
Five Requirements
When Considering Email Security

What You Will Learn

The continually evolving threat landscape is what makes discovery of threats more relevant than defense as a modern approach to email security. Enterprises must focus on content inspection, behavior-anomaly detection, and advanced forensics to gain visibility into threats that are already present. They must understand where the data is, how it is being accessed and shared, and by which users in what places using what types of devices.

Today's organizations need an email security solution that:

- Provides protection across the entire attack continuum—before, during, and after an attack
- Stays ahead of the evolving threat landscape
- Protects sensitive data and prevents it from leaving the organization
- Handles the wide variety of spam and viruses
- Addresses new attack vectors as they emerge

Challenges

Email is the number-one threat vector for cyber attacks, according to the *Cisco 2015 Annual Security Report*.* The increasing amount of business-sensitive data sent by email means the potential for leakage is great. Hacking is now industrialized, and targeted campaigns are more sophisticated. Email virus attacks and spear-phishing schemes are on the rise, delivering malware designed to infiltrate data centers where high-value data resides. The advanced malware that malicious actors deploy can easily evade point-in-time security solutions and spread quickly through a network.

Mass spam campaigns and unsafe email attachments are no longer your only email security concerns. The email threat landscape contains increasingly sophisticated blended threats and targeted attacks. By scouring social media websites, criminals now find information on intended victims and create sophisticated and highly targeted attacks using personal information and social engineering tactics that may be tied to global news events. Nonintegrated point solutions and multiple management platforms intended to enhance security only create gaps that adversaries can use to launch targeted malware that can modify its behavior and evade detection.

Clearly, hackers are benefiting from the expanded attack surface: As the Cisco® Talos Security Intelligence and Research Group (Talos) researchers noted in the *Cisco 2014 Annual Security Report*, "Security is no longer a question of if a network will be compromised. Every network will, at some point, be compromised." Cisco Talos researchers report that malicious traffic is visible on 100 percent of corporate networks, which means all organizations should assume they've been hacked.**

In today's threat landscape, where the security perimeter has been pushed to the cloud and data is a prime target for attack, the chance of a compromised network is essentially assured. That's why today's organizations need an email security with the following capabilities.

*Cisco 2015 Annual Security Report, Cisco, Jan. 2015.

**Cisco 2014 Annual Security Report, Cisco, Jan. 2014.

FIVE REQUIREMENTS WHEN CONSIDERING EMAIL SECURITY

1. Provides Protection Across the Entire Attack Continuum—Before, During, and After an Attack
2. Stays Ahead of the Evolving Threat Landscape
3. Handles the Wide Variety of Spam and Viruses
4. Protects Sensitive Data and Prevents It from Leaving the Organization
5. Addresses New Attack Vectors as They Emerge

Requirement 1: Provides Protection Across the Entire Attack Continuum—Before, During, and After an Attack

Employees once checked text-based email from a workstation behind a company firewall. Today they access rich HTML messages from multiple devices, anytime and anywhere. Ubiquitous access creates new network entry points that blur the lines of historically segmented security layers.

Today's email security solutions provide continuous monitoring and analysis across the extended network, so enterprises have greater ability to stop threats and protect users across the full attack continuum—before, during, and after an attack. And when compromise inevitably occurs, security personnel will be better positioned to determine the scope of the damage, contain the event, remediate, and bring operations back to normal as quickly as possible.

Requirement 2: Stays Ahead of the Evolving Threat Landscape

Modern web security requires the ability to block malware from both suspicious and legitimate sites before it reaches a user. Business tools that increase productivity can significantly increase the probability that users will encounter malware. Even legitimate websites can pose a threat by malware designed to hide in plain sight. Web security in this environment must be capable of dynamic reputation- and behavior-based analysis. It also must be nuanced enough to support policies that give employees customized access to the sites they need while selectively denying the use of undesired sites and features like web-based file sharing.

Requirement 3: Handles the Wide Variety of Spam and Viruses

Phishing continues to prove its value to criminals as a tool for malware delivery and credential theft because users still fall prey to familiar spam tactics, according to the *Cisco 2015 Annual Security Report*.

One of the latest methods is "snowshoe" spam, so named because much like a snowshoe, which leaves a large but faint footprint, the attacker spreads a lot of small messages across a large area to avoid detection by traditional defenses. Snowshoe spammers rapidly change body text, links, and the IP addresses used for sending spam, and never repeat the same combination. The possibilities are seemingly endless. These various types of attacks are successful because they are well disguised, blend different techniques, and constantly evolve.

Although there is no such thing as 100 percent protection from spam and viruses, organizations can reach a catch rate higher than 99 percent by layering and integrating multiple antispam engines and multiple antivirus engines. A security architecture that tightly integrates multiple engines and allows them to work together automatically and transparently not only increases protection levels but also reduces false-positive rates, as they serve as a check and balance against each other.

