

Abnormal Security: Cloud Email Security Platform for Oil, Gas & Utilities

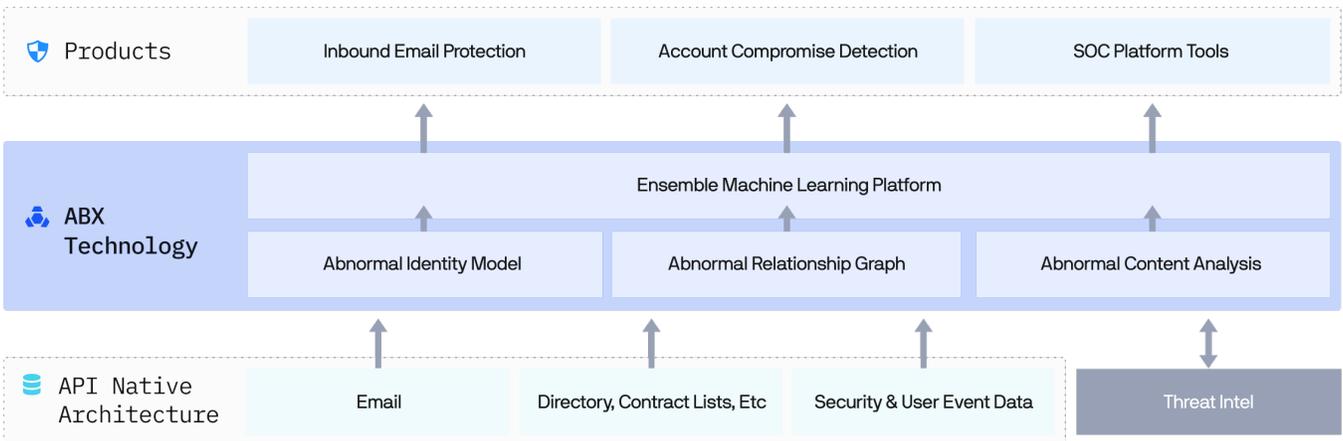
Oil, Gas and Utility organizations are some of the most targeted environments for attackers. As one of the critical infrastructure sectors, the energy sector uniquely faces the widest spectrum of attacks from attackers ranging from for-profit criminals all the way to well-funded nation-state actors. The cybersecurity risks are exacerbated with the increasing interconnected-ness between IT and OT as companies undergo rapid modernization driven by massive cost savings and benefits from the use of connected meters, pumps, valves and other devices.

Key Industry Challenges

- Email is the initial attack vector of nearly all attempts to compromise
- Digital Supply Chain Attacks / 3rd parties represent the one of the greatest risks to the sector
- The cybersecurity skills shortage is even amplified within the energy sector

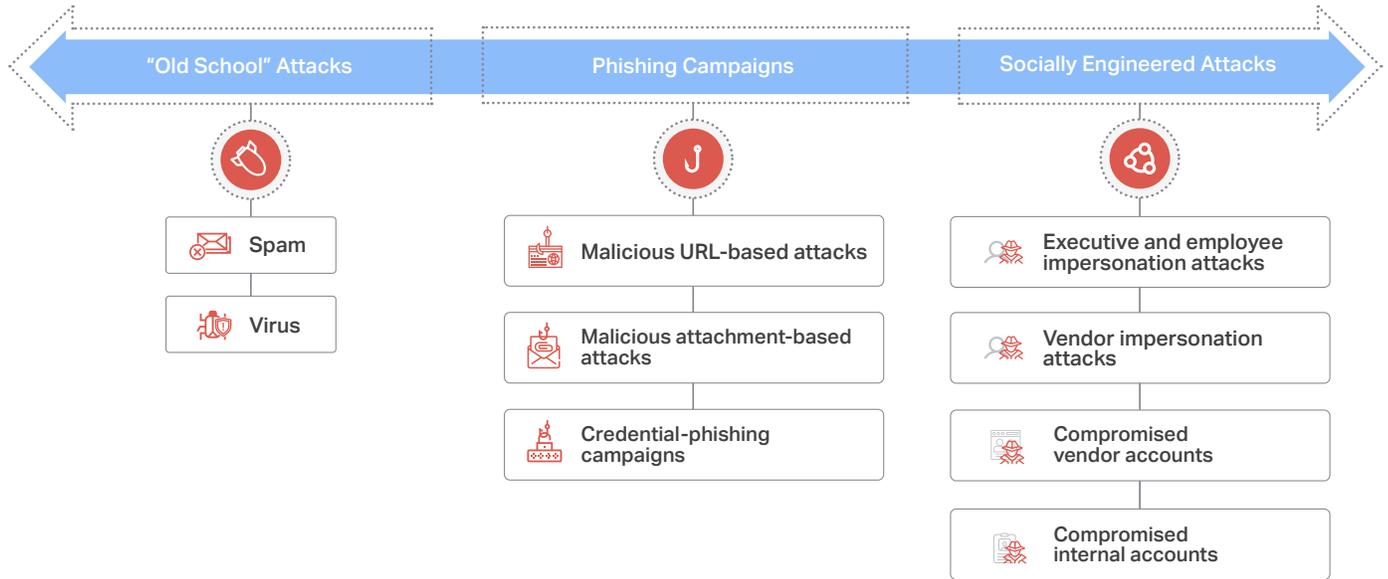
Abnormal Security Cloud Email Security Platform

