IDC TECHNOLOGY SPOTLIGHT

Web Security: Essential Component of Threat-Centric Defense Strategy

September 2015

Adapted from *Security in the 3rd Platform: Marching Toward Proactive Defense* by Christian A. Christiansen and Robert Westervelt, IDC #255791

Sponsored by Cisco Systems

Web-borne attacks remain the prevailing pathway criminals take to gain access to sensitive corporate resources. Attackers are getting smarter about covering their tracks, carrying out multidimensional attacks that combine time-tested techniques with evasion mechanisms and encrypted communication to thwart traditional security solutions, according to forensics investigators who have taken part in many of the latest breach investigations. The transition to SaaS-based services and an ever-increasing mobile workforce that demands unrestrained access to corporate resources have resulted in the excruciatingly difficult task of mitigating the increased risks. Attackers are seizing on system complexity and the continued expansion of the network, which has eroded IT security's ability to maintain situational awareness — something that is central to identifying and containing threats before data is stolen. It's clear that organizations must increase their security effectiveness given the continued sophistication of malware designed to evade traditional security defenses and well-funded targeted attacks designed to maintain persistent presence on corporate networks. Most organizations have already invested heavily in building out and maintaining their security infrastructure; the good news is that there is room to gain more value out of existing security investments by creating more cohesiveness. Organizations can get more value out of their Web security defenses when combined with a unified security architecture that bridges the communication gaps that have long existed between endpoint and networking security solutions. Leveraging the threat intelligence gleaned from Web security platforms, a network security backbone, combined with security technologies that conduct threat analysis and automated response, can help boost the effectiveness of security operations and significantly reduce risk where it matters most. This paper explores how Web security plays a key role in defending against evolving threats and highlights how Web security fits into a unified security architecture and how Cisco Systems' threat-centric approach can be applied to address dangerous Web threats.

Introduction

Endpoint security and the Web security defenses protecting the endpoint are on the front lines in the battle against malware and targeted attacks attempting to gain access to corporate resources. Web security technologies are adapting to the growing use of cloud services and the explosion of mobile devices, which together have created a perimeter that is becoming more malleable every day. That digital fluidity is under attack by organized criminals in Eastern Europe, Russia, and China who are taking advantage of the growing complexity and strained security defenses.

These attackers seek account credentials, credit card data, healthcare information, and intellectual property. The stolen data enters the backbone of their operation, a place where organized cybercriminals have spared no expense to modernize their business operations. Criminal enterprises use integrated systems to support business intelligence and analytics to quickly examine, sort, and bundle the data. The goal is to fetch the highest price in underground hacking markets.

These criminals know that employees are seeking flexibility and portability and use cloud services that blur the line between personal data and workplace data. Meanwhile, open platforms are fostering collaboration among internal teams, business partners, and other external contractors. While IT teams are forced to embrace this growing hodgepodge of interconnected services and devices, criminals are mining social media to create clever social engineering attacks that feed their phishing campaigns. As organizations shed the rigid on-premises applications of the past to achieve productivity gains, IT teams are left struggling to ensure risk mitigation measures are in place and effective.

This strain on endpoint security requires a modern approach to risk mitigation supported by the creation of a unified defense strategy. The new approach combines network security infrastructure and endpoint security components to create agile defenses capable of sharing threat data to heighten situational awareness.

Overwhelming Delivery of Attacks via the Web

Attackers have their modernized back-end systems, but they continue to take advantage of time-tested attack techniques. A treasure trove of Web site vulnerabilities, weaknesses in content management systems, and flaws in Web browsers and browser components provide a low barrier of entry to the corporate network. The litany of high-profile data breaches continues because stealing account credentials and other personally identifiable data has a cascading effect on corporate security incidents. Attackers gain advantage using a combination of vulnerabilities, configuration weaknesses, and human fallibility. However, another factor is the siloed security systems that defend corporate resources but remain isolated from the rest of the security infrastructure.

