Advanced Email Security

Leverage leading-edge technologies and threat intelligence to immediately block even the most sophisticated email-based cyberattacks.

US Signal's Advanced Email Security powered by Perception Point and Acronis is a comprehensive solution that integrates cutting-edge threat prevention with the speed, scale and flexibility of the cloud. Multiple scanning engines and in-depth threat intelligence protects against attacks like phishing, spam, commodity malware, and BEC. Hardware visibility, combined with software agility, enables it to see what other security solutions miss.

Propriety software algorithms examine code at the CPU-level, intercepting attacks at the earliest stage possible before malware is even delivered. That all enables US Signal's Advanced Email Security to provide Zero Day, N-day, and everyday threat coverage — protecting your business against the full range of potential attacks.

AT-A-GLANCE

+ Single platform protects against full range of email borne threats
+ Works with Microsoft 365, Microsoft Exchange, Open Xchange, Gmail, or any cloud email service
+ Easy, one-click cloud deployment with no changes to existing processes
+ In-line engines work in a matter of seconds
+ Scans 100% of email traffic — regardless of volume
+ Analyzes any code executed by the system for 100% visibility into malicious intent
+ Unpacks files and follows URLs to detect evasive malicious intent
+ Blocks malicious content before it ever reaches end users
+ SOC2 compliant; no data is stored on servers
+ Expert intelligence team continuously monitors incidents

ONE DETECTION PLATFORM FOR ANY CYBER THREAT

Protect against any content-based attack, including files, URLs, and plain texts. Deploy across channels, regardless to scale or traffic volume.

Zero-Days + N-Days

Phising

BEC

ATO + Lateral Phising

Malware

Evasion

PROTECTION FEATURES

US Signal's Advanced Email Security combines a full array of defense and risk mitigation technologies and strategies to offer the most comprehensive email security, including:

Fast Scanning
Detects malicious hidden content by recursively unpacking the content into smaller units (files and URLs). They're dynamically examined by multiple engines in under 30 seconds – faster than legacy sandboxing solutions that can take more than 20 minutes.

Next-generation Dynamic Detection
Stops advanced attacks such as APTs with CPU-level analysis that detects and blocks them at the exploit stage by identifying deviations from normal execution flow during runtime.

Threat Intelligence
Stays on top of emerging threats with the combined threat intelligence of market-leading sources and a unique engine that scans URLs and files.

Static Signature-based Analysis
Identifies known threats with best-in-class, signature-based AV engines enhanced with a unique tool to identify highly complex signatures.

Spam Filter
Blocks malicious communications with anti-spam and reputation-based filters that draw on data from several advanced technologies.

Anti-phishing Engines
Detects malicious URLs based on leading reputation engines, along with advanced image recognition technology to validate URL legitimacy.

Anti-spoofing
Prevents payload-less attacks — including look-alike domains, spoofing, and display name deception — through the use of machine-learning algorithms with IP reputation, SPF, DKIM, and DMARC record checks.

Incident Response Service
Provides direct access to cyber analysts who act as an extension of your service delivery team. In addition to monitoring all customer traffic and analyzing malicious intent, they provide ongoing reporting and support, including handling false positives, remediating, and releasing when required.

HOW IT WORKS

1. **Reputation and Anti-Spam Filters**
Receives the email then applies the reputation and anti-spam filters to quickly flag an email as malicious.

2. **Recursive Unpacker**
Unpacks the content into smaller units (files and URLs) in a recursive manner to identify hidden malicious attacks. All of the extracted hidden components go separately through to the next security layers.

3. **Threat Intelligence and Scanning**
Combines multiple threat intelligence sources with a unique internally developed engine that scans URLs and files in the wild to warn about potential or current attacks.

4. **URL Reputation Engines and Image-recognition Analysis**
Best-in-class URL reputation engines coupled with image-recognition analysis engine identify impersonation techniques and phishing attacks.

5. **Signature-based AV Engine**
Combines leading signature based anti-virus engines to identify malicious attacks and a proprietary tool that specializes in identifying highly complicated signatures.

6. **Payloadless Attack Prevention**
Prevention of payload-less attacks including spoofing, look-alike domain, and display name deception.

7. **CPU Level Blocking**
Unique CPU-level technology acts earlier in the kill chain than any other solution. Blocking attacks at the exploit phase – pre-malware release – for true APT prevention.