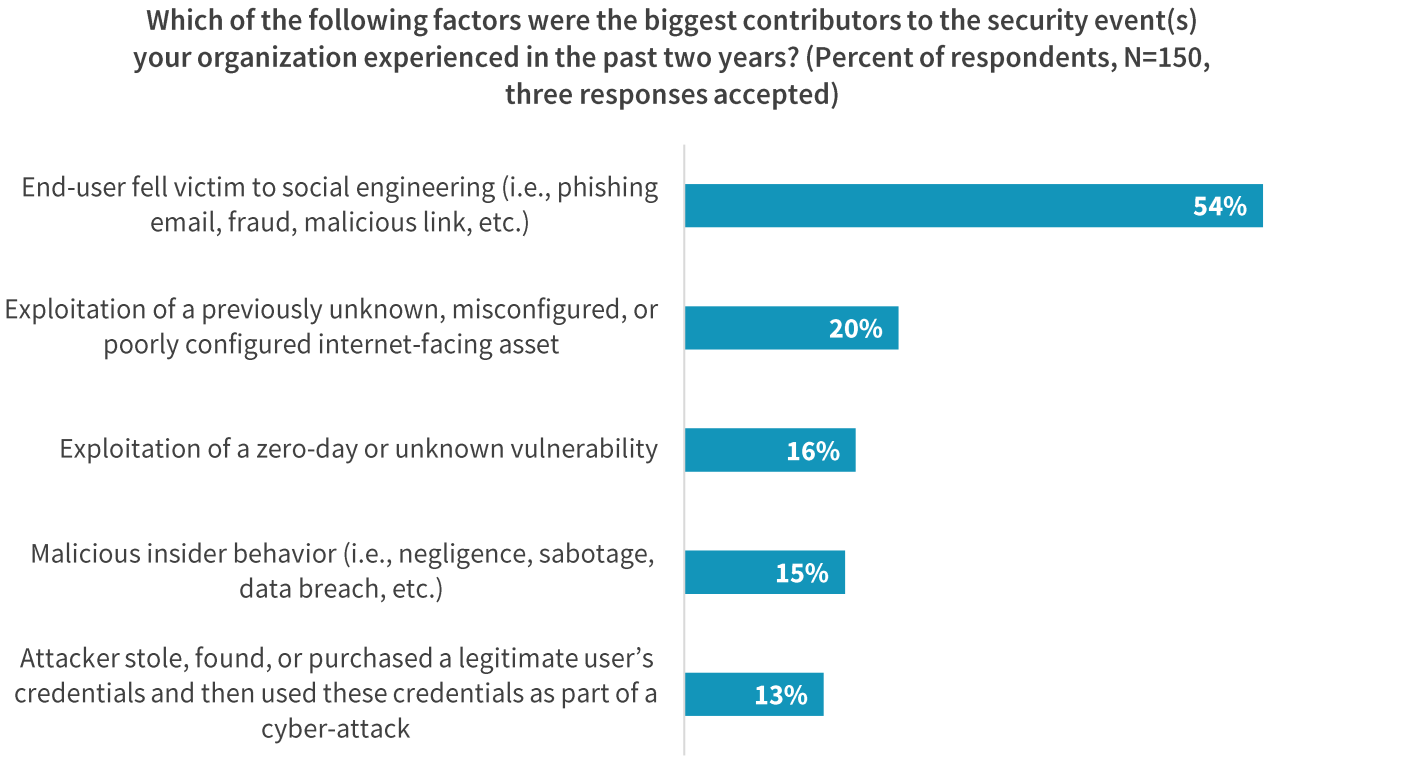
This technical validation report details TechTarget's Enterprise Strategy Group (ESG) analysis of the Abnormal Cloud Email Security platform. ESG validated Abnormal's API integration, behavioral AI capabilities, and VendorBase database.

Background

Security incidents cause lost productivity and can be expensive to recover from. According to Enterprise Strategy Group (ESG) research, loss of productivity and the high resource cost of remediation were the most common impacts of security incidents cited by organizations.[1] These incidents can be especially detrimental when they occur via email.

In particular, business email compromise (BEC) is a dangerous form of email attack that is missed by many email security tools. The goal of BEC attacks is to steal money or information, typically by impersonating company executives or legitimate vendors. These attacks often employ social engineering tactics to deceive or manipulate recipients into providing sensitive data or sending the attacker money via invoice fraud or payroll diversion. ESG recently asked companies what the biggest contributing factors were to security events they've experienced in the past two years. Most respondents (54%) indicated that social engineering attacks against end users were one of the biggest contributors, showing how prevalent this problem continues to be.

Figure 1. Top Five Biggest Contributing Factors to Security Events



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Attackers know that BEC works and will continue to use it to take advantage of employees. Therefore, organizations need to protect against these difficult-to-detect attacks without compromising existing workflows.