In addition, filters that look at the reputation of the sender's IP address can help protect against attacks like snowshoe spam that hijacks IP address ranges.

Requirement 4: Protects Sensitive Data and Prevents It from Leaving the Organization

Research by Cisco Talos suggests that organizations may not be able to prevent all malware from infiltrating their networks. However, modern email security solutions can help reduce the chance that critical data will leave the network either by accident or by design.

Organizations need the ability to detect, block, and manage risks in outbound email. Solutions with content-aware, policy-based data loss prevention (DLP) and encryption capabilities can offer that protection. Outbound antispam and antivirus scanning, along with outbound rate limiting, helps organizations keep compromised machines or accounts from ending up on email blacklists.

Requirement 5: Addresses New Attack Vectors as They Emerge

Preventing data from leaving the network and ending up in the hands of unauthorized users also requires organizations to know at all times which users are attempting to gain access to the network, from what location, and from what type of device. This requires a highly secure mobility solution that can provide information on user identity and location, device operating system and version, and user access privileges. Next-generation firewalls can then enforce network access based on context.

Enterprises should look for email security solutions that offer flexible deployment options that encompass physical appliances, virtual appliances, the cloud, and hybrid offerings. In addition, solutions should be able to scale from hundreds to thousands of users with little disruption. Highly distributed organizations with an expanding base of mobile workers particularly need to extend content and data security to all users as quickly as business needs require, while also making good use of existing infrastructure and IT resources.

Why Cisco?

To protect their data, networks, and users, today's organizations need a threat-centric email security model. They must be able to address the full attack continuum across all attack vectors and to respond at any time, all the time, in a continuous fashion—before, during, and after an attack. With Cisco email security, organizations can monitor and control data flowing into and out of the enterprise. Advanced threat defense from Cisco starts with the work of Talos. Composed of leading threat researchers, Talos is the primary team that contributes threat information to the Cisco Collective Security Intelligence (CSI) ecosystem, which includes Cisco Threat Response, Intelligence, and Development (TRIAD); Cisco Managed Threat Defense; and Security Intelligence Operations. Cisco CSI is shared across multiple security solutions and provides industry-leading security protections and efficacy.

Talos calls on an unrivaled telemetry data set of billions of web requests and emails, millions of malware samples, open-source data sets, and millions of network intrusions to create intelligence that provides a holistic understanding of threats. This capability translates to the industry-leading effectiveness of Cisco security solutions. Our security intelligence cloud produces "big intelligence" and reputation analysis for tracking threats across networks, endpoints, mobile devices, virtual systems, web, and email.

Antispam Defenses

Cisco provides a multilayered antispam approach for comprehensive protection. Cisco combines the outer layer of filtering based on sender reputation and an inner layer of filtering that performs a deep analysis of each message for a defense that stops spam from reaching company inboxes. The emails that pass through reputation filtering are scanned with the unique Cisco Context Adaptive Scanning Engine (CASE), which reviews sender reputation; examines the complete context of a message, not just the content; filters the URL within a message body; and filters more accurately than traditional spam-screening techniques. CASE provides a catch rate greater than 99 percent and a false-positive rate less than 1 in 1 million.

Outbreak Filters

Protect your email with a zero-hour antivirus solution that defends against brand-new viruses. Outbreak filters defend an average of 13 hours ahead of traditional reactive antivirus solutions. The Cisco Threat Operations Center (TOC) analyzes Talos threat intelligence data and issues rules to quarantine suspicious messages worldwide. It can issue rules on any combination of six parameters, including file type, file name, file size, and URLs in a message. Blended threats are addressed as outbreak filters rewrite URLs linked in suspicious messages.

Cisco Advanced Malware Protection

Cisco AMP integrated capability spans Cisco FirePOWER™ network security appliances, endpoint protection for PCs, Cisco email security, Cisco web security, and mobile and virtual systems. It offers flexible deployment options and extensive coverage to close ever-expanding attack vectors.

DLP and Encryption

Prevent leaks, enforce compliance, and protect your brand with Cisco email security DLP, featuring integration with RSA Security. Remediation choices include encryption, adding footers and disclaimers, adding blind carbon copies (BCCs), notifying, quarantining, and more. They can be applied in different ways depending on the severity of the policy violation. Cisco email security provides control over content, even after messages have been sent. With Cisco email encryption, senders don't fear mistyped recipient addresses, mistakes in content, or time-sensitive, emails because the sender always has the option to lock the message.

Conclusion

Robust email security solutions, like those from Cisco, are a core component of a modern security strategy because they rely on real-time intelligence; provide precise access control; and are content, context, and threat aware. With Cisco email security solutions, you are protected across the entire attack continuum.

Cisco service offerings are available to help you assess and deploy your security solution quickly and cost-effectively. Our portfolio includes professional and technical support services as well as assistance in planning, design, and implementation.

For More Information

For more information on Cisco email security solutions, visit our email security page.