CrowdStrike Technology Partner

Abnormal

CROWDSTRIKE

Solution Brief

ABNORMAL SECURITY AND CROWDSTRIKE INTEGRATION: BIDIRECTIONAL BEHAVIORAL ATTACK DETECTION AND RESPONSE

Discover and remediate compromised email accounts and endpoints

CHALLENGES

Today's email attack campaigns do not look like they did a decade ago. Now, they may not leave behind clear evidence, and they often spread laterally very quickly across endpoints, cloud and network assets. Socially engineered business email compromise attacks have accounted for **over $43 billion USD in losses since 2016** and continue to grow. Rapid detection and response are key, but security analysts are slowed down by the manual effort needed to integrate siloed data from various solutions. Without native connections between email and endpoint security tools, security teams bear the burden of manually correlating signals from multiple security domains.

SOLUTION

Abnormal Security's artificial intelligence (AI)-based attack detection and CrowdStrike Falcon® Identity Threat Protection capabilities complement one another, offering analysts higher-fidelity detection of sophisticated threats and faster, more effective response playbooks. This bidirectional technology integration combines the power of two best-in-class security platforms to enable analysts to discover and remediate compromised email accounts and endpoints swiftly. Best of all, it can be enabled in just a few clicks, providing better protection with no additional work.

KEY BENEFITS

Uncovers compromised endpoints and email account takeover attacks that traditional security solutions often fail to detect

Increases operational productivity by breaking down data silos and correlating endpoint, identity and email events into consolidated views

Accelerates incident response with automated response workflows that stop lateral movement and downstream risks

CrowdStrike Technology Partner

ABNORMAL SECURITY AND CROWDSTRIKE INTEGRATION: BIDIRECTIONAL BEHAVIORAL ATTACK DETECTION AND RESPONSE

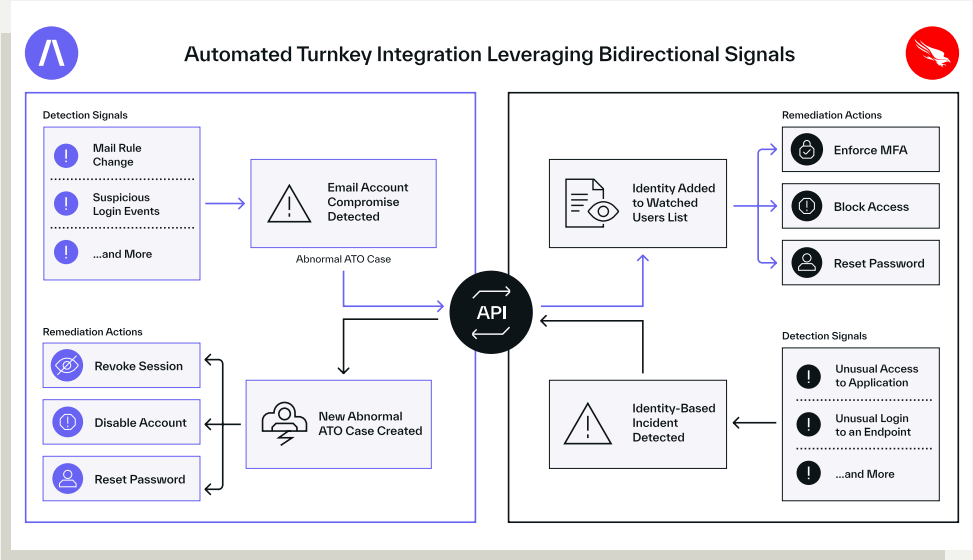
BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
Identification of sophisticated and complex email attacks	Leverage behavioral AI to understand normal behavior of identities and detect anomalous and potentially malicious activity	Help prevent email attacks missed by traditional email security solutions that are reliant on known indicators of compromise
Detection of and response to account takeover	Combine CrowdStrike's identity-based incident detection and Abnormal's behavioral analytics to detect potential account takeovers and initiate remediation actions, such as logging the user out of Microsoft 365, blocking account access, and resetting the user's password	Detect email accounts that have been compromised, and remediate any messages sent by them before attackers can do further damage
Context-rich investigation of identity-based incidents	Send CrowdStrike Falcon identity detections to Abnormal, where email activity can be analyzed and compromised email accounts can be remediated	Connect the dots between users and devices in a consolidated view, and respond quickly to potential compromise

TECHNICAL SOLUTION

The CrowdStrike Falcon® platform enhances Abnormal's email attack detection by sending identity-based incidents (e.g., failed authentication attempts from a new endpoint) to Abnormal for further investigation. Security analysts can then automatically mitigate the risk of lateral phishing by signing the user out of active Microsoft 365 sessions, blocking account access, remediating email messages and resetting their password.

When Abnormal detects a potential active account takeover within Microsoft 365 (e.g., a call center agent sends a voicemail file to many employees), Abnormal automatically adds the user to the Watched Users list within Falcon Identity Threat Protection. Security analysts may configure automatic remediation actions for Watched Users that include enforcing MFA, blocking user access and resetting passwords.



"Comfort Systems USA builds, supports and maintains our customers' most critical building systems. I'm excited to see Abnormal Security and CrowdStrike working together to protect our employees against the types of attacks traditional solutions often fail to detect. With the ability to correlate user behavior events across endpoint, email and authentication sources, our security team can quickly uncover account takeover attacks and take preventative measures."

— Christopher Chambers,
Vice President of Information Security, Comfort Systems USA

"The enhanced, integrated offerings from CrowdStrike and Abnormal further strengthen our security infrastructure and quickly orchestrate responses when needed. These solutions provide enhanced protection for our organization as well as significant time savings and process efficiencies."

— Drew Robertson,
CISO, Finance of America Companies

CrowdStrike Technology Partner

ABNORMAL SECURITY AND CROWDSTRIKE INTEGRATION: BIDIRECTIONAL BEHAVIORAL ATTACK DETECTION AND RESPONSE

KEY CAPABILITIES

- Helps to protect employees from hard-to-detect, sophisticated email attacks
- Consolidates endpoint, identity and email detections into comprehensive views
- Automates response actions that limit lateral movement and downstream risks

Abnormal Security is a trusted **CrowdStrike Technology Alliance Partner,** offering innovative integrated solutions that deliver best-in-class email attack detection and response with account and endpoint automated remediation. Abnormal Security is also a member of the **CrowdXDR Alliance**, a revolutionary security alliance that delivers unified XDR enterprise-wide.

ABOUT ABNORMAL

Abnormal Security provides the leading behavioral AI-based security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails in milliseconds — all while providing visibility into configuration drifts across your environment. You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly.

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**
Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**
Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

Learn More in the CrowdStrike Store