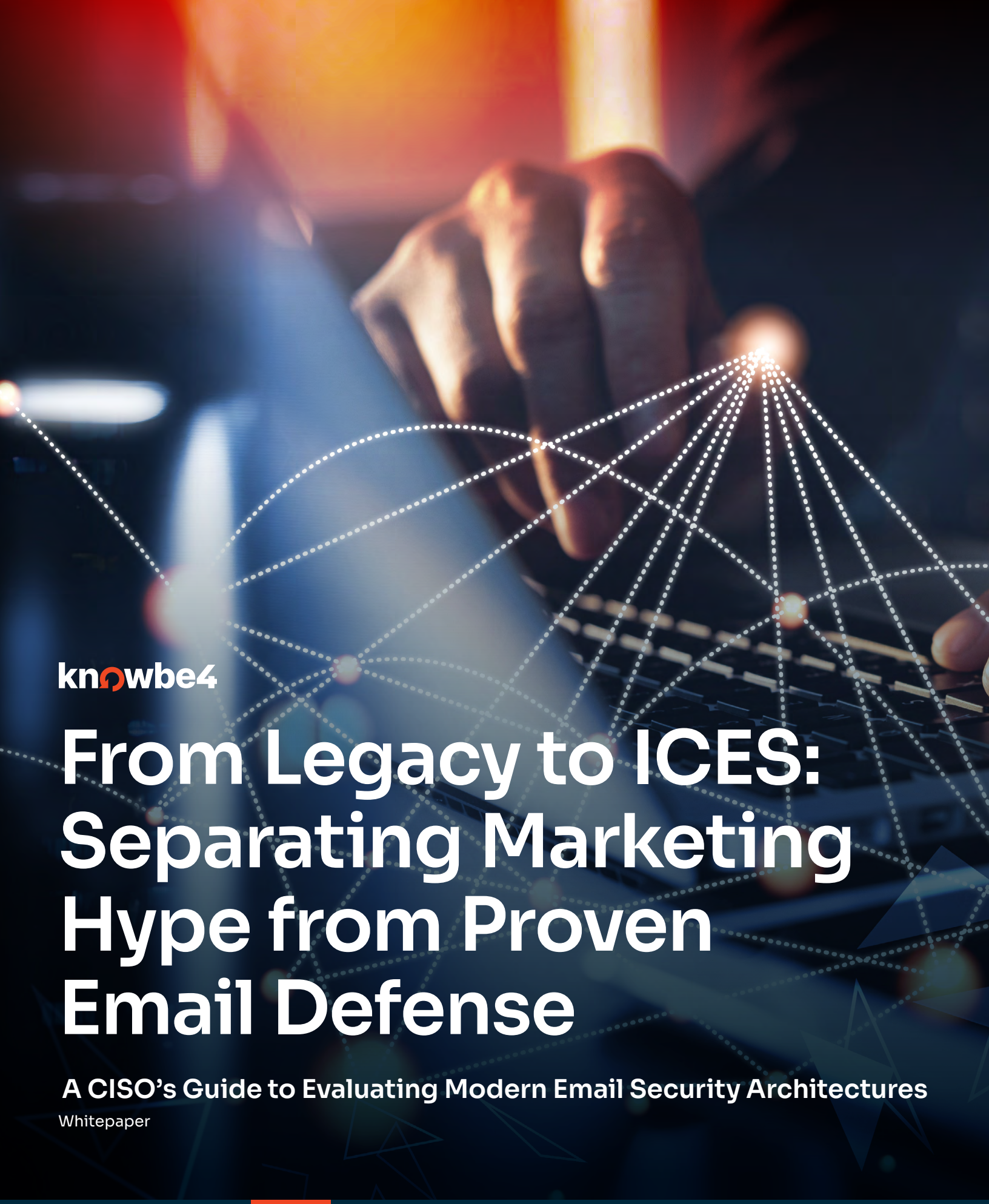

knowbe4

From Legacy to ICES: Separating Marketing Hype from Proven Email Defense

A CISO's Guide to Evaluating Modern Email Security Architectures

Whitepaper

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

CR-0494 0526

Introduction

The email threat landscape is evolving at an unprecedented pace. Cybercriminals, fueled by advancements in AI and a thriving crime-as-a-service ecosystem, are deploying increasingly sophisticated attacks designed to circumvent traditional perimeter defenses and exploit technology and human errors.

