Email Security Buyer’s Guide

Email: The Leading Attack Vector for Cyber Attacks

Cybercriminals are turning to email more than ever to deliver threat-centric content, using it to introduce malware into corporate systems, steal data, and extort money. With the growing adoption of cloud mailbox services like Office 365, blended attacks can target an organization from more than one side.

Although a variety of attack types continue to wage war on business email, three categories of attack are now causing the greatest concern.

- **Ransomware.** A particular kind of malware that blocks a target company’s access to its own data, ransomware caused losses of US$1 billion in 2016 (csoonline.com).
- **Business email compromise (BEC).** A real moneymaker for cybercriminals and an even bigger threat than ransomware, BEC persuades high-value targets to send funds or sensitive information to malicious individuals. According to the Internet Crime Complaint Center (IC3), US$5.3 billion was stolen due to BEC fraud between October 2013 and December 2016 (ic3.gov).
- **Phishing** continues to be an effective attack method with clever social engineering and targeted spear phishing that dupes users into activating their campaigns and eventually compromising entire organizations. During the second quarter of 2017, 67 percent of the malware hitting organizations was delivered via phishing attacks (nttcomsecurity.com).

With email security, cybercriminals can weaponize three areas of the message.

- The body of the email
- Attachments
- URLs within the email

US **$1 Billion** loss
from ransomware[2]

US **$5.3 Billion**:
the cost of compromised
business email[3]

67% of malware
delivered via phishing[4]

[1] Cisco 2017 Midyear Cybersecurity Report, Cisco (2017). https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

[2] Korolov, Maria. “Ransomware Took In $1 Billion in 2016–Improved Defenses May Not Be Enough to Stem the Tide,” CSOonline.com (January 5, 2017). https://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html

[3] “Business E-Mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam,” Internet Crime Complaint Center (IC3) and the Federal Bureau of Investigation (May 4, 2017). https://www.ic3.gov/media/2017/170504.aspx

[4] GTIC 2017 Q2 Threat Intelligence Report, NTT Security (August 8, 2017). https://www.nttcomsecurity.com/en/gtic-2017-q2-threat-intelligence-report/

Buyer’s Criteria for Email Security

Cisco security research[5] shows your organization needs an email solution that delivers on five critical requirements to ensure the deeply layered protection your business needs today and in the future.

1. Effective intelligence, analysis, and response across your security posture
2. Rapid retrospective remediation
3. Protection against BEC
4. Protection against data leakage and risk from outbound email
5. Encrypt sensitive business information

Requirement 1: Effective Intelligence, Analysis, and Response Across Your Security Posture

As cyber attacks have become more sophisticated, so has the security deployed against them. Cybercriminals now deploy a wide range of threats that challenge traditional security methods. To be effective, your email security solution needs to go beyond the basic perimeter tools that inspect email at a single point in time. In addition to covering the basics, it must also integrate multiple layers of security in a more holistic approach that continuously analyzes threats and monitors traffic trends.

With this approach, your solution can react rapidly to threat indicators based on the very best intelligence. This gives your security team the level of deep visibility and control it needs to reduce the time to detection (TTD)[6] of an attack, scope the event, and contain malware before it causes damage.

How Cisco Provides Effective Security Across Multiple Vectors

Cisco deploys a number of methods to create the multiple layers of security needed to defend against multiple attack types.

- Geolocation-based filtering safeguards against sophisticated spear phishing by quickly controlling email content based on the location of the sender.
- The Cisco® Context Adaptive Scanning Engine (CASE) provides spam capture rates greater than 99 percent and an industry-low false positive rate of less than one in one million.
- Automated threat data drawn from Cisco Talos™ identifies threats with increasing speed, reducing TTD and exposing even the newest zero-day attacks.
- Advanced Malware Protection (AMP) delivers global visibility and continuous analytics across all components of the AMP architecture for endpoints and mobile devices and in the cloud and network to identify malware based on what it does, not what it looks like.
- AMP also provides persistent protection against URL-based threats via real-time analysis of potentially malicious links.

