mimecast™

# Top 10 Capabilities that Organizations Need in a Secure Email Gateway:

## A buyer's guide

# Security Depends on Email Security

Email has become one of the most common and successful attack vectors for cybercriminals. The combination of new threats and the need for enhanced protection is driving the adoption of cloud-based secure email gateways (SEGs), including email itself, are moving to the cloud.

The best, cloud-based SEGs provide multiple forms and layers of protection against email-borne threats. Unlike with many older email security products, these solutions' defensive capabilities protect against much more than broadly distributed threats that arrive with incoming mail. They protect against data exfiltration and domain spoofing, analyze URLs and file attachments, deliver threat intelligence, and much more. Given how many attacks are email-based, cloud-based SEGs are a key foundational component of a strong cyber defense.

Strong email security can have broad positive impact on an organization. Everyone uses email - including attackers. So, deploying email protection benefits many parties: users, help desk, compliance, SecOps/IT Ops, executives, and legal, to mention a few. It is critical that the SEG meet the needs of all those groups, and so the SEG buying process will often include these diverse groups to ensure that all the bases are covered.

**To help you become more informed and to help organizations choose the best SEG, this buyer's guide will detail the ten most important capabilities organizations should seek in a solution.**

# Top 10
## Capabilities for best-in-class SEGs

The 10 key features explored in this section deliver broad coverage that will provide effective current and future defenses against email-borne threats. This list may seem large, but to ensure comprehensive protection, each of these capabilities is extremely important.

### One: Use of multiple analytic techniques to detect malware and malicious attachments.

No technology silver bullet exists to provide the perfect detection of malware. The most effective SEGs will be able to rapidly adapt to changing threats. They'll combine best-in-class third party and proprietary engines and feeds to deliver the best protection at any point in time. To be effective, the SEG must use multiple anti-virus engines, behavioral sandboxing, static file analysis, file type exclusions, and have the ability to check for and block executable files, and other dangerous file types. This is a big list, but it provides the depth necessary to offer real protection given all the ways malicious files can hide.

### Two: Safeguarding against bad clicks.

Despite increased user training focused on raising user awareness of the dangers of "bad clicks," they still happen. Attackers are quite clever, and what looks innocuous may not be. For example, some attackers will scrape content from legitimate sites and use domain names similar to well-known and trusted sites to persuade users to click and trust the site they land on. What looked to the user like a safe URL might have had just one letter changed, which can be difficult for a person to notice. And given the fact that malicious web sites often only live for a few hours, traditional blacklisting-based techniques are proving increasingly ineffective.

### Three: Protection against advanced domain spoofing and brand impersonation.

Attackers have become incredibly proficient at spoofing email addresses and making emails look and sound legitimate. The same is true for domains that appear similar but are not legitimate. For example, "Microsoft Support" email phishing attacks have become quite common. But to really protect email and users, domain spoofing protection is needed. It must include multiple types of domain checking. Your SEG needs to know if the domain is new (too new to be blacklisted, but so new as to be suspicious), if it is from whom it is supposed to be from, and if there are other domain irregularities. Using Domain-based Message Authentication, Reporting and Conformance (DMARC) and other brand protection tools are important to delivering the best possible defense. The best solutions will also be able to "score" a specific email using multiple techniques to proactively identify if the sender is who they say they are.

### Four: Open APIs and integration with other security solutions.

One of the current major problems that reduces the effectiveness of the SecOps team is the proliferation of security systems, consoles and reporting. The data coming in is so voluminous that finding the real threats may be difficult and conducting investigations often take too long. The SEG must help to address this problem by being a good team player with APIs and integrations that work with other security systems and thus help

bring data and systems together for the security team. More importantly, APIs and connectors allow threat intelligence and information about attacks to be shared, making all cyber-defenses more effective. A good example of this is the ability to update SEG defenses based on threats being seen elsewhere in the API infrastructure or vice versa. The ability to help drive toward an integrated defensive posture is a key goal for SecOps teams. The ability to integrate the SEG also makes it possible to drive greater synergy across an organization's prevention/detection/response systems and processes as well.

### Five: The ability to inspect internally generated messages for sensitive data movement, malware, or malicious links.

One of the most common blind spots for email security is a lack of inspection of internally generated emails, which can be as dangerous as inbound mail. For example, many attacks, particularly account takeover attacks, will compromise internal email inboxes, which can then be used to infect others in the organization and to exfiltrate data. During the lateral movement phase of an attack, internal messages are often used to spread malware, malicious links, or sensitive content. Increasing the scrutiny of internally generated email will ensure that compromised accounts can't be used as Trojan horses to spread an attack. To be most effective the SEG must also provide both automated and manual removal of unwanted, malicious, or compromised mail, post-delivery.

