Cisco Secure Email

Cisco Secure Email Buyer's Guide

Protecting the #1 threat vector

Email: The Leading Attack Vector for Cyber Attacks, Again

Organizations continue to face a daunting challenge. Email is simultaneously the most important business communication tool and the leading attack vector for security breaches.

The ubiquitous, and casual, use of email makes it the perfect avenue to deliver threat-centric content, insert malware into corporate systems, steal data, and extort money.

With the growing adoption of cloud mailbox services like Microsoft 365, and the massive exodus from corporate campuses over the last year, blended attacks can target an organization from anywhere.

Although a variety of attack types continue to wage war on business email, three categories of attack remain the greatest cause concern:

1. Ransomware
2. Business Email Compromise (BEC)
3. Phishing

715% YoY increase
in Ransomware attack during 2020[1]

US $75,000:
the average amount requested in in wire-transfer based BEC attack[2]

95% of network attacks
in 2020 caused by successful phishing attacks[3]

[1] BitDefender 2020 Mid-Year Threat Landscape Report, 2020. https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

[2] ”How Email Attacks are Evolving in 2021, Threatpost.com, February 11, 202. https://threatpost.com/email-security-attacks-bec/163869/

[3] Kritikal Blogsm “Staggering Phishing Statistics in 2020. https://www.kratikal.com/blog/staggering-phishing-statistics-in-2020/

Buying criteria for email security

Given the tactics used by these three categories of attack, Cisco recommends deploying an email security solution that delivers on five critical requirements. Your email security should:

1. Leverage the strength of a platform approach
2. Deliver layered security and retroactive remediation
3. Protection against business email compromise
4. Safeguard against data leakage and risk from outbound email
5. Encrypt sensitive business information

1 Leverage the strength of a platform approach

Given the ever-increasing sophistication of the threat landscape, it is essential that your email security solution takes full advantage of the benefits of having a built-in platform approach for better, faster threat response.

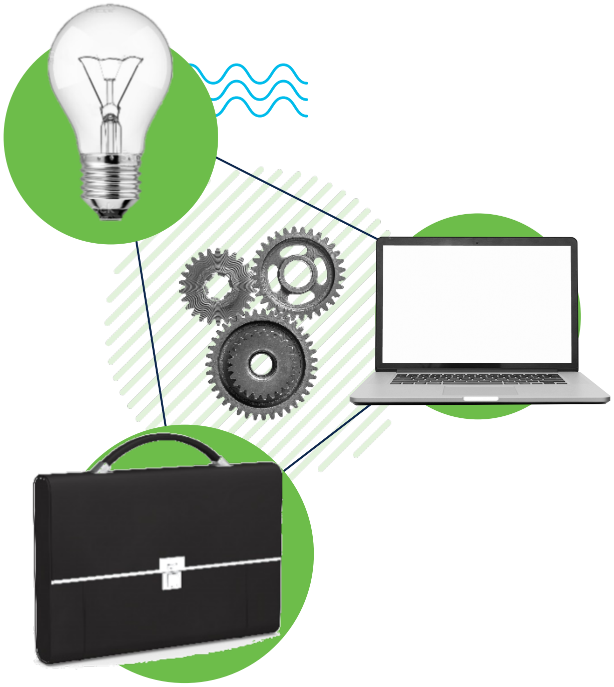
Unlike a SIEM or a SOAR, which both add value in their own ways, Security Platforms offer native integrations that make it much easier to scale security functionality across traditionally segmented threat vectors like email. Instead of being limited to the context that is generated by the native detection and response engines, a platform-enabled email security solution gains intelligence from the entire environment. Better intelligence means faster, and better, security decisions. Additionally, platforms enable a higher level of automation, which alleviate administrative burdens and further accelerate the detection and remediation of threats while minimizing human error.

Anytime a vendor claims to have a security platform, make sure to figure out what they mean by “platform”. Not all platforms are created equal, nor do they provide the same benefits.

The three main platform types you’ll encounter include:

1. Solution-based platforms
2. SIEM or SOAR-based platforms
3. Portfolio-based Platform

Learn about the differences here.



How Cisco delivers on the promises of a platform approach

Cisco SecureX is a cloud-native, built-in platform that connects Cisco Secure Email to the rest of the Cisco Secure Portfolio as well as 3rd party solutions. The broadest, most integrated platform on the market, SecureX removes bottlenecks that currently hinder convoluted security workflows. Our security platform:

- Simplifies security with customizable dashboards that provide operational metrics, insights in to emerging email threats, and access to additional security functionality in a single click.
- Unifies device information into a comprehensive device inventory, delivering the contextual awareness needed to identify gaps in coverage and simplify security investigations.
- Accelerates threat response and incident management by combining email intelligence with that of other threat vectors into a single view.