Faster Detection Reduces Potential Harm

Cisco has lowered the median TTD from just over 39 hours in November 2015, when the company first started tracking, to approximately 3.5 hours for the period of November 2016 to May 2017.

Source: Cisco 2017 Midyear Cybersecurity Report. Cisco (July, 2017).

Threat Intelligence

Talos is Cisco’s team of more than 250 full-time threat researchers, who track new and emerging threats. Intelligence is gathered from a wide range of sources, including other Cisco security products, which is then shared with Cisco Email Security customers for more effective protection. By seeing a threat once and blocking it everywhere, Talos provides best-in-class protection and safeguards against blended attacks as they are emerging and blocks them.

[5] Cisco 2017 Midyear Cybersecurity Report. Cisco (July, 2017). https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

[6] Cisco defines time-to-detection (TTD) as the time between a compromise and the detection of the threat.

Retrospective Security for Office 365

AMP uses automated retrospective security to take action on infected inbound and outbound emails for Office 365 customers to help remediate breaches faster and with less effort.

If a seemingly good attachment is later discovered to be malicious, an automated API call is made to Azure and the file is forwarded or deleted.

Requirement 2: Rapid Retrospective Remediation

When malware, phishing attacks, or a malicious URL get through your front-line defenses, your business needs continuous threat monitoring and assessment in place to detect the problem, quickly understand the impact or potential effect of the event, and then remediate it as quickly as possible.

How Cisco Provides Automated Retrospective Remediation

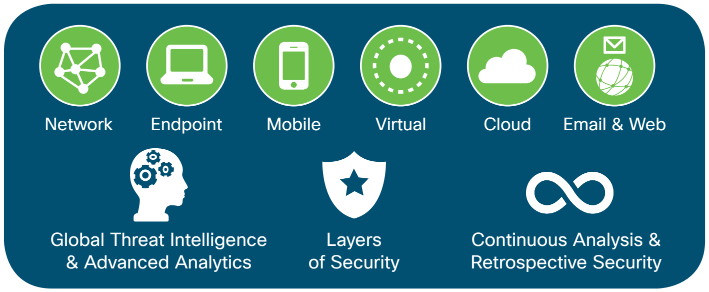
Cisco continuously examines your security environment for malicious files or URLs that may have slipped through or suddenly changed disposition.

- Advanced outbreak filters provide ongoing deep inspection of URLs. With real-time click-time analysis, so that even websites that change from good to malicious behavior can be blocked quickly.
- AMP continuously leverages real-time Talos monitoring and analytics and Cisco Threat Grid intelligence to identify previously unknown threats or sudden changes in the disposition of a file.
- AMP also takes steps to remediate by automatically triggering dynamic reputation analysis and providing visibility into where the malware originated, what systems were affected, and what the malware is doing. After automatically prioritizing remediation, AMP takes action on both inbound and outbound email based on these insights.

Requirement 3: Protection Against BEC

Business email compromise (BEC), or impostor email, is a form of phishing attack in which a cybercriminal impersonates an executive (often the CEO) and attempts to get an employee, customer, or vendor to transfer funds or sensitive information to the phisher.

BEC attacks are highly focused and use social engineering techniques to scrape compromised email inboxes, study company news, and research employees on social media to make the email look convincing. Because they don't use malware or malicious URLs to threaten organizations, BEC attacks can be very difficult to detect.


Network
Endpoint
Mobile
Virtual
Cloud
Email & Web
Global Threat Intelligence & Advanced Analytics
Layers of Security
Continuous Analysis & Retrospective Security

Protection Across Multiple Attack Vectors

Advanced Malware Protection (AMP) provides continuous analysis and retrospective security across your security environment in addition to traditional point-in-time detection techniques.

How Cisco Safeguards Against BEC

Cisco uses a multilayered approach to BEC that monitors worldwide email and web traffic using sophisticated web reputation filters and advanced email authentication technologies to identify spear phishing attempts.