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 traditional secure email gateways. 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.



Stop Advanced Email Attacks

Organizations in the energy sector need an uncompromising security solution capable of solving 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.



KEY BENEFITS

01 Stop Advanced Email Attacks

Stop the full range of email 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 to prevent internal 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

The need to assess the risks within the supply chain are undeniably critical within the sector. Energy regulators have come to terms with the realities of this risk with the introduction of CIP-013-1. Abnormal Security can dynamically assess the supply chain risk with **Vendorbase** – a global, federated database of vendor risk to mitigate attacks from compromised suppliers.



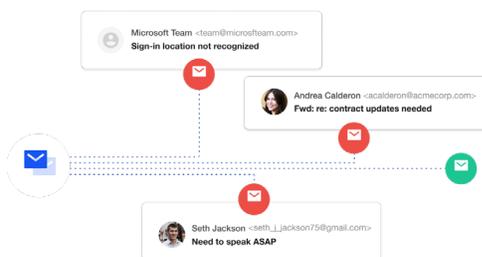
Automation with M-SOAR (Email Security Orchestration Automation and Response)

Security teams within the energy sector are stretched thin and need tools that allow them to focus on the most critical tasks. Abnormal Security provides the automation required to enable security teams to work more efficiently and focus on critical tasks only addressable by humans.



Email Protection

Using data science technologies in conjunction with organization-specific data provided by the API architecture, Abnormal Security blocks the full range of email attacks, including the low volume, highly targeted attacks that the energy sector faces. Vendorbase provides targeted protection against supply chain attacks in support of NERC CIP-013-1.



“Abnormal Security’s ability to turn around and modify the service to end user needs is by far better than any other vendor I have.”

Large Oil & Gas Company
CISO



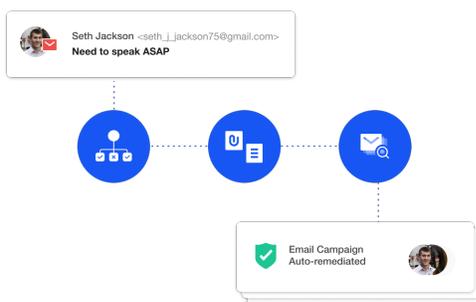
Account Takeover Detection

Mitigate the risks of lateral movement and attacks from internally compromised 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 when end-users engage with malicious actors
- Auto-remediation of ATO: automate the remediation of compromised accounts



Abnormal Security seamlessly integrates into your security environment (SIEM, SOAR and more) with APIs.

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](https://twitter.com/AbnormalSec).

Contact Us

 www.abnormalsecurity.com
 [@AbnormalSec](https://twitter.com/AbnormalSec)

797 Bryant Street
San Francisco, California 94107