White Paper

Content Security: Protect Your Network with Five Must-Haves

What You Will Learn

The continually evolving threat landscape is what makes the “discovery” of threats more relevant than “defense” as a modern approach to content 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. The content security solutions they rely on must therefore have the capability to:

1. Provide protection across the attack continuum: before, during, and after an attack
2. Stay ahead of the evolving threat landscape
3. Protect sensitive data—and prevent it from leaving the organization
4. Reduce risk through strong controls
5. Address new attack vectors as they emerge

Challenges

Content security has never been more challenging for organizations in an era where the theft or compromise of data is often the primary incentive for an attack. According to the *Cisco 2014 Annual Security Report*, “Data is the prize most adversaries want to reach through their campaigns because it is essentially currency…whether it’s a major corporation’s intellectual property or an individual’s healthcare data—it is desirable and, therefore, at risk.”[1]

Adding to the challenge are changing business models—from cloud computing and virtualization to mobile working and the bring-your-own-device (BYOD) trend. These models are extending the network and making it more porous, moving more and more data outside enterprise control and creating more vectors for attack. Meanwhile, nonintegrated point solutions and multiple management platforms intended to enhance security only create more gaps that adversaries can use to launch targeted malware that can modify its behavior and evade detection.

Hacking is now industrialized, and targeted campaigns 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.

Clearly, hackers are benefiting from the expanded attack surface: Cisco Security Intelligence Operations (SIO) researchers report that malicious traffic is visible on 100 percent of corporate networks, which means all organizations should assume they’ve been hacked.[2]

[1] Cisco 2014 Annual Security Report.
[2] Ibid.

Must-Have 1: Protection across the attack continuum: Before, during, and after an attack

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. According to the *Cisco 2014 Annual Security Report*, "All organizations should assume they've been hacked, or at least agree that it's not a question of if they will be targeted for an attack, but when…and for how long."[3]

Organizations must be prepared to address a broad range of attack vectors with solutions that operate everywhere a threat can manifest itself—on the network, on endpoints, from mobile devices, and in virtual environments. Today's content security solutions provide continuous monitoring and analysis across the extended network, so enterprises have a 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.

Must-Have 2: The capability to stay ahead of the evolving threat landscape

Threats operate in real time. To make informed decisions about security, organizations need to have access to threat intelligence that is gathered from all potential attack vectors, correlated in the cloud, and delivered in real time—and in the right context. This requires the use of big data analytics that can aggregate data and events across the extended network to provide visibility even after a file has moved into the network or between endpoints.

Content security solutions that offer industry-leading web reputation and zero-day threat intelligence can stop threats before they enter the network. Real-time threat intelligence and file reputation data are also required to identify and address attacks already under way—before they have a chance to spread. With file retrospection and alerting capabilities, security teams can identify malicious files that pose a threat and gain visibility into which users on their network may have been infected and when.

And while many threat defense and antimalware solutions on the market focus on catching threats by tagging and identifying each exploit's method of attack, this approach simply cannot keep pace with today's rapidly emerging threats. Instead, organizations should look for content security solutions that focus not on the method of attack but on the symptoms of an infection. How the threat got in is becoming less important than finding it and containing it before it spreads.

Must-Have 3: The capability to protect sensitive data—and to prevent it from leaving the organization

Can we protect sensitive data? Cisco SIO research suggests that organizations may not be able to prevent all malware from infiltrating their networks. However, modern content security solutions can help reduce the chance of critical data leaving the network either by accident or by design. Enterprises need solutions that can scan all inbound and outbound web traffic in real time for both new and known malware, and that use dynamic reputation and behavior-based analysis to analyze every piece of web content that is accessed.

Organizations also need the ability to detect, block, and manage risks in both inbound and 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 blacklist solutions.

[3] Ibid.

Must-Have 4: Reduced risk through robust controls

Content security solutions that can be managed through a single appliance enhance threat protection by providing a comprehensive view of an organization's security operations. Centralized management reporting functions for content security also ease the burden on IT personnel while enabling the consistent enforcement of acceptable-use policies and compliance policies.

Today's organizations need advanced control over dynamic web content and applications for all users regardless of location. As they expand their use of the web for competitive advantage, organizations also increase their exposure to tangible risks that can undermine data security. Some of the most sophisticated web-based threats are designed to hide in plain sight on legitimate and well-trafficked websites and serve up data-stealing malware to unsuspecting users. However, blocking websites is not practical or realistic in today's Web 2.0 world—but blocking features is.

Content security solutions that offer web application visibility and control help administrators to create and enforce detailed policies within websites that contain embedded applications—without hindering workforce productivity or burdening IT resources. This helps organizations to reduce their exposure to web-based malware and to prevent data loss.

Sophisticated content security solutions will not only identify applications but also identify and categorize microapplications, so administrators can easily allow or deny access to the relevant parts of an application. For instance, microapplications on Facebook can be categorized into business, community, education, entertainment, games, and so on. Similarly, applications like Google+, LinkedIn, Twitter, and iTunes can be broken down into microapplications.

Enterprises also need content security solutions that help enable them to control application behavior—what action a user is taking within an application. As an example, a videos category can identify whether a user is uploading, tagging, or posting a video. An administrator can then set a precise control for this category, allowing users to view and tag videos but not to upload a video.

Must-Have 5: Capability to address 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 content security solutions that offer flexible deployment options that encompass physical appliances, virtual appliances, cloud, and connectors. 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 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 attack. Robust content security solutions, like those from Cisco, are a core component of a modern content security strategy because they rely on real-time intelligence, provide precise access control, and are content-, context-, and threat-aware.

With Cisco® Web Security and Cisco Email Security, organizations can monitor and control data flowing into and out of the enterprise. These solutions detect and block threats using cloud-based intelligence from Cisco SIO, the world's largest cloud-based security ecosystem. Cisco SIO has visibility into more than a third of global Internet traffic. Cisco correlates intelligence in the cloud from more than 100 terabits of daily security intelligence derived from live data feeds from more than 1.6 million deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions.

Organizations that use Cisco Cloud Web Security can further enhance their threat-detection capabilities with Cisco Cognitive Threat Analytics, a cloud-based solution that reduces time to discovery of threats operating inside the network. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection.

Cisco AnyConnect® VPN technology provides information on user identity and location, device operating system and version, and user access privileges that help enable Cisco's next-generation firewall solutions to enforce network access based on context. Cisco AnyConnect is the most widely used VPN, as well as the most mature and comprehensive secure mobility client in the market today.

Cisco Advanced Malware Protection (AMP) combines the cloud security intelligence of Cisco and Sourcefire (now part of Cisco). Cisco AMP's integrated capability spans 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.

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

With these content security solutions from Cisco, organizations can gain a visibility-driven and threat-focused approach to security—and layered protection across the attack continuum.

- **Before:** Cisco SIO delivers web reputation and zero-day threat intelligence to prevent threats from entering the network.
- **During:** Threats are identified during an attack through file reputation and file sandboxing.
- **After:** Retrospective analysis provides protection in cases where advanced malware has slipped past other layers of defense.

For more information on Cisco's content security solutions, visit the links below:

- Email Security
- Web Security

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA CC11-731831-00 05/14