### Six: Delivery of threat intelligence.

Threat intelligence is a very important resource for defending against cyberattacks. Because the SEG will constantly encounter email-based attacks targeting an organization, it can provide very useful data that can be leveraged within other security systems. This information should inform both the SEG and other security products such as a SIEM. The ability to share threat intelligence from the SEG with other tools adds real-time and external threat data into the defensive posture of the organization. Information about attacks that have been prevented is very useful for the SecOps team as it analyzes the threats coming at their organization. The SEG provides critical information about attacks including who, why, and how specific individuals have been attacked.

SEG threat intelligence is also valuable for comparing attack data for one organization against other firms. Such comparisons, based on geography, industry, or company size, can provide important insights into whether an attack is targeting just your organization or is more general. This information can be critical in determining the response. The combination of threat intelligence integration internally and comparisons against other firms in the community is the foundation of actionable intelligence, and a critical capability that a SEG must provide.

### Seven: Protection from malicious URLs combined with dynamic user awareness education.

Most users will participate in the raising of overall cybersecurity levels if given the chance. The right SEG can help make end users a more effective last line of defense for the organization. A well-designed SEG will engage users with useful and interesting services that help them become an integral part of the organization's defensive posture - whether they are accessing their email from a laptop, a desktop, or a smartphone. The seamless protection of a next-generation SEG helps eliminate the smartphone as an email attack vector, as is too often the case today. Regardless of platform, the SEG should help users understand how it protects them, explaining why specific emails are blocked and delivering a level of training to help users be more cognizant of malicious emails and the choices they are making. Web-based challenges are also an excellent way of engaging the user. The SEG should interact with users, sending warnings such as "Are you really sure you want to click on that?" And the SEG will let SecOps know which users are ignoring those warnings or engaging in risky behavior, so that those users can get additional training, information, scrutiny, or protections. Best-in-class SEGs don't take users out of the picture, they provide information to help the user make better informed decisions. And they must provide self-service so that every potentially malicious or quarantined email does not create a ticket for support or SecOps.

**Eight: Tools for transporting large files or sensitive emails outside of the regular email system.**

Many corporate email systems have limitations for large file sending or messages with highly sensitive information. Faced with these limitations, many users resort to an external solution to send their large files, even though that solution is unsecured and unauthorized. That's why the best SEGs include tools for transmitting large files or sensitive information or attachments with full protection. Not only are the files protected, but the organization can ensure that sensitive data isn't being exfiltrated. The SEG's detection, audit, tracking, and management tools also protect sensitive datasets and keep this sensitive content and large files away from the public internet, to ensure that nothing is lost in transit or to exploits of the public infrastructure.

**Nine: The ability to provide security, continuity, and backup and recovery in a single integrated solution.**

Providing security is the primary job of any SEG, but the most advanced solutions do more. The use of cloud-based SEG solutions provide not just security, but better resilience and backup capabilities than on-premises or cloud-based email services. Many hosted or cloud-based email systems don't have great backup and archiving capabilities. Some (such as Microsoft 365) keep emails for only weeks, unless they are marked for legal hold.

The persistent backup capabilities of the best-in-class SEGs is critical to full email protection. The advanced SEG's backup protection also protects against ransomware or a technical failure. And to complement enterprise grade backup, the best SEGs include automated, point-in-time recovery capabilities so that mailboxes can be rehydrated whenever needed. Delivering email continuity is another critical feature as primary email systems, whether on-premises or cloud-based, periodically become unavailable. Organizations need an independent system that can support a 100% SLA for their email systems.

**Ten: The ability to demonstrate improved efficacy of the new SEG.**

When contemplating an upgrade to a new cloud-based SEG solution, the new SEG option should be able to sample a prospective customer's delivered email and quickly show details on how malicious emails or otherwise unwanted emails are getting around the existing SEG. This testing is critical to providing an analysis of how protection can be improved, and how defenses against email borne threats can be enhanced with a replacement SEG. As new threats and email attacks evolve, older defenses often can't keep up. With this analysis of what is getting by the current SEG, the organization will more clearly understand the increased efficacy of the next-generation SEG before they purchase.



# Key takeaways

Protecting the organization against email-borne threats is only becoming more difficult as attackers create new and more clever ways to fool users and embed threats and malware. The best SEG solutions provide better protection than older products or those that are available with an email platform itself.
To ensure that your organization is getting the maximum protection, it is important that the new SEG solution you are evaluating has, at a minimum, the 10 capabilities discussed here.

Learn more

mimecast