Abnormal

The Essential Guide to Cloud Email Security

Why yesterday's defenses can't stop today's AI-driven attacks.

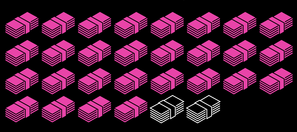
THE PROBLEM

SEG Blind Spots

Email remains the #1 entry point for attacks.
But today's campaigns don't need malware or links to succeed.

$2.77B

lost to business email compromise in 2024



= 100 million

261 days

to identify and contain a phishing-related breach

84%

of employees fall for phishing emails within 10 minutes

Attackers exploit:

Trust

hijacking vendor accounts and impersonating executives

Identity

stealing credentials, bypassing MFA, and deploying malicious apps

AI

mirroring tone and exploiting relationships in real conversations, at scale

Built for yesterday's indicators, SEGs can't defend against attacks that exploit human behavior and workplace expectations.

THE EXPOSURE

Why SEGs Fail

Payload Focus

Leaves employees exposed to convincing text-based attacks

No Vendor Profiling

Compromised suppliers redirect payments undetected

No Internal Visibility

Hijacked accounts spread laterally inside the org

Slow Manual Remediation

Threats sit in inboxes long enough to be acted on

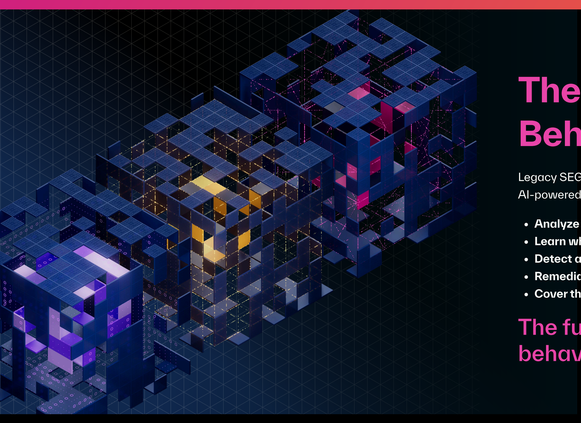
Miss Early Takeover Signs

Unusual logins and malicious apps slip past

Ignore Misconfigurations

Risky cloud settings open hidden backdoors

**Result: SEGs don't just miss advanced threats.
They turn employees into the last line of defense.**



The Only Real Defense? Behavioral AI

Legacy SEGs weren't built to protect cloud email. AI-powered attackers demand AI-powered defense. The solution outfitted for modern threats will:

- **Analyze identity, context, and behavior** across every message
- **Learn what's normal** for each employee, executive, and vendor
- **Detect anomalies invisible to static filters**
- **Remediate instantly, not hours later**
- **Cover the collaborative cloud environment**, beyond email

The future of email security is behavioral, adaptive, and AI-powered.

Source: The Essential Guide to Cloud Email Security