

Critical Capabilities When Evaluating Integrated Cloud Email Security





Introduction

Email remains the most exploited attack vector in today's cyberthreat landscape. From credential phishing and business email compromise (BEC) to ransomware and accidental data loss, organizations face a constant barrage of threats targeting users' inboxes. Enterprises need advanced, flexible and integrated email security platforms as they migrate to cloud-native environments like Microsoft 365 and Google Workspace.

Traditional gateway-based tools are no longer sufficient. Modern attacks are increasingly sophisticated, often bypassing legacy defenses with social engineering, zero-day tactics and insider threats. Additionally, regulatory pressures and the shift to hybrid work have elevated the importance of outbound protection, visibility and seamless user experience.

This paper outlines the critical capabilities that Security Operations (SecOps) and IT teams should prioritize when evaluating Integrated Cloud Email Security platforms (ICES). It explores four key pillars:

- 1 **Core Threat Protection Capabilities**
- 2 **Outbound Security and Data Loss Prevention**
- 3 **Visibility, Management and Reporting**
- 4 **Cloud-Native Architecture and Integrations**

Whether you're replacing a legacy product or building a modern security stack, understanding these capabilities is essential to choosing the right platform.

1. Core Threat Protection Capabilities

ICES platforms must deliver multilayered protection that goes beyond traditional filtering. The following core capabilities are essential for SecOps and IT teams to effectively detect, remediate and prevent targeted attacks.

→ Advanced Phishing Detection and Remediation

At the forefront is AI- and machine learning-driven phishing detection, which analyzes content, headers and behavioral signals to identify known and emerging phishing techniques—including zero-day threats and social engineering. These systems go beyond static rules by detecting brand impersonation, domain lookalikes and display name spoofing, which are commonly used in credential harvesting and executive fraud. Critically, best-in-class platforms also offer post-delivery protection, allowing threats that slip past initial filters to be identified and removed from all user inboxes—shrinking dwell time and reducing the organization’s exposure window.

→ Business Email Compromise Protection

Unlike traditional phishing, BEC often lacks obvious payloads or malicious links, making detection more difficult. Leading ICES platforms use behavioral analysis to identify anomalies in communication patterns, such as unusual tone, timing or financial requests. Sender identity verification technologies like DMARC, SPF and DKIM are enforced to authenticate inbound email and flag spoofed messages. Lastly, enterprise-grade platforms should also include executive impersonation detection, which applies logic to protect high-risk users from being spoofed or targeted in fraud attempts.

→ Malware Ransomware Defense

To address malware and ransomware, modern ICES platforms incorporate deep file inspection and sandboxing to detonate suspicious attachments and analyze embedded code behavior in a safe environment. Malicious URLs are neutralized through URL rewriting and time-of-click analysis, blocking delayed or redirected payloads that evade static scanning. Lastly, the integration of threat intelligence feeds helps enrich detection capabilities by correlating email artifacts against known indicators of compromise, enabling faster and more confident threat verdicts.

Together, these capabilities form a layered, adaptive defense that enables SecOps and IT teams to detect, respond to and mitigate the full spectrum of email-borne threats.

2. Outbound Security and Data Loss Prevention

Protecting sensitive data from leaving the organization via outbound email is just as critical as stopping inbound threats. Effective ICES platforms must provide comprehensive outbound security and data loss prevention (DLP) capabilities that reduce the risk of data exposure, maintain regulatory compliance and guard against user error.

→ Data Loss Prevention for Email

At the core of outbound protection is email DLP. These systems detect and block the unauthorized transmission of sensitive information such as personally identifiable information, protected health information and payment card data. To meet the varied needs of different organizations, ICES platforms should offer both predefined DLP policies aligned with industry best practices and the ability to create custom rules tailored to specific compliance goals. Integration with regulatory frameworks like GDPR, HIPAA and CCPA ensures that outbound email handling supports legal and governance obligations.

→ Encryption and Secure Messaging

Encryption and secure messaging are also essential. Policy-based encryption allows organizations to apply protections automatically based on content, recipient or sender behavior, while also enabling manual encryption when needed. For recipients outside the organization, secure portals or message pickup links provide a seamless way to access encrypted content. Support for Transport Layer Security (TLS) ensures secure transmission between mail servers, and some platforms include compatibility with third-party key management or customer-managed encryption keys for added control.