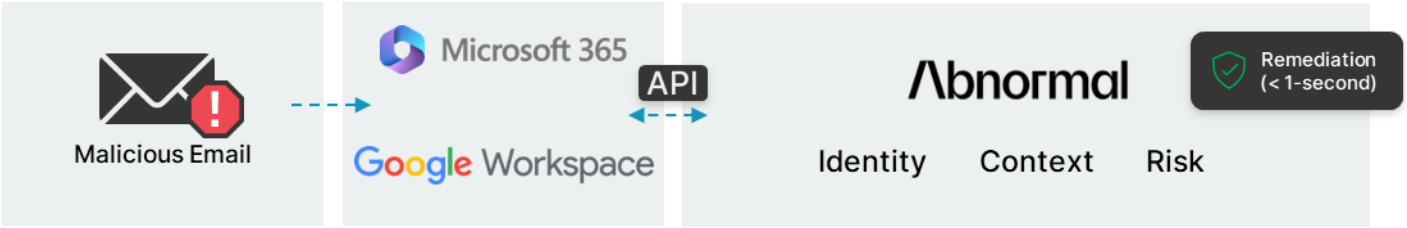
[1] Source: Enterprise Strategy Group Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022. All Enterprise Strategy Group research references and charts in this technical validation are from this survey results set.

Abnormal Cloud Email Security

Abnormal Cloud Email Security provides a cloud-native email security platform that prevents BEC and the full spectrum of email attacks through a behavioral AI approach. Abnormal integrates with existing email providers like Microsoft 365 and Google Workspace via an API connection. Getting started is quick and easy.

Figure 2 outlines the process Abnormal uses to protect business email. Abnormal learns the behavior of every identity within the cloud email environment (i.e., employees, vendors, and applications). When a user receives a malicious email, Abnormal will process and analyze that email without affecting message delivery. According to Abnormal, it typically takes between 25 and 50 milliseconds to process messages. After remediation, Abnormal provides a clear description of why a particular email was remediated, listing all relevant factors.

Figure 2. Abnormal Cloud Email Security



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Abnormal maintains a database of vendors used by all customers called VendorBase. This database rates each vendor based on risk factors seen throughout the Abnormal community of customers. For example, if Abnormal sees emails that indicate account compromise coming from a particular vendor, the vendor's risk rating will increase. Other Abnormal customers can see that federated risk signal, and Abnormal will factor it into analysis of inbound emails from that vendor, across all customers.

The platform consists of three additional Knowledge Bases that surface information to administrators.

- PeopleBase: Provides a directory of each of the active users in the environment. It uses contextual, behavioral data to build a dynamic user genome. PeopleBase also provides an activity timeline of recent events, including sign-on patterns, suspicious email activity, and more.
- TenantBase: Provides a catalog of each of the email tenants Abnormal Security protects and the relevant permissions governing access to them.
- AppBase: Provides a running inventory of all of the third-party applications that have access to data within Microsoft 365, both add-in and enterprise. It offers a summary of important information about application permissions and data access, as well as an activity timeline of recent events to highlight configuration changes.

Enterprise Strategy Group (ESG) Technical Validation

ESG evaluated the Abnormal Cloud Email Security platform to examine how Abnormal Behavior Technology (ABX) can protect organizations from socially engineered attacks that bypass traditional email security solutions. We focused specifically on Abnormal's behavioral AI capabilities and VendorBase to determine efficacy.