> “
>
> Cisco Secure Endpoints (Formerly AMP for Endpoints) and Cisco Secure Email with SecureX threat response are valuable integrations because that is where we see most attacks happening.”
>
> *— Wouter Hindriks*
>
> *Senior IT Architect, Missing Piece*

To learn more about the platform visit cisco.com/go/securex

2

Deliver layered security and retroactive remediation

To be effective, your email security solution needs to go beyond basic, single point-in-time inspection and should integrate multiple layers of security that repeatedly analyze threats and monitors traffic trends. It is inevitable that ransomware, malware, phishing attacks, or malicious URLs will get through front-line defenses, and so continuous threat monitoring and assessment will be the best way to detect the problem, understand the impact or potential effect of the event, and then remediate it as quickly as possible.

Threat Intelligence

Talos is Cisco's team of more than 350 full-time threat researchers, analysts, engineers, linguists, developers, and other operators work around the clock digging deep into threats, tracking actors, creating and shipping detection, and adding deep, meaningful context to threat intelligence.

This intelligence is gathered from a global 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.

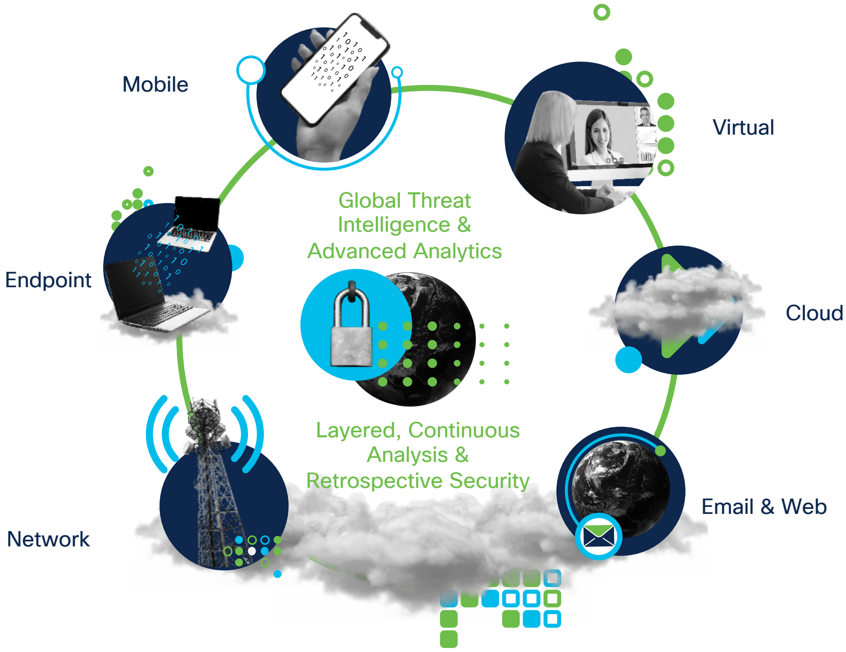
How Cisco Secure Email provides layer security and automated retrospective remediation

Cisco Secure Email deploys a number of methods to create the multiple layers of security needed to defend against multiple attack types and continuously examines your security environment for malicious files or URLs that may have slipped through.

- 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.
- 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.
- Cisco Secure Email Malware Defense provides persistent protection against URL-based threats via real-time analysis of potentially malicious links.
- Malware Defense 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.
- Malware Defense 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, Malware Defense takes action on both inbound and outbound email based on these insights.

Protection Across Multiple Attack Vectors

Malware Defense provides continuous analysis and retrospective security across your security environment in addition to traditional point-in-time detection techniques.


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

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.

Retrospective Security for Microsoft 365

Malware Defense uses automated retrospective security to take action on infected inbound and outbound emails for Microsoft 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.

