Abnormal Security

Industry Solution Brief

# Abnormal Security: Cloud Email Security Platform Healthcare

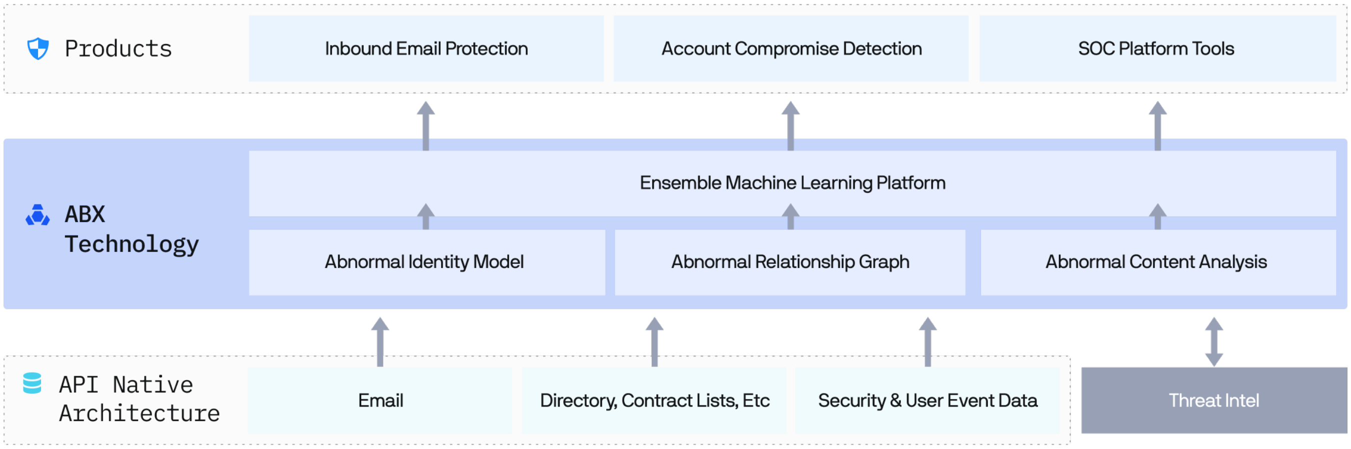
Healthcare organizations face a complex operation balancing the critical mission of enabling patient care while handling sensitive data that is highly sought after by malicious for-profit and nation-state actors alike. The risks go beyond the external threat actors -- healthcare providers, health insurers, pharmaceutical, biotechnology and medical device companies have faced lawsuits for inadequate safety measures in the wake of phishing attacks that have led to data breaches. Furthermore, the impact of cybersecurity is no longer just about HIPAA/HITECH compliance - cyberattacks represent a core threat to the healthcare industry's mission to provide patient care.

## Key Industry Challenges

- *Address a wide scope of attacks, from persistent for-profit criminals after valuable healthcare records to well-funded nation-state actors seeking proprietary research and data*
- *Threat actors leveraging compromises of vendors / business associates to launch attacks from. 59% of of data breaches have been attributed to 3rd parties*
- *Lack of visibility into attack propagation, such as internal phishing*