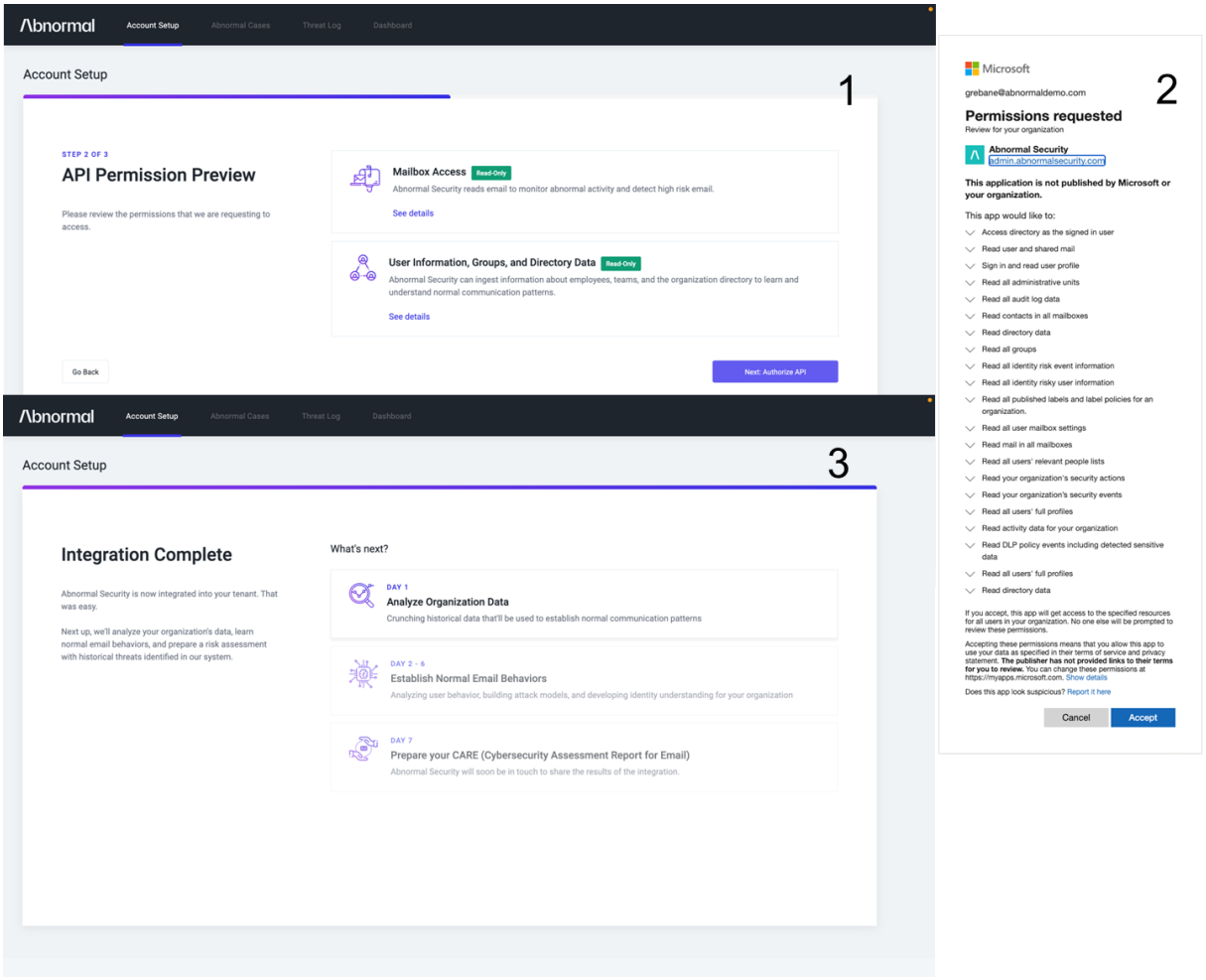
API Integration

First, we walked through the API integration setup process with Microsoft 365.

Enterprise Strategy Group (ESG) Testing

Figure 3 steps through the process. To integrate, Abnormal creates a tenant for the customer and sends a link that company administrators then use to start the integration process with Abnormal. After accepting the terms of service, admins are presented with the API Permission Preview page (step 1). Clicking Next will redirect administrators to their cloud email provider login flow. After logging into the cloud email, they need to accept the consent form listing the permissions required by Abnormal (step 2).

Figure 3. API Integration Setup



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

When the integration is complete, the Abnormal platform shows an overview of the next steps to be performed by Abnormal's AI engine (step 3).

Why This Matters

Security teams are already taxed beyond capacity. Enterprise Strategy Group (ESG) research has found that the high resource cost of remediation is one of the most common impacts of security incidents cited by organizations. Adding to the burden of an already overworked security team will not lead to optimal results.

ESG validated that Abnormal's API integration is fast and easy to set up. A couple of clicks and an OAuth authorization is all that is needed to get started.

While this saves time and effort, since administrators don't need to configure complicated rules or tune Abnormal's engine, this isn't the whole story. Once Abnormal is connected to the cloud email service, it has visibility to correlate user identity and behavior indicators with signals in email content and east-west traffic communication, assessing your employees and vendors, continuously establishing baselines of known behavior on a per-user basis. In practice, Abnormal is detecting missed attacks within hours of deployment—without requiring security professionals to manage the platform after integration.