Meanwhile, security researchers have gained increased visibility into the constantly evolving threat landscape. Targeted attacks fueled by corporate espionage and state-sponsored activity are also often delivered via the Web. These attackers use tactics similar to those of financially motivated criminals, but their campaigns often consist of multiple stages and combine zero-day exploits and sophisticated malware that evade traditional defenses. The resources behind many of these attacks support reconnaissance activity and the ability to identify the best way to stealthily gain access to the network and maintain persistence for extended periods of time, leveraging hidden backdoor access to the victim organization. IDC surveys consistently found victim organizations were breached for weeks and months before law enforcement, a business partner, or customers informed the company of a problem.

There are countless examples of attacker sophistication associated with high-profile breaches. Some of the latest threats that are cause for concern are as follows:

- **Ransomware:** CryptoLocker, which was designed to encrypt system data and hold victims ransom by extorting a fee for the decryption key, reaped millions of dollars from individuals and businesses in just a few short months. Copycat ransomware continues to be detected and can spread through a drive-by attack, links shared on social media sites, or malicious files hosted on popular SaaS services. This threat has raised awareness of the need for modern Web security defenses, a secure backup mechanism, and a unified security infrastructure.
- **Banking malware:** Despite efforts by the financial industry to eradicate the notorious Zeus banking trojan family, the threat continues to be a problem to end users and businesses. Zeus is often seen as a consumer problem, stealing account credentials and draining the bank accounts of its victims. Recent law enforcement action highlighted the costly damage to businesses. Criminals took advantage of workers infected by the banking malware delivered via hijacked advertising networks, draining corporate accounts in days. Meanwhile, legitimate sites are becoming staging grounds for drive-by attacks, raising the risk of more employee infections by malware. Businesses are at risk if privileged users aren't protected by Web security solutions and other controls.

Web Security: A Key Component of a Unified Security Architecture

As control of and visibility into corporate assets erode, much more attention is being paid to bridging the siloed security systems and creating a unified security infrastructure supported by a network security backbone. Security is being built into network infrastructure to support user authentication, manage privileged access, and extend policies and enforcement mechanisms across the distributed network.

Web security products protect against both inbound malware threats and outbound data leakage threats and are increasingly tapped by other security components to leverage their threat intelligence data for better situational awareness. The underlying security functions remain the same, but the components are now increasingly able to communicate threat intelligence data. This interoperability results in the ability to automate the process of calibrating the security posture to changing threat conditions. Network, Web, and messaging security continue to address the common weak points targeted by attackers, but they can now fine-tune their detection mechanisms. This additional situational awareness enables identity, authentication, and authorization products to be extended to cloud-based services to bolster the user experience by tying together multiple services with single sign-on. SaaS-based services that contain sensitive data can be further protected with multifactor authentication, SaaS-based intrusion prevention, or file integrity monitoring capabilities. In some cases, encryption and tokenization are being offered with data loss prevention capabilities.

This transition to a unified defense is evolving to a strong centralized command-and-control point connected to decentralized sensors and policy enforcement points. The network is the support beam behind the threat-centric security model:

- The underlying network infrastructure must be open to support accessing and using global intelligence feeds and data from disparate security systems to identify vulnerabilities and address them across the distributed environment.
    - Web security solutions increasingly provide threat intelligence data to security information event management systems and other monitoring solutions to provide situational awareness and identify threats by correlating events that were once isolated. They are also capable of feeding data into next-generation security analytics that leverage big data projects.
- The underlying network infrastructure must be capable of enabling bidirectional communication to protect myriad endpoints and the data repositories they use. Network infrastructure should support multiple deployment models — physical, virtual, cloud, or services — to address the distributed nature of the corporate network.
    - Traditional on-premises secure Web gateways are increasingly being coupled with SaaS Web security components to extend protection to branch offices and mobile workers. SaaS enablement accelerates the time in which organizations can add new features and vendors can update protection mechanisms.
- The underlying network infrastructure must support data analytics and integrate with emerging specialized threat analysis and protection products. These emerging products are designed to identify advanced threats by leveraging data from external and internal sources and often by bridging the divide between Web, email, and network security.
    - Web security should be able to integrate with SaaS-based and on-premises virtual and/or emulation sandboxes for suspicious file analysis, mechanisms for robust network traffic inspection, and security analytics that support incident response with required context.