To learn more about security for Microsoft 365 visit cisco.com/go/cmd

How Cisco Safeguards Against BEC

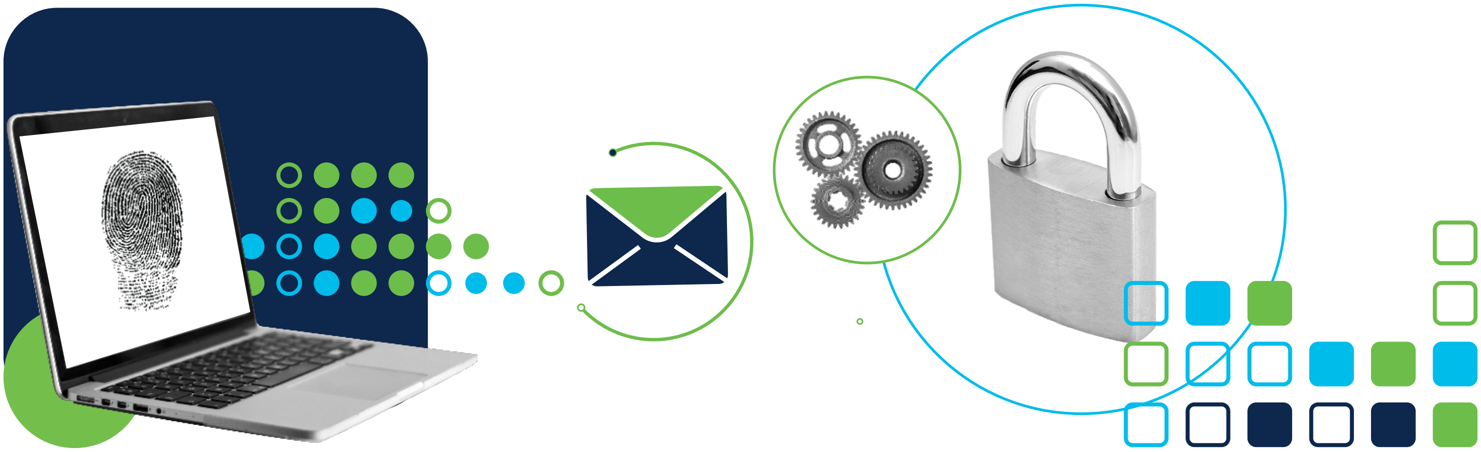
Cisco uses a multilayered approach to BEC that monitors worldwide email and web traffic using sophisticated web reputation filters and advanced email authentication technologies to identify spear phishing attempts

- Forged Email Detection 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.

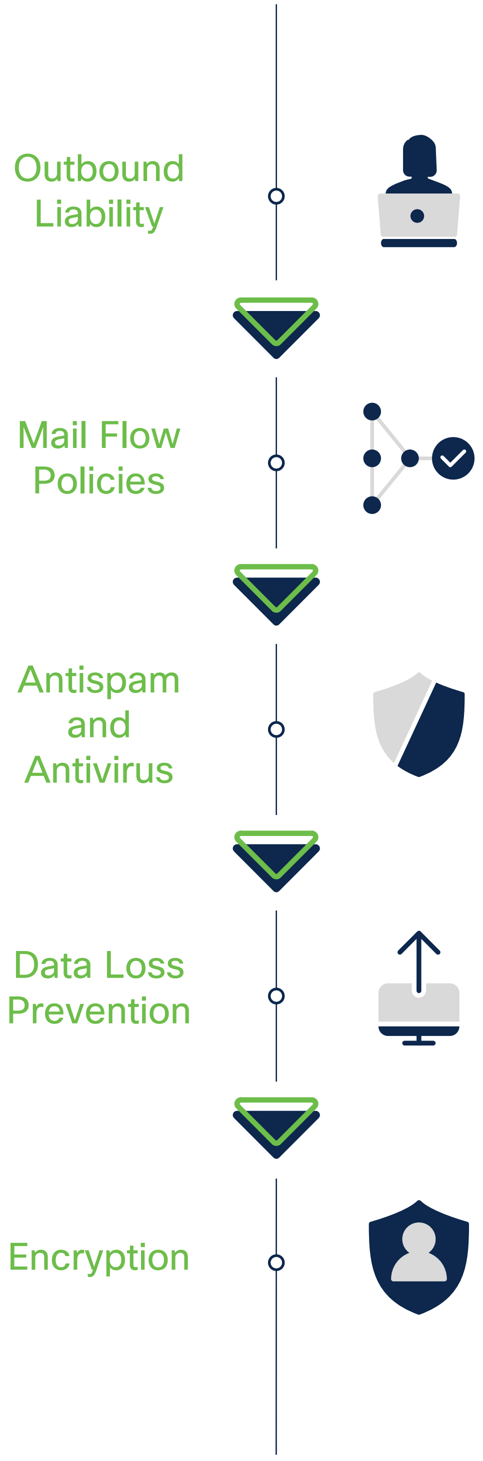
4 Protection Against Data Leakage and Risk from Outbound Email

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 block-listing of the organization’s email domain, even when the emails are signed.



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

- Vides 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 Data Loss Prevention 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.
- Over 150 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.
- Policies include:
  - 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
- 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.



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

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.

Read our recent datasheet for more information on Cisco's encrypted email service.