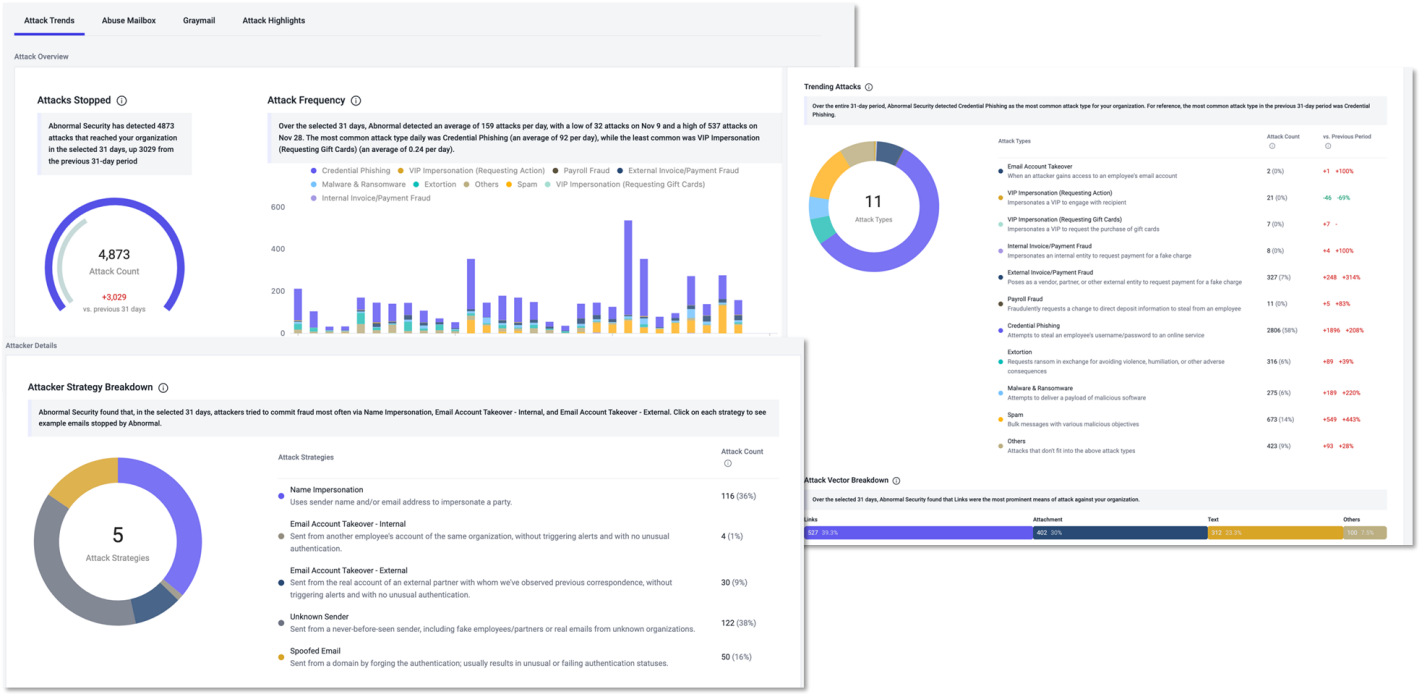
Behavioral AI

We validated Abnormal's behavioral AI, which is used to analyze emails to detect and prevent email-based attacks.

Enterprise Strategy Group (ESG) Testing

Abnormal's dashboards provide a breakdown of recent detections occurring within the email environment. Figure 4 shows the dashboards that display attack frequency, trending attacks, and the most common attacker strategies. Other dashboards show attacker locations, the most frequently impersonated entities, and which employees are receiving the most malicious emails.