- The underlying network infrastructure must pull together fragmented security solutions to support security operations and accelerate incident response.
    - Web security platforms that support incident responders by providing additional context about infections and augment remediation efforts by supporting automated quarantining and removal are increasingly in demand.

Once embraced, this threat-centric model supports modern security systems by helping them capture a baseline of endpoint and network activity. The network infrastructure serves as the nerve center that raises and lowers the security posture when threats are identified to prevent a similar attack on another part of the extended network and to help protect against future attacks.

Growing Cisco Security Portfolio Supports Unified Security Architecture

Cisco's $2.7 billion acquisition of Sourcefire in 2013 catapulted the networking giant as a modern player in the security market, but it was only the first step in supporting a unified defense strategy. Sourcefire's advanced threat protection, endpoint visibility and control, and incorporated cloud threat intelligence support Cisco's portfolio. Cisco quickly executed on integrating Sourcefire's components. Sourcefire's Advanced Malware Protection (AMP) technology was added into Cisco's email and Web security appliances and Cloud Web Security Service. Cisco pledged to continue to foster Sourcefire's open source roots and extend the FirePower network security appliance line.

Sourcefire also added contextual awareness and protection to Cisco's portfolio, and its FirePower services were further extended to Cisco's ASA UTM appliances. The increased endpoint visibility gleaned from AMP with Web security detection and prevention helps fuel the accuracy of the fully integrated solution.

The acquisition of ThreatGRID further built out Cisco's ability to support a unified defense strategy by incorporating advanced malware analysis with threat analytics and content in an on-premises appliance or cloud-based SaaS offering. The pieces work together to aggregate and correlate data across the extended network. Further building on Cisco's strategy is the company's recent acquisition of OpenDNS, which could be used to further support Cisco's Web security offerings by leveraging the core DNS security technology and OpenDNS' broad customer base for even deeper threat intelligence.

The acquisitions also bolstered the Cisco Security Technical Alliance program, establishing a healthy ecosystem of technology partners willing to embrace Cisco's threat-centric model. A core part of establishing a unified defense strategy is extending consistent policies across the distributed network. Cisco's Identity Services Engine (ISE) is a modern platform that acts as the access policy broker for employee and guest access to corporate resources. It uses Cisco's Platform Exchange Grid (pxGrid) technology to share contextual data with integrated partner ecosystem solutions. This technology bridges isolated solutions into a cohesive security architecture.

Cisco Threat-Focused Web Protection

Cisco's offerings include IronPort-branded Web security gateway appliances and Cisco Cloud Web Security, an SaaS solution. An on-premises/cloud configuration is also available for Cisco Web Security Appliance/Service deployments via a hybrid licensing offering.

Cisco added the AMP capabilities to its Web Security, Cloud Web Security, and Email Security gateways. The integration adds file reputation functionality, file analysis sandboxing via Cisco's ThreatGRID acquisition, and a feature called "file retrospection" to identify malicious files that are designed to appear benign to antimalware inspection engines but are programmed to become malicious at a later time. The features require an additional license.

Support for ISE was recently added to extend policies and controls to third-party partner solutions and other Cisco products that make up the Cisco security architecture. The integration enables ISE to collect threat information from the gateway.

Cisco was one of the first vendors with a SaaS-based Web security offering as a result of its acquisition of ScanSafe in 2009. The ScanSafe service is now called Cisco Cloud Web Security, and it currently has more than 10,000 users. Cisco integrated Cognitive threat analytics to identify threats more quickly in the Cloud Web Security offering. Cisco partners with Elastica for ShadowIT and extending policies to popular SaaS applications.