How Cisco Encrypts Data

Cisco Secure Email 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 Secure Email represents a suite of deployment options

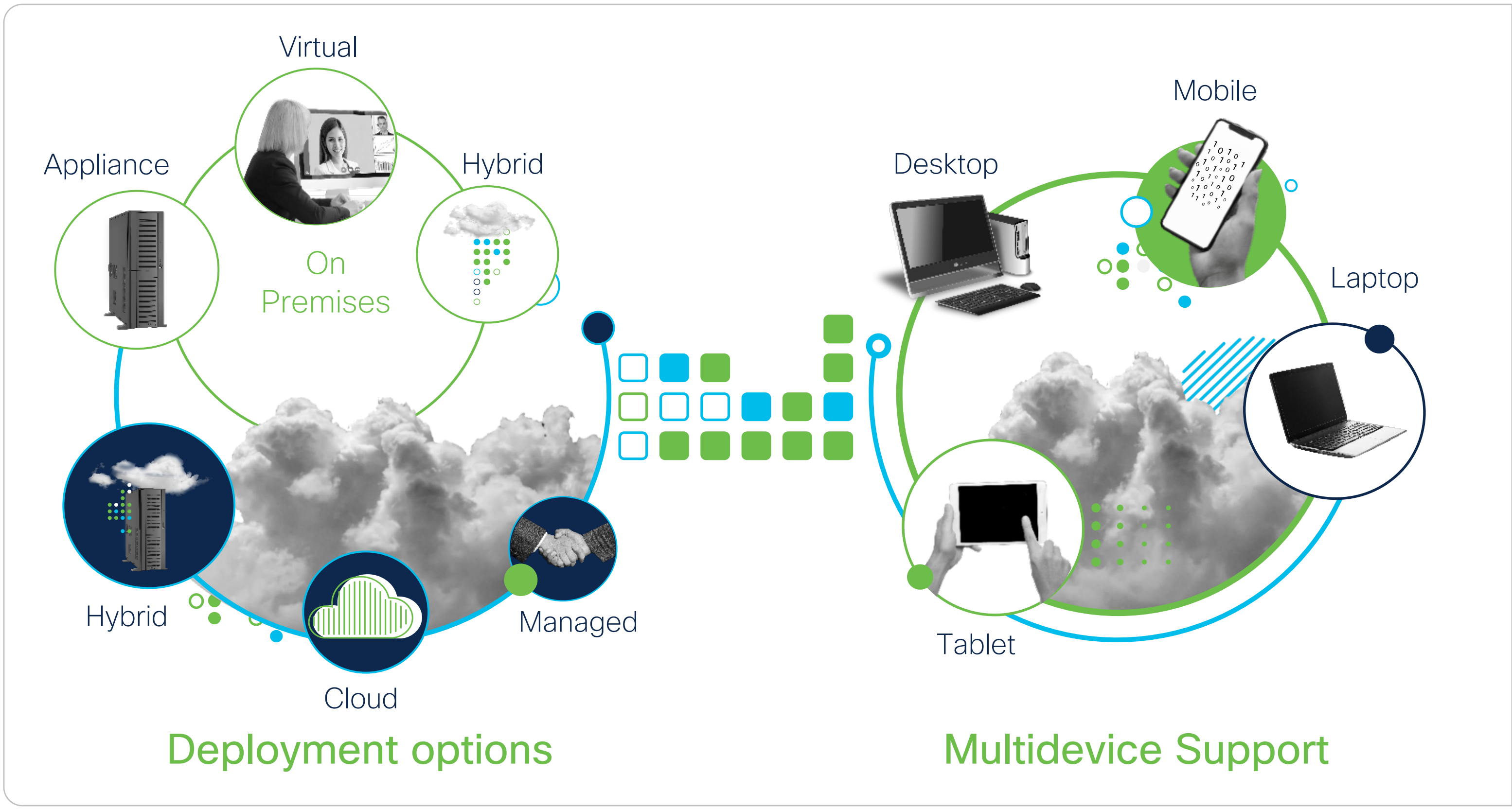
There's a growing interest in an evolution of email security; a comprehensive solution that provides the highest levels of security, unparalleled integration and the ability to greatly reduce complexity. This is exemplified by Cisco Secure Email.

A proven industry leader, Cisco Secure Email delivers comprehensive protection for on-premises or cloud-based email by stopping ransomware, phishing, spoofing, business email compromise, malware and other common cyber threats. It protects against malicious content, remediates attacks and prevents loss of sensitive information. Built-in capabilities with SecureX provide visibility and integration across the entire security portfolio to simplify the ability to search for and remediate threats.

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.

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.

To learn more, visit cisco.com/go/emailsecurity



Try Cisco Secure Email today

Today organizations need a platform-enabled, multilayered email security model to protect against sophisticated multi-vector threats such as BEC, ransomware, and URL-based attacks.

Our best-of-breed protection is exactly what your businesses need to keep on-premises and cloud email safe. Our platform 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:

- **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 Microsoft 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

The best way to understand the benefits of Cisco Secure Email is to put us to the test in a free, 45-day trial.

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

How to buy

To view buying options and speak with a Cisco sales representative, visit www.cisco.com/c/en/us/buy.