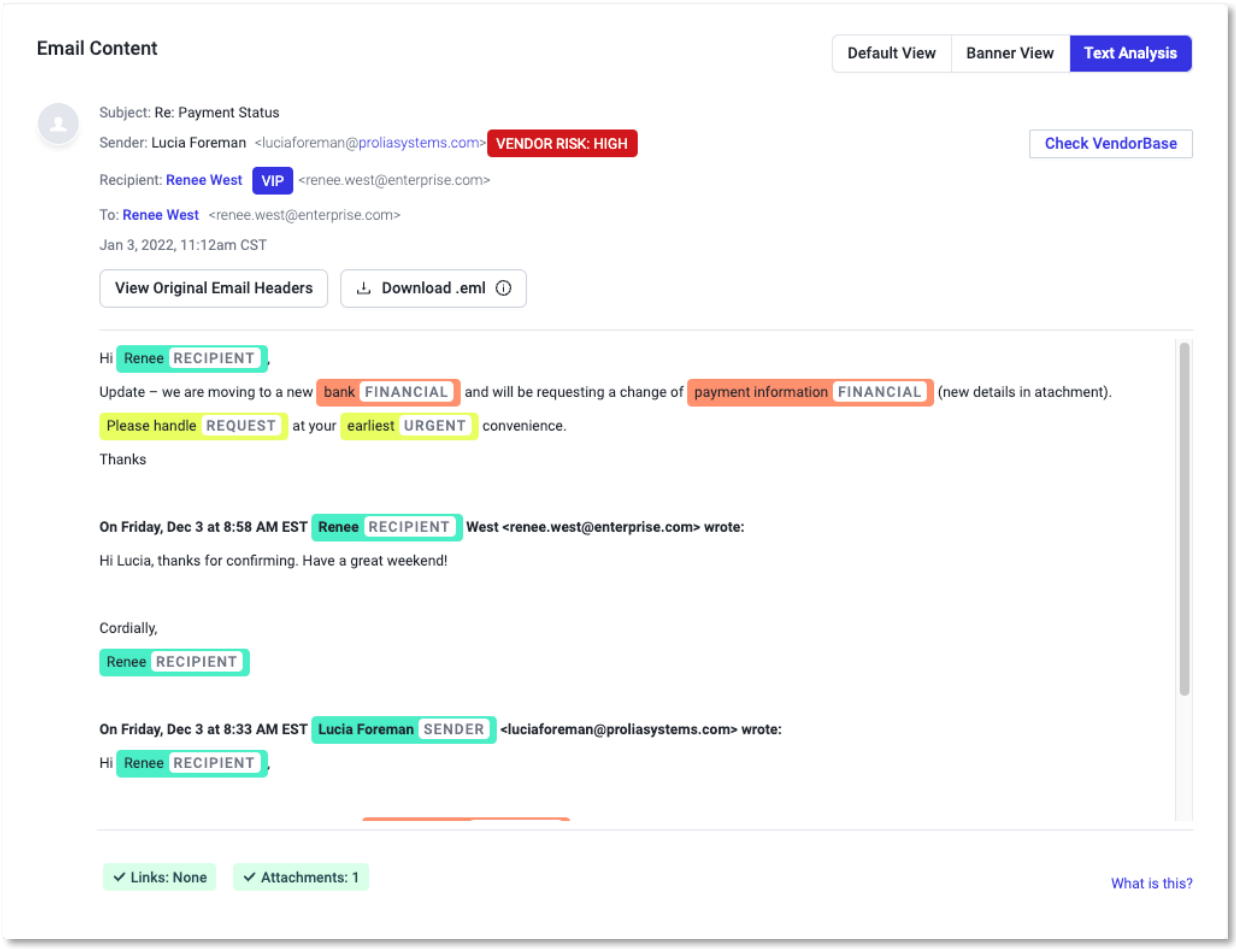
Figure 4. Abnormal Dashboards



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Abnormal's behavioral AI uses a combination of identity, behavior, and context signals to learn, understand, classify, and remediate email-based attacks. The solution uses its cloud-native API-based approach to ingest thousands of diverse signals from Microsoft 365 or Google Workspace and apply NLP/NLU to every email to create a baseline of communication patterns, relationships, and more across every identity in an organization and across the supply chain (see Figure 5).

Figure 5. Analysis of Email Content



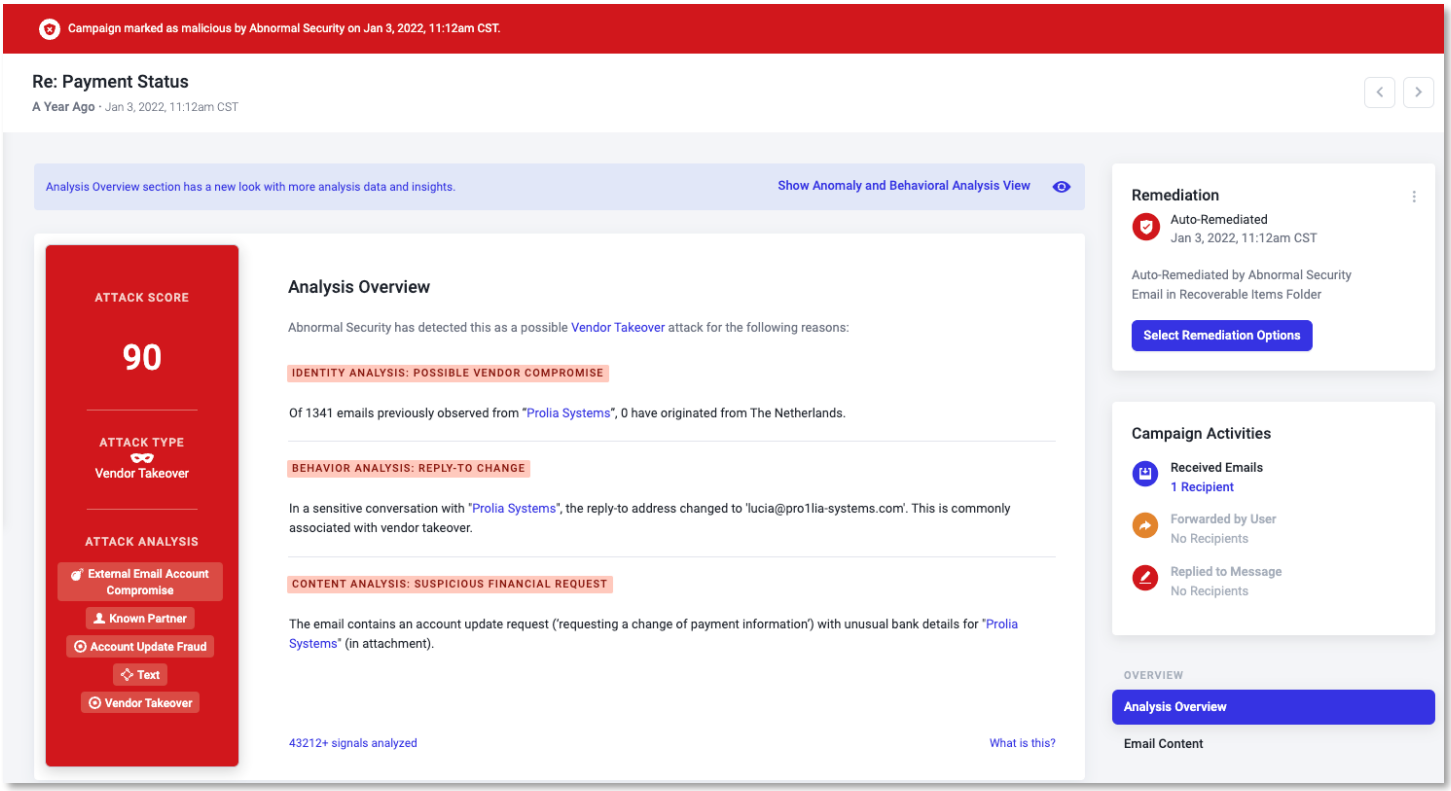
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Abnormal detection engine uses multiple ML models, such as the BERT Large Language Model (LLM), to enhance the efficacy with which Abnormal interprets and evaluates text-based attacks, using context and word associations to understand the correct meaning of email conversations and stop new classes of attacks.

