Abnormal

Legacy SEGs Can't Stop Vendor Email Compromise

Organizations are paying the price.

THE PROBLEM

SEG Blind Spots

Text-based vendor email compromise (VEC) attacks use no links, no attachments, and no malware. They slip past legacy filters undetected, landing in employee inboxes and presenting as legitimate messages.

44%
of read VEC messages are replied to, forwarded, or both

98.5%
of advanced attacks go unreported

$300M+
in attempted fraud across 1,400 organizations in 12 months

THE EXPOSURE

Why SEGs Fail

Reliance on static signals

Can't detect payload-less attacks with no traditional indicators of compromise

Lack of behavioral context

Unable to determine if sender is trusted or if activity is unusual

No understanding of intent

Treat malicious requests as benign because intent isn't analyzed

Dependence on employees for detection

Shift security burden to humans, who regularly miss sophisticated attacks

VEC attacks masquerade as routine business communications—and SEGs treat them that way.

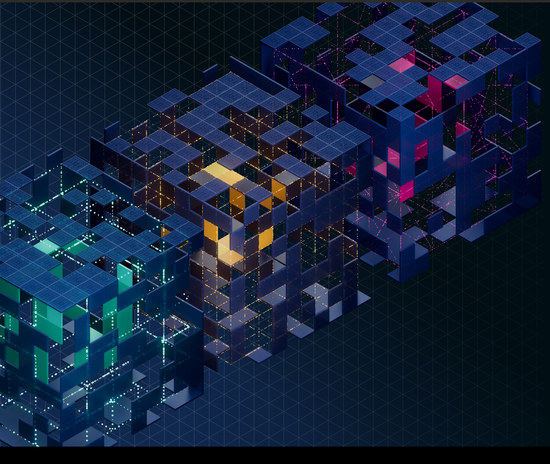
THE IMPACT

High VEC Engagement Rates

72%
post-read interaction rate in large enterprises *(Bigger orgs, bigger attack surface)*

86%
post-read interaction rate by entry-level sales staff *(Fast-moving, inbox-driven roles)*

7%
of VEC engagements came from previously targeted users *(Employees fall for attacks more than once)*



The Only Real Defense? Behavioral AI

- Builds baselines for normal communication
- Flags behavioral anomalies invisible to SEGs
- Detects intent—not just signatures
- Intercepts malicious emails before employees can engage

Precision matters. Stop relying on tools built for a different era of email.

Source: Read, Replied, Compromised: Data Reveals 44% Engagement Rate with VEC Attacks