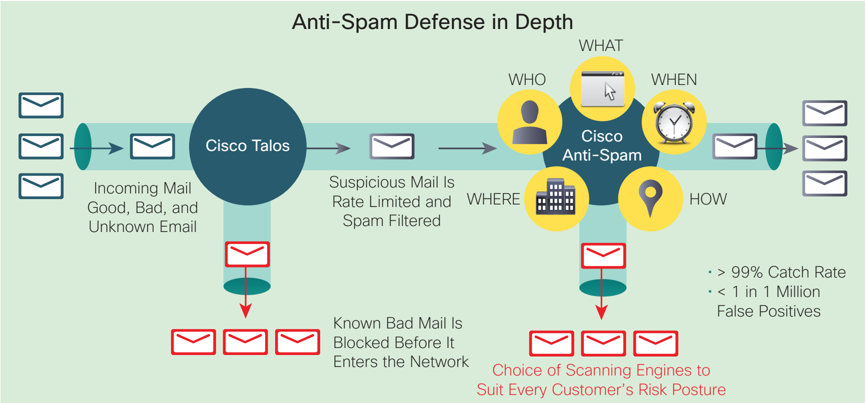
At-a-Glance

Cisco Email Security Appliance

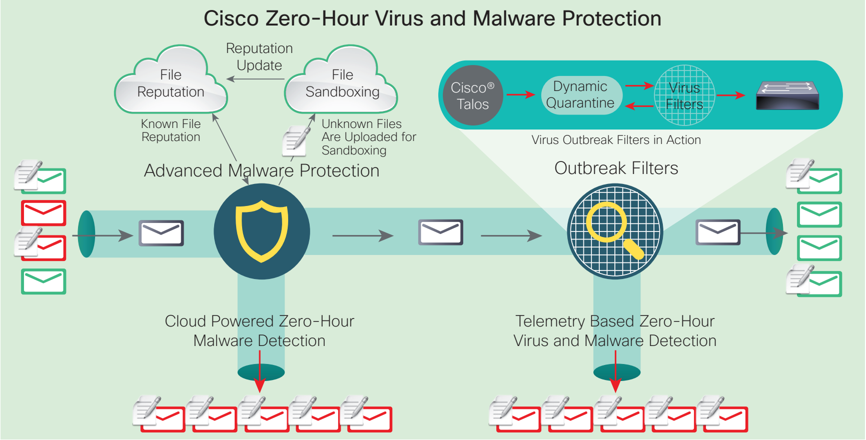
Protect Your Business from Email-Based Attacks

Email is a critical business communication tool, but it can expose daunting threats. The average cost of a security breach is $4.5 million, according to the Radicati Group's "Email Statistics Report, 2012–2016." And email gateways are the number one threat vector for a security breach. Sophisticated and highly targeted attacks use personal information and social engineering tactics to deceive users and direct them to malicious sites serving up malware.


Anti-Spam Defense in Depth
Incoming Mail Good, Bad, and Unknown Email
Cisco Talos
Suspicious Mail Is Rate Limited and Spam Filtered
WHO
WHAT
WHEN
WHERE
HOW
Cisco Anti-Spam
Known Bad Mail Is Blocked Before It Enters the Network
Choice of Scanning Engines to Suit Every Customer's Risk Posture
• > 99% Catch Rate
• < 1 in 1 Million False Positives

Today's email-based threats demand a dedicated array of resources, technologies, and expertise to safeguard systems against existing and evolving attacks. Cisco® Email Security Appliance (ESA) answers the call by staying one step ahead of these advanced threats to keep your inbox highly secure.

This all-in-one appliance defends against spam, advanced malware, phishing, and data loss. Our Advanced Malware Protection (AMP) feature, available with a simple add-on license, provides continuous protection before, during, and after an attack - by blocking threats, mitigating the scope of an attack, and remediating it quickly. And the AMP system, along with the Threat Grid appliance, can now be deployed completely on premises with the AMP private cloud license. This is important for customers who have stringent policy requirements that do not allow for use of the AMP public cloud.


Cisco Zero-Hour Virus and Malware Protection
File Reputation
Reputation Update
File Sandboxing
Known File Reputation
Unknown Files Are Uploaded for Sandboxing
Advanced Malware Protection
Cisco® Talos
Dynamic Quarantine
Virus Filters
Virus Outbreak Filters in Action
Outbreak Filters
Cloud Powered Zero-Hour Malware Detection
Telemetry Based Zero-Hour Virus and Malware Detection

Benefits

- **Get faster, more comprehensive email protection** often hours or days ahead of the competition.
- **Gain access to one of the largest networks of threat intelligence** with Cisco Talos, built on real-time collective security analytics.
- **Protect outbound messages** through on-device data loss prevention (DLP), email encryption, and optional integration with RSA's Enterprise DLP solution.
- **Lower your total cost of ownership** with a small footprint, easy implementation, and automated administration that yield savings for the long term.
- **Gain maximum deployment flexibility** with an on-premises, cloud or hybrid deployment. Change your deployment mix at any time during the term of your contract.

> “With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam [are] a reality.”

Kenichi Tabata
Komatsu Ltd., Japan

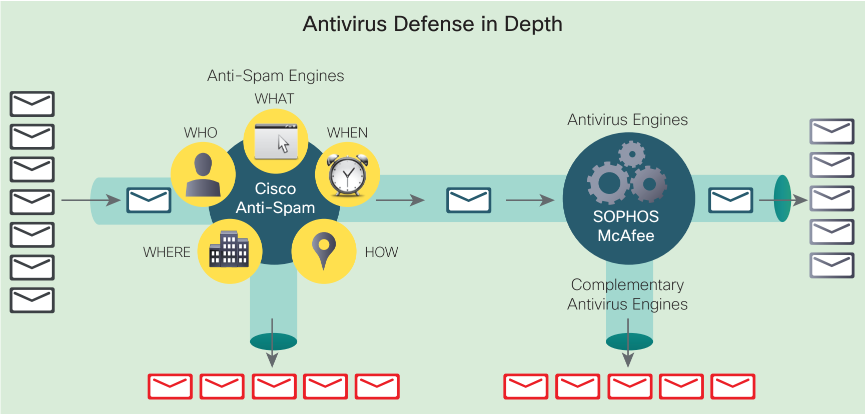
Next Steps

Learn More

Find out more about the Cisco ESA at http://www.cisco.com/go/esa. A Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco products will work for you.

Deploy Multilayered Defense to Tackle Multiple Threats

Integrated into the Cisco ESA is our Cisco Talos service, which provides a 24-hour view into global traffic activity. This intelligence enables us to analyze anomalies, uncover new threats, and monitor traffic trends. Automatic policy updates are pushed to network devices every three to five minutes.


Antivirus Defense in Depth

We make it easy to stop spam from reaching your inbox. A multilayered defense combines an outer layer of filtering based on the reputation and validity of the sender and an inner layer of filtering that performs a deep analysis of the message.

You can also protect against spoofing attacks with Forged Email Detection. These targeted attacks focus on executives also known as high-value targets. This feature provides detailed logs on all attempts and actions taken.

With ESA you can also:

- Stop phishing and blended threats
- Identify graymail and tag with “safe unsubscribe” option
- Satisfy requirements for highly secure messaging with dependable, secure encryption – keys are stored on-premise or in the cloud.
- Comply with industry and government data-loss prevention regulations
- Defend against advanced threats and targeted attacks
- Track users that have clicked malicious URLs
- Set and enforce detailed email policies

With a choice of physical appliance, virtual, cloud-based or hybrid deployment, you can find a solution that meets the needs of your business.