ESG validated Abnormal's behavioral AI and how it analyzes several factors such as geolocation, mail rule changes, sender/recipient relationships, message tone/vocabulary, attachment content, and more. By understanding the known baseline for each of these elements, Abnormal can detect unusual signals that deviate from previously observed patterns—relying on known good rather than known bad to remediate difficult-to-detect and never-before-seen threats.

Further, Abnormal's detailed analysis allows administrators to clearly see why emails were deemed malicious. The factors considered are clearly laid out so anyone can understand the reasoning and use this information to better educate users (see Figure 6).

Figure 6. Analysis Overview for Potential Attack



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

In the scenario observed by ESG, an email was sent by a compromised vendor asking to change financial details to accounts never before seen by Abnormal for this vendor.

Why This Matters

Enterprise Strategy Group (ESG) research found that over half of organizations surveyed (54%) listed social engineering attacks as one of the most common sources of security incidents. Social engineering over email is prevalent and it works. But not every attack is obvious. Eloquent emails sent from a trusted email address can be malicious and incredibly difficult to detect by both tools and end users.

ESG observed how Abnormal's advanced machine learning algorithms analyzed several factors that may be overlooked and used them to determine abnormal email activity. Factors including how quickly someone changes locations, what banking details vendors have used in the past, or subtle language indicating urgency are identified and used to prevent attacks from reaching users.

Abnormal can find and remediate difficult-to-detect email attacks that may otherwise look legitimate and evade traditional detection methods. These emails are less frequent but can be the costliest for organizations. Detecting these gives companies incredible value and ensures that their users do not have to make decisions on the legitimacy of each email.

