WHAT CAN (SHOULD) YOUR EMAIL SECURITY SOLUTION DO FOR YOU

When evaluating email security solutions, consider what you expect a solution to provide – and what you really need.

1 INBOUND EMAIL PROTECTION

US Signal	Other	
☑	☐	**Payment and payroll fraud protection** - It can stop emails that mimic an external entity for nefarious purposes, as well as those that appear to be from an employee in order to steal money or payroll-related information.
☑	☐	**Impersonation protection** - It protects against impersonation attacks on company executives and other key internal staff.
☑	☐	**Extortion and ransomware protection** - It can stop emails that threaten users with negative actions unless they take a specific action or pay a ransom.
☑	☐	**Credential phishing protection** - It can stop emails that contain links or redirect recipients to fake login pages in an attempt to steal account credentials.
☑	☐	**BEC and social engineering attack protection** - It can protect against email attacks that try to compromise recipients' trust to steal money or data.
☑	☐	**URL scanning and decoding** - It scans URLs and traces all redirections down to the URL's final destination.
☑	☐	**Attachment scanning** - It scans email attachments for malicious and zero-day links.
☑	☐	**Email authentication checks** - It can perform DMARC, DKIM, and SPF authentication on email domains.
☑	☐	**Automated and customizable remediation** - It can automatically delete, quarantine, or apply other remediation actions to detected threats.

2 EMAIL ACCOUNT COMPROMISE PROTECTION

US Signal	Other	
☑	☐	**Anomalous login detection** – It can detect and alert on anomalous login into user accounts.
☑	☐	**Unusual mail forwarding rule detection** – It can detect and remove unusual mail forwarding rules set up by attackers or malicious insiders.
☑	☐	**Impossible travel detection** – It can detect and alert on simultaneous login from geographically disparate locations that are impossible.
☑	☐	**Internal mail protection** – It scans internal emails to prevent lateral movement of attacks.
☑	☐	**Automated and customizable remediation** – It can revoke user access following suspicious account behaviors.

3 PHISING / ABUSE MAILBOX REMEDIATION

US Signal	Other	
☑	☐	**Phishing / Abuse Mailbox Remediation** – It connects with your company's abuse/phishing mailbox to automatically scan all reported emails.
☑	☐	**Automated remediation** – It can configure automated remediation actions for user-reported emails flagged as suspicious or safe.
☑	☐	**Threat insights** – It provides threat analysis, IOCs, and in-email highlights for all user-reported threats.
☑	☐	**Bulk remediation across mailboxes** – It can group and automatically remediate identical and similar emails across affected user mailboxes.
☑	☐	**Policies to protect against future threats** – It includes self-learning mechanisms that acknowledge manual actions to automatically apply the same actions to similar and identical future threats.
☑	☐	**End user notifications** – It provides labels and warning banners to end users containing information about the attack with calls-to-action.

4 DETECTION CAPABILITIES

US Signal	Other	
☑	☐	**Identity-based detection** – It can analyze signals based on user identity.
☑	☐	**Behavior-based detection** – It can analyze signals based on user behavior.
☑	☐	**Language-based detection** – It can analyze signals based on language eg. sentiment and tone, topics discussed, writing styles.
☑	☐	**Threat feed integrations** – It allows for native integrations into threat feeds for real-time threat information, and REST API availability for integration with other threat feeds.
☑	☐	**Image analysis** – It can detect fake login screens and attachments using image analysis techniques.

5 REMEDIATION CAPABILITIES

US Signal	Other	
☑	☐	**End user quarantine** – It provides end users with individual quarantine folders where they can manage and release emails.
☑	☐	**End user feedback** – It includes warning banners and inline messages to increase user awareness and empower them to perform triage tasks (mark safe, mark suspicious).
☑	☐	**Automated and bulk remediation** – It automatically deletes, quarantines, or marks questionable emails as safe based on predetermined remediation actions. Automated email actions can be applied across user mailboxes.
☑	☐	**Abuse mailbox automation** – It forwards emails to the company abuse/phishing mailbox automatically for investigation and remediation across user mailboxes.

6

ARCHITECTURE + ENTERPRISE CAPABILITIES

US Signal	Other	
☑	☐	**Cloud platform** – It's offered as a cloud service.
☑	☐	**API-first architecture** - It can connect to mail providers over APIs, without the need for MX record modifications or email rerouting.
☑	☐	**Autoscaling** - It can autoscale up or down dynamically depending on data and resource load.
☑	☐	**Exchange support** - It supports on-premise Exchange deployments.
☑	☐	**Hybrid model support** - It supports hybrid deployments, such as Active Director on Microsoft 365 but using Exchange on-premise.
☑	☐	**Multi-tenant support** - It supports multi-tenant deployments.
		Audit logs - It provides detailed audit logs to track user activity.
☑	☐	**Role-based access control** - It provides different roles that govern data visibility and level of access to product capabilities.
☑	☐	**SSO support** – It protects solution access through single sign-on (SSO).
☑	☐	**Third-party accreditation** - It meets the requirements of regulations and/or industry standards such as SOC2, HIPAA, GDPR, and CCPA.
☑	☐	**Monitoring** - It provides continuous monitoring and reporting by an expert intelligence team.

THE EXTRAS

Use this page to note additional "must haves" and "nice to haves."

**This checklist is for informational purposes and is not intended to use as a security plan. Depending on your organization's business requirements, needs and other variables, there may be other factors to consider when developing and implementing a security plan.*

LEARN WHAT US SIGNAL OFFERS

US Signal's Advanced Email Security detects and stops email-borne cyber threats before they can reach end users' inboxes. It can be used with Microsoft 365, Microsoft Exchange, Open-Xchange, Gmail, or any cloud email service, and is SOC2 compliant, HIPAA certified, GDPR compliant, and CCPA compliant.

The solution recursively unpacks embedded files and URLs and separately analyzes them with dynamic and static detection engines. This enables it to detect advanced evasion techniques used to hide malicious content, preventing malware and other email threats that make it past conventional defenses.

It leverages proprietary software algorithms that examine code at the CPU level, so it can act earlier in the attack chain to block exploits before malware is released. The solution also uses machine-intelligence-enhanced Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) record checks.

The technology in Advanced Email Security scales to cover 100% of the email traffic. This shortens scanning time to a maximum of 30 seconds with verdicts delivered almost immediately. Yet another unique feature of the solution is that an expert intelligence team continuously monitors all customer traffic, analyzes malicious intent, and provides ongoing reporting and 24/7 support.

Learn more at: ussignal.com/advanced-email-security

US SIGNAL® Acronis