Challenges

The security industry must adapt quickly to emerging threats while reducing risks associated with the changing behaviors of employees. The challenge is in enabling customers to leverage their existing security investments in adopting a unified defense strategy. The opportunity for Cisco is in its overarching strategy, which provides the tools to bridge those siloed security solutions using the network infrastructure as the nerve center of the cohesive security architecture.

Cisco's Web security offerings often are overshadowed by the company's vast network infrastructure portfolio, which can obscure the benefits provided by Cisco's approach in connecting its Web security products with its AMP and ISE capabilities.

As a networking infrastructure giant, Cisco is viewed as a solution for large enterprises, and this misconception causes small and midsize businesses to look elsewhere for security offerings. The company has a strong base of reseller partners with managed services capabilities and SaaS deployment expertise that can help break this fallacy. These partners can help guide midmarket organizations through the deployment offerings and properly configure a Web security deployment.

Cisco faces further integration with its portfolio, including bridging reporting capabilities for organizations extending their Web Security Appliance deployment with its cloud offering and its OpenDNS acquisition. Plans are in the works to address this integration, and until then, the company is nurturing its strong technology partner ecosystem to address any pain points.

Essential Guidance

Web security will continue to be the entry point of most attacks. The following measures could enable any organization to begin building the bridges necessary for a unified defense:

- **Assess risk:** Thoroughly analyze existing security investments before rationalizing the purchase of emerging technologies. Consider ways to gain more value from existing security investments. Identify and evaluate technologies designed to bridge communication gaps in existing security solutions.
- **Increase visibility:** Real-time content and security scanning is an essential part of Web security protection. Be more proactive about generating reports to gain visibility into which users and groups consistently generate the most risk. Assess the security infrastructure protecting the organization's key assets. Identify the at-risk employees with privileges to those key assets, and address the security policies and enforcement mechanisms that mitigate the increased risk posed by those employees.
- **Monitor proactively:** Move from highly fragmented and poorly implemented defenses to predictive protection. This includes evaluating the usefulness of threat intelligence and contextual awareness gleaned from existing monitoring solutions deployed on the network.

- **Examine response:** Identify process and technology gaps that hinder incident response and remediation from silicon to cloud. Give incident responders the right tools to efficiently carry out remediation activities. Review recent incidents and address process breakdowns. Consider improvements that extend existing policies and automate response as much as possible to give IT security time to address the most critical issues.

Conclusion

IDC believes that increased pressures on enterprise security groups will continue to drive the requirement for more automation within a cohesive security architecture. Security infrastructure must have components capable of sharing threat data and using it to conform to situational security posture changes. With large-scale attacks occurring and the incessant pace of high-profile data breaches, it is clear that all companies need to be more prepared to deal with these attacks. IT is a necessary component of doing good business, and IT security remains at the top of the IT department's spending list.

A unified defense posture can provide increased visibility and enough context behind alerts for incident responders. There has been an emphasis on solutions that can bridge endpoint, mobile, and network visibility, linking them to an on-premises or cloud-based analysis engine capable of providing responders with the most relevant and actionable information. Networking vendors are adding endpoint security technologies to gain visibility and bolster the effectiveness of network defenses. Web security is one of the key endpoint components that can provide the necessary context to better protect end users. Web is often the first line of defense against attacks. It is increasingly being extended through SaaS and on-premises deployments to protect workers regardless of their location or the devices they are using.

IDC believes that Cisco's Web security offerings and growing security portfolio offer customers compelling options. As a historical leader in network security, Cisco has continued to embed security into its networking components and is continuing to grow its security technology partner ecosystem. Cisco has also bolstered its Web security and threat intelligence capabilities with the acquisition of OpenDNS. It is creating the necessary cohesiveness to support a unified security strategy with the network infrastructure as the nerve center that bridges all the key components. If Cisco can address the challenges highlighted in this paper, IDC believes the company has a significant opportunity for success.