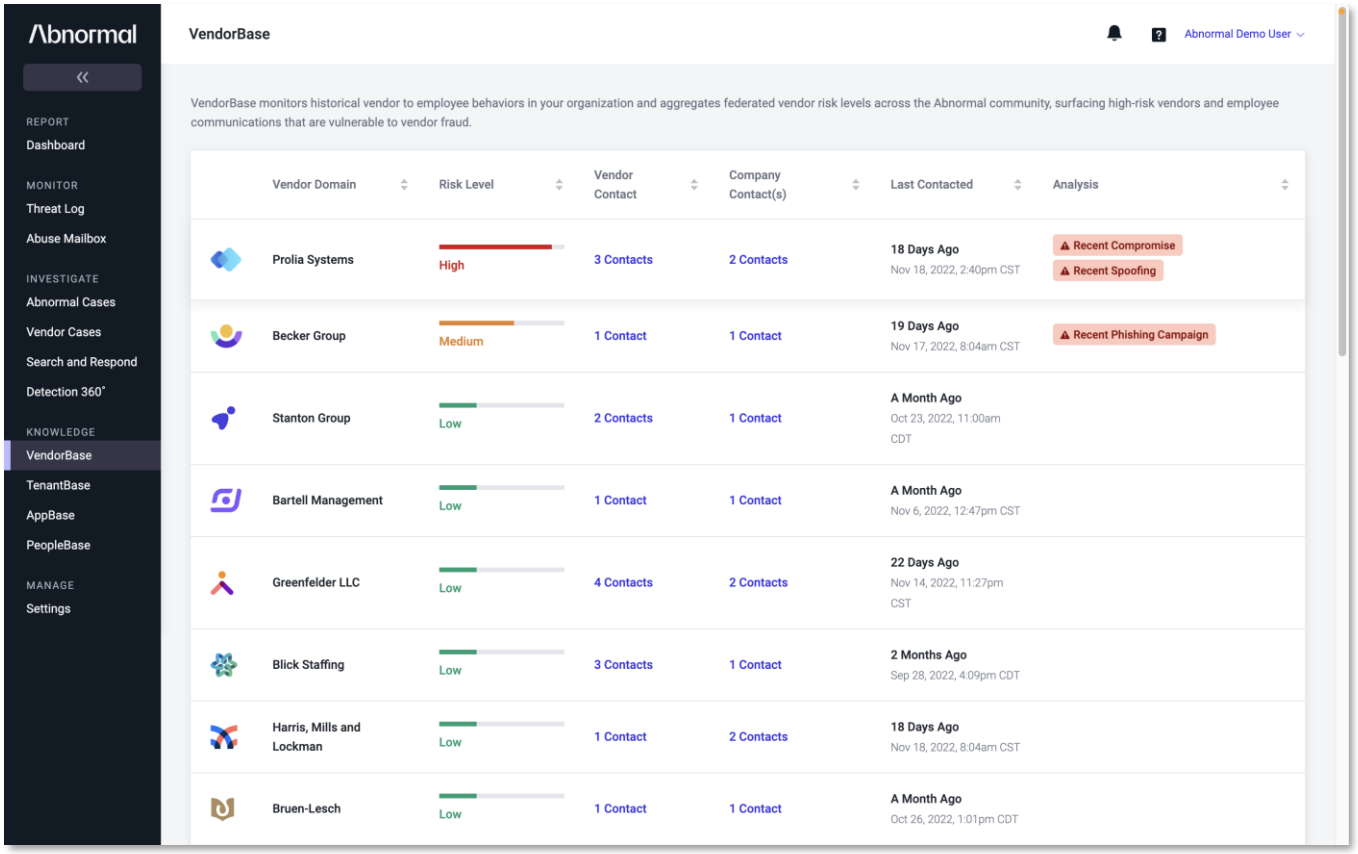
VendorBase – A Federated Database of Vendor Risk

Abnormal VendorBase is a federated database built by Abnormal to track the risk of vendors across all customers. There is no need for administrators to add vendors. Instead, Abnormal builds the database while indexing user inboxes, keeping track of key information such as where emails from the vendor originate, the names of vendor contacts, which employees regularly receive emails from the vendor, and sensitive information included in each email.

Enterprise Strategy Group (ESG) Testing

VendorBase automatically identifies the vendors from company email communications, building a list of the vendors in the supply chain without any manual input (see Figure 7).

