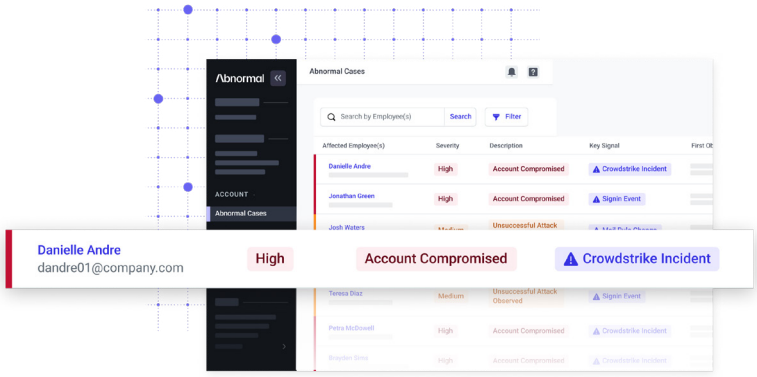
Abnormal

Abnormal Security + CrowdStrike

Abnormal and CrowdStrike complement one another with high-fidelity detection of sophisticated threats and faster, more effective response playbooks.

Socially-engineered business email compromise attacks have accounted for over $43B in losses since 2016 and continue to grow. With a 15% increase in financial losses over the past year alone, it's clear that organizations need a new, integrated solution to combat this problem.*

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.



The bidirectional integrations between Abnormal Security + CrowdStrike provide the solution.

- Protect employees against hard-to-detect, sophisticated email account takeover attacks.
- Consolidate email attacks, account takeovers and identity based incidents into comprehensive views for faster, more effective investigations.
- Automate response actions that limit lateral movement and downstream risks by requiring multifactor authentication, signing users out of sessions, and more.
- Deploy in seconds via API integration with a few clicks.

The Abnormal + CrowdStrike Advantage

Protect your largest attack surface areas. Uncovers socially engineered email attacks, compromised endpoints and account takeovers that traditional security solutions often fail to detect.

Enrich security context. Breaks down data silos by correlating endpoint, identity and email events into cross-domain detections alongside other third-party tools.

Respond faster. Accelerates incident response with automated workflows to contain risks.

*2022 FBI IC3 Report.

Learn more. abnormalsecurity.com →