This shift has led a significant majority of cybersecurity leaders—**nearly 87%**—to either consider replacing their secure email gateway (SEG) or to have already done so.

Here's the issue: SEGs were engineered for a previous generation of threats. Their architecture, which inspects mail before it reaches the cloud tenant, lacks the deep contextual insight needed to identify today's most damaging attacks.

The time has come to give traditional SEGs a critical look. How best to determine if they still meet your needs? Read on to explore a strategic framework for assessing your current email security architecture, identifying the signs that your SEG is becoming obsolete, and planning a successful transition to a more effective, integrated defense model.

1. The Evolving Threat Landscape: Why SEGs Are Falling Behind

Traditional SEGs were designed to combat known threats, primarily by scanning for malicious attachments and spam signatures. While effective against bulk attacks, this model is fundamentally ill-equipped to handle the nuance and sophistication of modern cyber threats.

The Rise of Sophisticated, Payload-less Attacks

Today's attackers increasingly favor techniques that leave no obvious malicious footprint. These include:

- **Business Email Compromise (BEC):** Impersonating executives or trusted partners to initiate fraudulent wire transfers or solicit sensitive information
- **Vendor Email Compromise (VEC):** Hijacking legitimate vendor accounts to submit fraudulent invoices or alter payment details
- **Account Takeover (ATO):** Using stolen credentials to infiltrate an organization from within, launching attacks that appear to come from a trusted source
- **Advanced Phishing Techniques:** Employing methods like HTML smuggling, QR code phishing ("quishing") and hijacking legitimate hyperlinks to evade detection
- **Polymorphic Malware:** Constantly morphing cyber threat that slips past traditional defenses like SEGs, antivirus tools and rule-based detection products

These attacks succeed by exploiting human trust and bypassing technical filters. Because SEGs operate outside the native cloud environment, they are blind to the rich contextual and behavioral data needed to spot these anomalies, such as unusual communication patterns or requests that deviate from established workflows. Research shows that **a significant percentage of advanced threats** successfully bypass SEG detection, leaving the organization vulnerable.

Key Indicators Your SEG Is Being Bypassed:

- You are seeing an increase in user-reported phishing emails that were not blocked by the SEG
- Your incident response team is frequently remediating BEC or VEC attacks
- Threat analysis reveals that a high percentage of malicious emails passed standard authentication checks such as DMARC (Domain-based Message Authentication, Reporting and Conformance), a primary tool for SEGs

2. Limitations of Legacy SEG Architecture

The architectural model of a SEG is its primary weakness in a cloud-first world. By routing all email through an external gateway, organizations introduce latency and lose critical visibility.

Lack of Contextual Intelligence

An integrated, API-based security solution operates within the cloud tenant (e.g., Microsoft 365). This provides access to a wealth of data that an external SEG cannot see, including:

- **Internal Mail Flow:** The ability to analyze email traffic between employees to detect account takeovers and internal phishing
- **Communication Mapping:** Understanding established relationships and communication patterns to flag anomalous requests
- **Behavioral Profiles:** Building a baseline of normal user behavior to more accurately identify suspicious activity

Without this context, a SEG's analysis is limited and less effective. Studies show that **over half of advanced attacks originate from compromised accounts,** which reputation-based SEG defenses struggle to identify.

Operational Inefficiency and Complexity

Managing a SEG alongside a cloud email platform like Microsoft 365 creates a complex and inefficient dual-layer administration model. Security teams are forced to juggle:

- **Two Policy Engines:** Creating and maintaining security rules in two separate systems
- **Two Quarantine Systems:** Managing and releasing emails from multiple locations
- **Two Administrative Consoles:** Increasing administrative overhead and slowing incident response

This complexity not only drains valuable resources but also increases the risk of misconfigurations and policy gaps. The manual effort required for threat hunting and remediation across disparate systems is a significant burden on already strained security teams.

3. The Superiority of an Integrated Defense Model

A modern email security strategy moves beyond perimeter-based blocking and embraces a defense-in-depth approach. This involves enhancing the strong native security of your cloud platform with a specialized Integrated Cloud Email Security (ICES) platform.