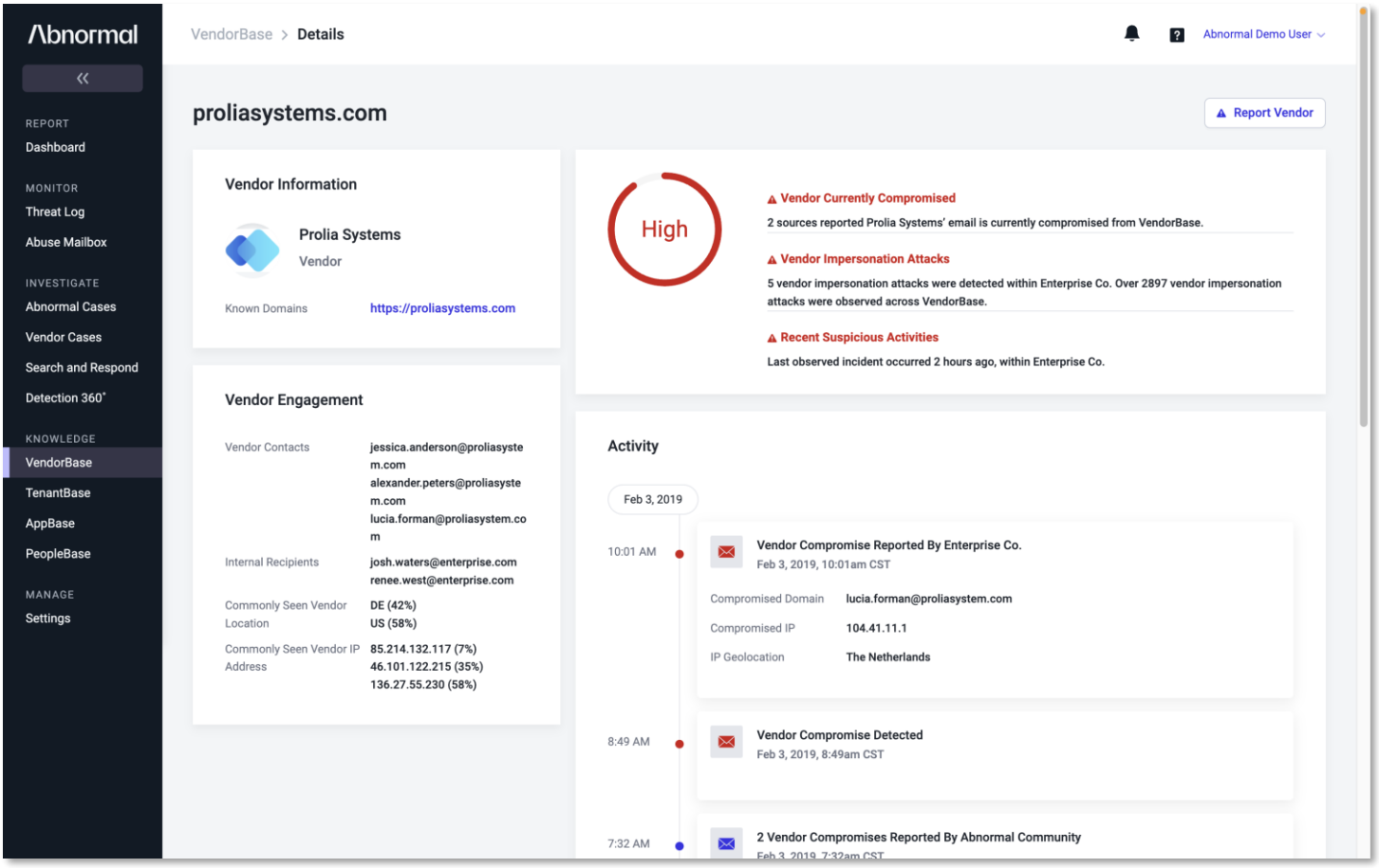
Figure 7. List of Vendors in VendorBase



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As shown in Figure 8, clicking a record in VendorBase allows users to see detailed information about the vendor's risk. Recent compromises and suspicious activity showcase why Abnormal is more likely to scrutinize incoming emails from those vendors to keep the organization safe.

Figure 8. Vendor Profiles



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The risk assessment of each vendor is computed using signals related to the vendor's identity, behavior, content, and email activity reported from all Abnormal customers.

Why This Matters

The danger of email attacks comes from their unpredictability. With early threat detection, companies can anticipate and prepare for future attacks to avoid devastating losses.

Enterprise Strategy Group (ESG) reviewed the VendorBase maintained by Abnormal. This database contains data collected from all Abnormal customers and helps to determine the relative risk of each vendor—especially useful as threat actors are increasingly using vendor relationships to initiate attacks.

Armed with advanced risk data, companies can be on alert for compromised vendor emails and inform their vendors of potential risks within their systems. In turn, when suspicious emails are detected by Abnormal for one customer, that vendor risk score is updated across all customers to help others within the Abnormal community. A strong community leads to all users being better prepared to defend themselves.

The Bigger Truth

Social engineering through email has become a dangerous attack vector. Socially engineered emails seek to steal credentials, data, or money by impersonating legitimate vendors or members of the executive team. And because they rarely contain traditional indicators of compromise, they can be incredibly difficult to detect.

Enterprise Strategy Group (ESG) validated that the Abnormal API integration allows organizations to get started quickly, without setting up complicated rules or spending time tuning the platform. Abnormal immediately begins the process of creating a baseline and profiling inboxes so that it is detecting missed attacks within hours of deployment.

Once integrated, Abnormal learns the behavior of every identity within an email system. It analyzes the risk of every event and blocks suspicious emails while providing a clear description of why a particular email was blocked, listing all relevant factors.

For example, ESG observed Abnormal reporting a potential account compromise due to a user logging in from Hong Kong only 90 minutes after the same user logged in from San Francisco, which is physically impossible. Soon after logging in, the user then changed mail rules to hide certain emails, making it a high probability that the account was compromised. This behavioral intelligence allows organizations to prevent some of the most expensive breaches that other tools may miss.

Further, VendorBase allows organizations to prepare for possible attacks by alerting them to potentially compromised vendors. Abnormal automatically tracks vendors used by the organization and adds them to VendorBase. Potentially malicious activity raises a vendor's risk rating, alerting an organization to danger before any emails are sent to its employees.

Abnormal Cloud Email Security protects organizations from targeted and sophisticated email attacks. The API integration and behavioral AI detect and remediate malicious emails before end users see them. If your organization is looking to protect its end users from BEC and other advanced email attacks, then ESG believes that you should consider the risk reduction capabilities of Abnormal Cloud Email Security.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188