- Forged Email Detection (FED) makes it easier to detect spear phishing attacks by examining one or more parts of the SMTP message for manipulation, including the “Envelope-From”, “Reply To”, or the “From” headers. A suite of authentication tools targets these parts: Sender Policy Framework (SPF) for sender authentication and DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) for domain authentication.
- Visibility into email senders and their domains enables authorization of legitimate senders and blocks fraudulent emails before they reach employees, business partners, and customers.

Requirement 4: Protection Against Data Leakage and Risk from Outbound Email

Email Security solutions must detect, block, and manage risks in outbound email. This includes guarding against malicious content sent to customers and business partners and preventing sensitive data from leaving the network—either by accident or by design. In addition to losing critical intellectual property, compromised email accounts containing malware can propagate a virus by launching sudden outbound spam bursts. This can lead to a blacklisting of the organization’s email domain, even when the emails are signed.

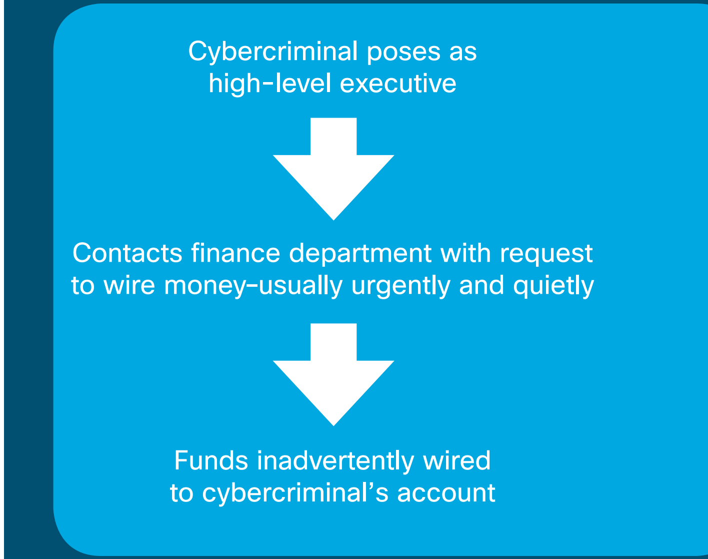
How Cisco Protects Against Data Leakage and the Risk of Outbound Threats

- AMP provides security layers for outbound email, including behavioral monitoring to detect compromised accounts, rate limiting for outbound traffic, and antispam and antivirus scanning--which can keep compromised machines or accounts from getting your company on email blacklists.
- Cisco DLP technology provides content, context, and destination knowledge to prevent accidental or malicious loss of data, enforce compliance, and protect your brand and reputation. You control who can send what information where and how.
- More than 100 up-to-date predefined policies help prevent data loss and support security and privacy standards for government, private sector, and custom company-specific regulations. For example, filters such as “HIPAA,” “GLBA,” or “DSS,” enable automatic scanning and encryption of payload according to policy to prevent the loss of data. Remediation choices include adding footers and disclaimers, adding blind carbon copies (BCCs), notifying, quarantining, encryption, and more.
- In addition, Transport Layer Security (TLS) digital certificates provide communications protection by authenticating the user as well as the network for privacy and data integrity between sender and recipient.

Predefined Policies for Compliance

Cisco Email Security helps organizations comply with these privacy and security standards:

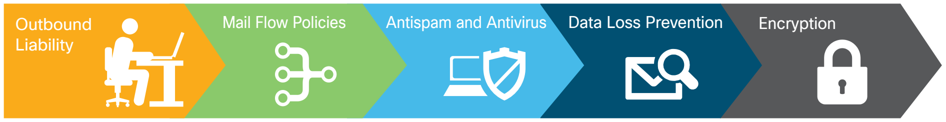
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- State and European privacy directives and regulations



Cybercriminal poses as high-level executive

Contacts finance department with request to wire money-usually urgently and quietly

Funds inadvertently wired to cybercriminal’s account



Cisco Email Security combines several layers of security for reducing the risk of outbound threats.

Requirement 5: Encrypt Sensitive Business Information

Companies should be able to rely on secure communications to conduct their business activities without fear of compromise. Encryption is one of the critical security layers for protecting data leaving your network. Whether it's malicious or accidental, encryption can keep sensitive information such as financial and personal information, competitor intelligence, and intellectual property from exposure.