## Abnormal Security Cloud Email Security Platform

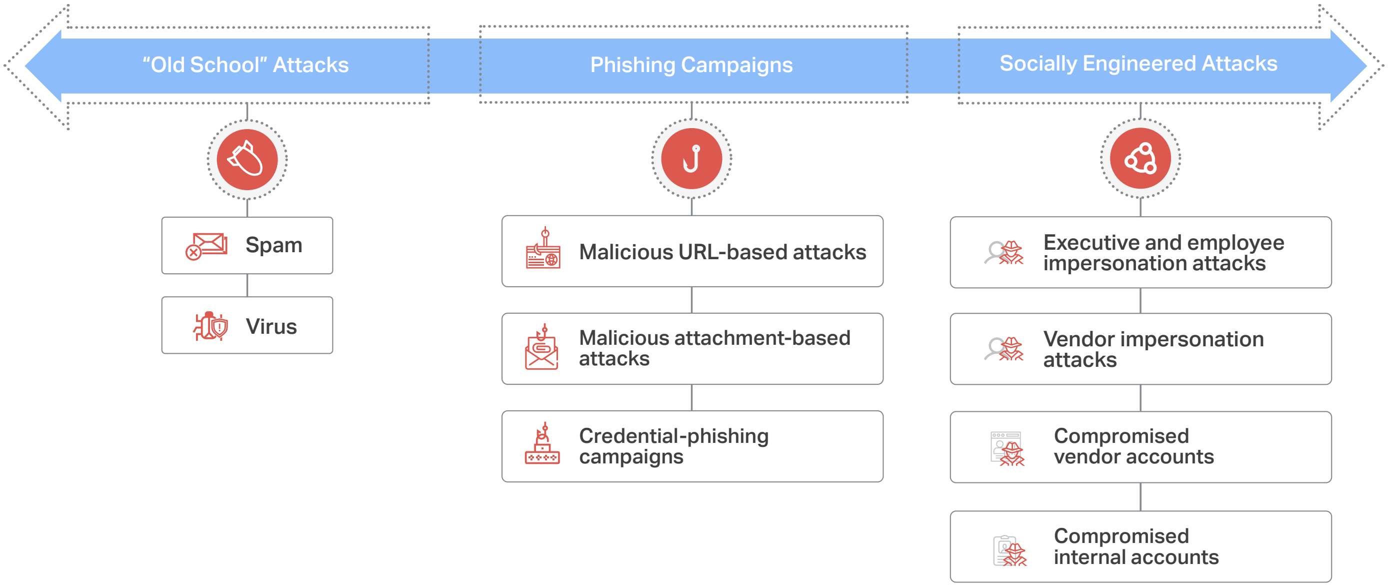
Through a simple API-integration to Office 365, Abnormal Security maximizes your investment in Microsoft's security capabilities in EOP while addressing the email attacks that continue to evade all forms of traditional email security. The Abnormal Security platform analyzes data beyond email, enabling Abnormal Behavior Technology (ABX) to use this rich set of organization-specific data to uniquely drive the Abnormal Identity Model, the Abnormal Relationship Graph, and Abnormal Content Analysis.



Products
Inbound Email Protection
Account Compromise Detection
SOC Platform Tools
ABX Technology
Ensemble Machine Learning Platform
Abnormal Identity Model
Abnormal Relationship Graph
Abnormal Content Analysis
API Native Architecture
Email
Directory, Contract Lists, Etc
Security & User Event Data
Threat Intel

## Stop Advanced Email Attacks

Healthcare organizations need an uncompromising security solution capable of stopping the entire spectrum of email attacks. Abnormal Security stops the most advanced email attacks that no one else is stopping, with a particular focus on the most dangerous: sophisticated, highly-targeted attacks. Block attacks from for-profit criminals targeting the most valuable asset on the black market: healthcare records. Stop sophisticated, motivated nation-state actors focused on stealing the R&D efforts for vaccines and treatments.



"Old School" Attacks
- Spam
- Virus

Phishing Campaigns
- Malicious URL-based attacks
- Malicious attachment-based attacks
- Credential-phishing campaigns

Socially Engineered Attacks
- Executive and employee impersonation attacks
- Vendor impersonation attacks
- Compromised vendor accounts
- Compromised internal accounts

### KEY BENEFITS

**01 Stop Advanced Email Attacks**

Stop the full range of attacks, from for-profit criminals to nation-state actors, with a unique focus on targeted, social engineering attacks.

**02 Increase Visibility & Control**

Monitor internal email traffic, detect and remediate compromised accounts while preventing internal phishing attacks.

**03 Improve Efficiency**

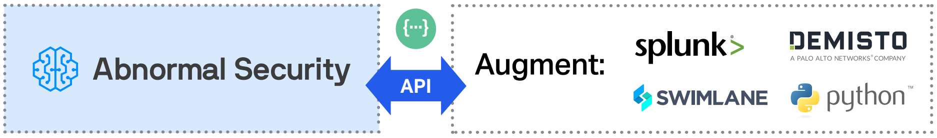
Automate the triage of end-user reported email attacks, auto-remediate compromised accounts and enable your security team to focus on more critical tasks.

