Abnormal | CDW

Can Your SEG Survive 2026?

The 10-Point Stress Test for Modern Email Security

Secure email gateways were built for an era of spam, malware, and known-bad payloads.

Modern threats look different.

The attacks causing the most damage today rarely look malicious. They resemble coworkers, vendors, executives, invoices, and everyday business communication.

If your email security strategy still relies on perimeter inspection and static detection logic, this stress test will help determine whether your architecture can keep up with what's next.

The Stress Test

If these statements describe your architecture, check the box, and tally up your responses at the end.

☐ **1. Your biggest email threats still pass SPF, DKIM, and DMARC**

Modern phishing, vendor compromise, and business email compromise attacks increasingly originate from legitimate infrastructure and trusted accounts, leaving traditional authentication checks with little to flag.

Next Level: If an email passes SPF, DKIM, and DMARC, what detection layers are left to determine whether it's malicious?

☐ **2. Your detection logic still depends on "known bad" indicators**

Legacy email security was built to detect recognizable malware, malicious URLs, and suspicious infrastructure. Modern attacks are specifically designed to avoid those signals.

Next Level: How would your security stack identify an attack with no malicious link, attachment, domain, or payload?

☐ **3. Your platform cannot identify attacks with no payloads or malicious links**

Many of today's most damaging attacks contain nothing overtly malicious at all—just convincing language, urgency, and carefully crafted social engineering.

Next Level: Would your defenses automatically stop a fraudulent wire request sent from a trusted account?

☐ **4. AI-generated impersonation blends into normal communication patterns undetected**

Generative AI has made it dramatically easier for attackers to mimic writing styles, vendor relationships, and everyday business communication at scale.

Next Level: Could your platform distinguish between a trusted vendor and an attacker who sounds exactly like one?

☐ **5. Your SOC spends more time tuning rules than investigating threats**

Static policies, allowlists, and false-positive management create operational drag while delivering diminishing security value against modern attacks.

Next Level: How many hours did your team spend maintaining email security controls last quarter?

☐ **6. Analysts still manually triage quarantined email at scale**

When remediation depends heavily on analyst intervention, threats remain in inboxes longer and security teams spend valuable time processing repetitive investigations.

Next Level: How much analyst time is spent reviewing emails that turn out to be benign?

☐ **7. Employees remain the last line of defense against socially engineered fraud**

When identity-driven attacks bypass detection, organizations are forced to rely on employees to identify subtle deception under pressure—a control that fails with increasing regularity.

Next Level: If your technology misses the attack, who is expected to catch it? Will they?

☐ **8. Your protection ends at the inbox perimeter**

Modern attacks move across email, cloud applications, messaging platforms, and compromised accounts. Visibility limited to the email gateway leaves critical gaps after delivery.

Next Level: What visibility do you have once an attacker moves beyond email?

☐ **9. Your email security loses visibility after message delivery**

Threats continue to evolve after messages reach the inbox through account takeover, internal phishing, mailbox manipulation, and multi-stage social engineering attacks.

Next Level: Can your security stack detect a threat that becomes malicious after it reaches the inbox?

☐ **10. Your security stack duplicates protections already native to Microsoft 365 or Google Workspace**

Many organizations maintain separate SEG infrastructure that overlaps heavily with native cloud protections while adding routing complexity, operational overhead, and additional policy management.

Next Level: **Which essential protections would disappear if your SEG was turned off tomorrow?**

What Modern Email Security Looks Like

The strongest platforms combine native cloud protections with behavioral detection, continuous visibility, and automated response, allowing security teams to detect attacks that look legitimate.

That means:

- Understanding identity and communication patterns
- Detecting threats after delivery, not just before
- Reducing manual triage and operational overhead
- Extending visibility across cloud applications and accounts

Legacy email security was built to inspect content.

Modern email security is built to understand behavior.

How Did Your Architecture Score?

If You Checked 3 or More Boxes...

Your email security architecture may be optimized for threats that no longer dominate the landscape.

Explore additional resources on modern attacks, SEG blind spots, and the shift to cloud-native email security.

See What's Next ›