Benefit 1: AI-Driven Behavioral Detection

ICES uses API integrations to gain deep visibility into your email environment. By applying advanced AI and machine-learning models, they can analyze a vast array of signals to detect threats that SEGs miss. This behavioral and contextual analysis is critical for identifying executive impersonation, vendor fraud and other subtle indicators of an attack. This approach allows security platforms to **stop a significantly higher percentage of targeted email attacks** than traditional solutions.

Benefit 2: Empowering Your People

Attackers know that humans are their primary target. While SEGs focus exclusively on technical filtering, a modern approach integrates the human element into the defense strategy. Key capabilities include:

- **Contextual Warning Teachable Moments:** In-the-moment warnings displayed within an email to alert users to specific risks (e.g., sharing sensitive data)
- **Real-Time Nudges:** Prompts that ask a user to confirm an action before sending an email to an unusual external recipient or with sensitive content
- **Integrated Security Awareness Training:** A feedback loop where real threats detected by the system inform targeted training and phishing simulations, strengthening your organization's security culture
- **Incident Response:** Easy end-user reporting and training on malicious emails that were once in their inboxes

Benefit 3: Streamlined Operations and Lower Total Cost of Ownership

Decommissioning a SEG in favor of an integrated solution delivers immediate operational benefits. It allows you to **centralize security management** into a single, unified console. This simplifies policy administration, streamlines incident response and reduces the administrative burden on your security team.

Additionally, eliminating a redundant SEG license fee often results in significant cost savings. These funds can be reinvested into a more effective approach that provides a measurable reduction in human risk and a stronger overall defense, delivering a greater return on your security investment.

4. Planning Your Transition

If moving away from your legacy SEG is the right move for you, here's a strategic plan outline for planning the transition.

Phase 1: Assess Your Current State

- **Analyze Performance:** Quantify the number and type of threats your SEG is missing. Review user-reported phishing incidents to establish a clear performance baseline
- **Review Native Capabilities:** Evaluate the security features inherent in your cloud email platform (e.g., Microsoft Defender for Office 365) to understand your foundational protection
- **Identify Gaps:** Determine where your current architecture is failing to stop advanced threats like BEC and account takeover

Phase 2: Evaluate Integrated Platforms/Tools

- **Define Requirements:** Prioritize capabilities such as AI-driven behavioral detection, API integration, automated incident response and tools for empowering users
- **Conduct a Proof of Concept:** Test leading ICES platforms in your live environment to validate their detection efficacy and operational benefits
- **Calculate Total Cost of Ownership:** Compare the costs of your current setup (including SEG license and administrative overhead) with the proposed integrated model.

Phase 3: Execute the Transition

- **Develop a Migration Plan:** Create a phased plan for redirecting mail flow (by changing MX records) and migrating security policies to minimize disruption
- **Train Your Team:** Ensure your security operations team is fully trained on the new platform's management console, incident response workflows and reporting features
- **Communicate with Stakeholders:** Clearly articulate the plan and its benefits to IT leadership, the security team and the broader organization

Conclusion

The only way to address evolving mail-based threats is a truly evolved security strategy. For most organizations leveraging modern cloud email platforms, the traditional SEG has become an expensive and redundant layer that offers diminishing returns. It creates operational friction while failing to stop the most sophisticated and damaging attacks that target organizations today.

By transitioning to an integrated security model—one that enhances native cloud defenses with an AI-powered ICES platform—CISOs can achieve a superior level of protection. This modern architecture not only catches more threats but also reduces complexity, lowers costs and transforms the human element from a liability into a formidable layer of defense. The question is no longer if you should replace your SEG, but **how soon you can make the strategic shift** to a more resilient and efficient security posture.

Explore KnowBe4's Approach to ICES

Learn More

Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Email Exposure Check

Find out which of your users emails are exposed before bad actors do

Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization

Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain

Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click

About KnowBe4

KnowBe4 empowers the modern workforce to make smarter security decisions every day. Trusted by more than 70,000 organizations worldwide, KnowBe4 is the pioneer of digital workforce security, securing both AI agents and humans. The KnowBe4 Platform provides attack simulation and training, collaboration security, and agent security powered by AIDA (Artificial Intelligence Defense Agents) and a proprietary Risk Score. The platform leverages 15-years of behavioral data to combat advanced threats including social engineering, prompt injection, and shadow AI.

By securing humans and agents, KnowBe4 leads the industry in workforce trust and defense. More info at **knowbe4.com**.

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com