## Dynamic Analysis of Supply Chain Risk

59% of data breaches have been attributed to 3rd party vendors. Regardless of your organization's security maturity, it is critical to continually assess the risks of your 3rd parties and business associates. Abnormal Security can dynamically assess your supply chain risk with Vendorbase – a global, federated database of vendor behaviors to stop supply chain compromise, cyber attacks, and fraud.

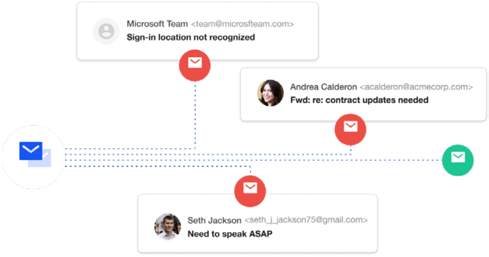
## Automation with M-SOAR (Email Security Orchestration Automation and Response)

Healthcare security teams are constantly juggling the enablement of high quality patient care while providing security and compliance against highly persistent and motivated attackers. These teams need tools that allow them to focus on the most critical tasks. Abnormal Security provides the automation required to enable the security team to work more efficiently.



## Email Protection

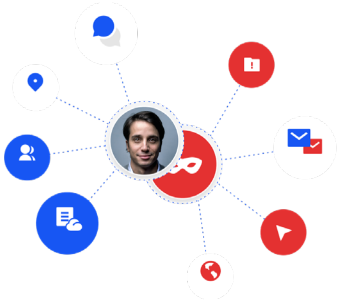
Using data science technologies in conjunction with the organization-specific data provided by the API architecture, Abnormal Security blocks the full range of email attacks, including the highly targeted attacks that the healthcare sector faces. Vendorbase provides targeted protection against attacks leveraging 3rd parties and business associates.



Microsoft Team <team@microsfteam.com>
Sign-in location not recognized

Andrea Calderon <acalderon@acmecorp.com>
Fwd: re: contract updates needed

Seth Jackson <seth_j_jackson75@gmail.com>
Need to speak ASAP



## Account Takeover Detection

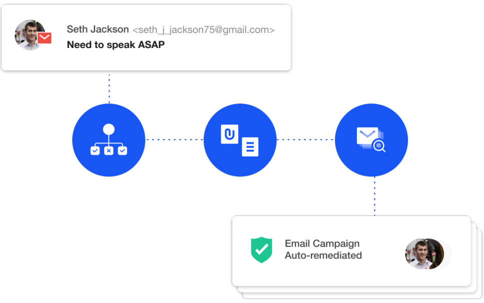
Mitigate the risks of lateral movement and attacks from internally compromised email accounts. Abnormal Security analyzes hundreds of signals to accurately detect and remediate compromised email accounts.

## SOC Platform Tools

Automate security processes to enable your team to focus on truly critical actions.

- *Abuse Mailbox integration*: automatically triage end-user reported email attacks
- *Unsafe engagement notification*: alert security teams on end-user engagement with malicious actors
- *Auto-remediation of ATO*: automate the remediation of compromised accounts

Seamlessly integrate into your security environment (SIEM, SOAR and more) with APIs.



Seth Jackson <seth_j_jackson75@gmail.com>
Need to speak ASAP

Email Campaign
Auto-remediated

### About Abnormal Security

The Abnormal Security cloud email security platform protects enterprises from targeted email attacks. Powered by Abnormal Behavior Technology (ABX), the platform combines the Abnormal Identity Model, the Abnormal Relationship Graph and Abnormal Content Analysis to stop attacks that lead to account takeover, financial damage and organizational mistrust. Through one-click, API-based Office 365 and G Suite integration, Abnormal Security sets up in minutes, requires no configuration and does not impact email flow. Backed by Greylock Partners, Abnormal Security is based in San Francisco, CA. Please visit www.abnormalsecurity.com and follow the company at @AbnormalSec.

> *"We had given up on being able to stop these modern payload-less attacks, relying instead on training our end-users to identify and ignore these emails. Abnormal Security is stopping attacks in ways that we didn't believe were possible."*

**Healthcare**
Director of Information Security

### Contact Us

www.abnormalsecurity.com

@AbnormalSec

185 Clara Street, Suite 100
San Francisco, California 94107