Abnormal

5 Essentials for Augmenting Microsoft 365 Email Security

Microsoft 365 provides the baseline for email security. The most effective approach builds on those capabilities instead of duplicating them.

READ TIME
6 min

FOR
Security Leaders

01 Start With Microsoft's Native Security Baseline

Native Microsoft defenses provide:

- Spam and malware filtering
- Phishing & spoofing defense
- Quarantine & policy controls

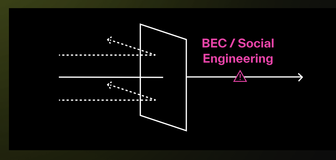
Microsoft 365

02 Address the Attacks Native Tools Don't Catch

Advanced attacks don't rely on malware or known indicators. They use:

- Legitimate accounts
- Familiar communication
- Real business workflows

They pass filtering, authentication, and standard detection controls.

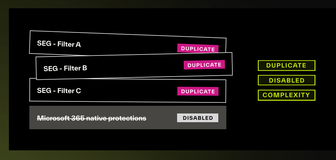


03 Avoid SEG Layers That Duplicate or Disrupt

When third-party SEGs sit in front of Microsoft 365, they:

- Duplicate filtering
- Disable native protections
- Add routing complexity

More tools. More overhead. Same gaps.

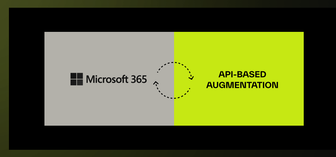


04 Extend Microsoft With API-Based Augmentation

The right approach integrates directly with Microsoft 365 by:

- Preserving native protections
- Adding behavioral detection
- Requiring no routing changes

No duplication. No disruption.



05 Achieve Full Coverage Without Added Complexity

Together, they cover the full attack spectrum.

Built for Microsoft 365. Designed for Modern Attacks.

Pairing native cloud protections with AI-native, behavior-based detection aligns email security with how today's attacks actually work.

Stronger Security. Lower Complexity.

LEGACY APPROACH

SEG → Microsoft

MODERN APPROACH

Microsoft + Behavioral Layer

Stronger Security | Simpler Stack | Clean Architecture | Measurable ROI