→ Misdirected Email Prevention

Misdirected email prevention helps reduce the frequency of human errors, such as sending sensitive information to the wrong recipient. Features like context-aware alerts and confirmation prompts before sending add an extra layer of protection, especially when emails involve sensitive content or unfamiliar external addresses.

Together, these outbound security capabilities form a critical layer of defense in today's data-driven, highly regulated environments.

3. Visibility, Management and Reporting

Effective email security requires full-spectrum visibility, streamlined administration and actionable insights. When evaluating ICES platforms, SecOps and IT teams should prioritize products that offer robust management and reporting capabilities that save time, support investigations and drive continuous improvement.

→ Unified Admin Console

A unified admin console is essential for centralized visibility and control. The platform should provide a real-time dashboard that displays threat activity, quarantine status, policy effectiveness and overall email hygiene across the organization. To support operational scale and security, role-based access control and delegated administration features allow organizations to assign responsibilities based on function or geography, without compromising oversight.

→ Detailed Reporting and Forensics

In-depth reporting and forensic tools are critical for both incident response and strategic planning. Message trace functionality enables security teams to track the lifecycle of a specific email—when it was received, delivered, quarantined or interacted with—to support rapid investigations. Campaign-level views help identify the source of an attack, impacted users and progression over time. For integration into broader security operations, ICES platforms should support SIEM logging and offer APIs for exporting data to third-party systems and dashboards.

→ End-User Controls and Education

Empowering end users is equally important. Intuitive interfaces for managing quarantined emails reduce help desk tickets and increase user autonomy. A built-in phishing reporting button encourages users to participate in the organization's defense, while integrations with security awareness training products help reinforce positive behaviors. ICES platforms should also provide real-time alerts or contextual coaching when users interact with suspicious messages, bridging the gap between security enforcement and user education.

Together, these visibility and management capabilities ensure that security teams have the insight, tools and user engagement needed to stay ahead of evolving threats and maintain a strong security posture.

4. Cloud-Native Architecture and Integrations

Modern email environments demand cloud-native security products that integrate seamlessly with the platforms organizations already rely on, specifically Microsoft 365 and Google Workspace. When evaluating ICES platforms, SecOps and IT teams should prioritize products built for the cloud from the ground up, with tight ecosystem compatibility and scalable, resilient infrastructure.

→ Integration With Microsoft 365, Google Workspace

Unlike legacy approaches that rely on MX record redirection, best-in-class ICES platforms offer native API-based integrations that connect directly to Microsoft 365 and Google Workspace. This enables deep, mailbox-level access for inline threat remediation, journaling and analysis without disrupting mail flow. Platforms should also support shared mailboxes and delegated access, which are common in both enterprise and service desk environments.

→ Threat Intelligence and Ecosystem Compatibility

To enhance detection accuracy and response speed, integration with the broader cybersecurity ecosystem is critical. ICES platforms should support the ingestion and enrichment of threat intelligence feeds, including formats like STIX and TAXII. Compatibility with SIEMs, SOAR platforms and EDR/XDR tools allows teams to execute end-to-end investigations and responses across security domains. Enterprise-grade platforms also enable feedback loops, using confirmed incidents and user reports to continuously refine detection models and accelerate time to resolution.

→ Scalability, Uptime and Support

A strong cloud-native platform must also deliver enterprise-grade performance and reliability. This includes high availability with 99.99%+ uptime SLAs, multi-tenant architecture for global scale, and dynamic service scaling to handle surges in email volume or threats. Equally important is 24/7 support with transparent incident response processes and defined SLAs to ensure rapid assistance when needed.

Cloud-native architecture and ecosystem integrations are foundational to building an email security strategy that supports rapid detection, deep interoperability and consistent protection across diverse environments.

Conclusion

As email threats evolve and cloud adoption accelerates, relying on outdated security models is no longer viable. Modern ICES platforms must offer more than just basic filtering—they need to deliver advanced threat protection, outbound data loss prevention, deep visibility and seamless cloud-native integrations. By focusing on these critical capabilities, SecOps and IT teams can strengthen their organization's email security posture, reduce operational burden and respond to threats with greater speed and precision.

Learn more about KnowBe4's

Cloud Email Security





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 the bad guys 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](https://www.knowbe4.com).



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

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.