How Cisco Encrypts Data

Cisco uses the most advanced encryption key service available today to manage email recipient registration, authentication, and per-message/per-recipient encryption keys.

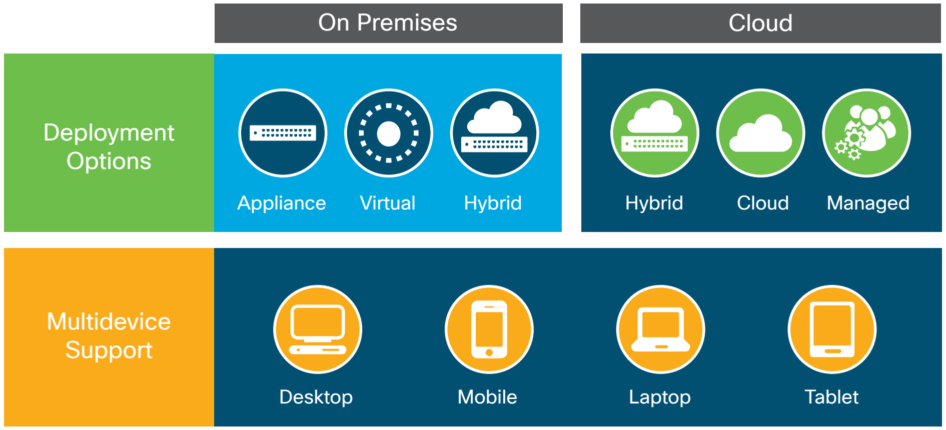
- Superior TLS support helps configure the best method of delivery. The gateway also gives compliance and security officers the control of and visibility into how sensitive data is delivered.
- A customizable reporting dashboard provides instant access to information about encrypted email traffic, including the delivery method used and the top senders and receivers.

Cisco Email Security Solution Offers

The Cisco Email Security solution offer high-availability layers of email protection against the dynamic, rapidly changing threats affecting organizations today. Our unique approach delivers protection, often hours or days ahead of the competition based on intelligence from Talos, the industry's largest security research organization.

Simple setup and automation provides protection within minutes. Our solution is cost-effective, on-guard, and up-to-date. Subscriptions start as low as 100 users and the same features and deployment choices are available to customers of all sizes.

Flexible deployment options include on-premises or in the cloud with hybrid models and managed services that support a range of endpoint devices. Regardless of how you choose to deploy, you get the same code base with the same features enabled. This means you can deploy security today on premises, and then migrate to a hybrid environment and even fully deploy to the cloud in phases while keeping consistent policies and familiar user interfaces across environments.



Flexible email security deployment options.

Why Cisco Email Security Solution?

Today organizations need a multilayered email security model to protect against sophisticated new and emerging multi-vector threats such as BEC, ransomware, and URL-based attacks. Cisco's architectural approach to security integrates across products, so you get effective intelligence sharing across the portfolio. The result is a faster, more synchronized response across security layers.

- Fortified by shared intelligence, our Email Security solution goes way beyond single-point-in-time scanning to provide:
- The most robust and predictive global intelligence from Cisco Talos that sees attacks before they impact your systems.
- Protection from risky files no matter when they become malicious and mitigation of damage if an infection occurs—with the same protection for Office 365 email users.
- Deep, real-time URL scanning, analysis and blocking that catches malicious changes at click time.
- Prevention of sensitive information from inadvertently getting out so you can stay compliant with industry and government regulations.
- Comprehensive and real-time reporting to reduce investigation and response times.
- Flexible deployment options with the same robust email protection on-premises and in the cloud so you can migrate with confidence.
- A small footprint, easy implementation, and automated administration to yield savings over time and a low total cost of ownership.

Try us for Free for 45 Days

The best way to understand the benefits of Cisco Email Security is to put us to the test in a free, 45-day trial. This easy-to-use trial also includes our most popular email security add-ons, including Advanced Malware Protection for Email and ThreatGrid.

For additional information, please visit: www.cisco.com/go/emailfreetrial