SearchSecurity

TechTarget

E-Guide

Exploring New Web Browser Security Capabilities

Since the introduction of Secure Web Gateway (SWG), the threats facing companies have continually grown and become more sophisticated. Luckily, new security features built into popular browsers are making it harder than ever for cybercriminals to strike. Read this expert E-Guide to explore new security capabilities and how they are making attacks more difficult.

Contents

Exploring New Features, Uses for Secure Web Gateway Appliances

By: Michael Cobb, Application Security

Originally, an enterprise would implement a secure Web gateway (SWG) appliance to enforce corporate policy (e.g., preventing employees from visiting YouTube during office hours). Back in 2008, as enterprises realized they couldn't rely solely on a firewall, antivirus, and simple URL filtering to prevent zero-day attacks, SWGs were viewed as the best way of integrating features provided at that time by various single-purpose devices -- such as URL filtering and bandwidth throttling -- into one appliance. Web application-level controls and centralized management were also big selling points, plus non-signature-based detection and filtering were beginning to appear.

With the threats facing enterprises changing so much since the introduction of SWGs, though, enterprises must reconsider what new features and functions are now included with SWGs and which features are the most important when picking a potential implementation. A continually growing and increasingly sophisticated attacker base, combined with the emergence of more diverse endpoints, mobility and BYOD, have all forced SWG technology to evolve rapidly to meet the needs of the modern enterprise.

In this article, we will reexamine what enterprises should expect from secure Web gateways in light of the technology's evolution, plus the differences between cloud-based and on-premises SWG appliance deployments.

Secure Web gateway features

To maximize the benefits contemporary SWGs provide, an enterprise must understand its requirements and the pros and cons of an on-premises, cloud-based or hybrid SWG deployment.

Any organization assessing secure Web gateway options should now expect to find a wide range of functions and features available, including:

- URL filtering
- HTTPS scanning
- Malware detection, both inbound and outbound
- Threat intelligence feeds
- Mobile support
- Application control
- Data loss prevention (DLP)
- Threat and traffic visualization

Due to the rapidly changing nature of the threat landscape, enterprises should note that differences abound in the quality of controls such as URL filtering, malware detection and support for DLP. For example, filtering and detection technology has advanced significantly in recent years. To solve the problem of outdated blacklists, SWGs now rely on multiple types of analytics, including reputation analysis, real-time browser code scanning, behavioral analysis, content control and data fingerprinting.

Another noticeable advance in modern SWGs is the increased flexibility and granularity administrators have in controlling Web, email and data traffic. Individual elements within a dynamic Web page can be analyzed and blocked, as can access to specific services at particular times of the day or when activity reaches a predefined threshold. Bandwidth utilization parameters can be specified for uplink and downlink traffic by content category. They can also be adjusted depending on specific access requirements for different users and groups.

To keep devices updated with the latest threat and attack information, many secure Web gateway products incorporate threat intelligence feeds from cloud-based services. DLP support is growing for a variety of mobile devices, which is vital for any enterprise that supports BYOD. By combining security classifications with custom data sets, context-aware data loss prevention is also improving. Many SWGs also support "call home" detection, or alerting on malware that seeks out remote instructions, to help cover any blind spots.

Visualization might seem like a gimmicky feature, but it enables administrators to easily see hotspots on the network that need further attention. For example, visualization of captured traffic can quickly highlight infected devices probing network neighbors looking for vulnerabilities to exploit. Also, administrators can observe information such as bandwidth utilization or sites visited in real-time, which provides better visual insight into how a network is being used and how rule changes affect productivity and security. This makes implementing complex rules that perform as intended much easier.

Secure Web gateway deployment trends

In terms of how secure Web gateways are being deployed, the most recent Secure Web Gateway Magic Quadrant 2012 from research firm Gartner Inc. indicated that on-premises enterprise-grade appliances still dominate the market, but the cloud-based SWG-as-a-Service segment is growing quickly. There are also hybrid deployments available that combine on-premises and cloud-based SWG elements.

To maximize the benefits contemporary SWGs provide, an enterprise must understand its requirements and the pros and cons of an on-premises, cloud-based or hybrid SWG deployment. With cloud-based services, an enterprise can apply the same protection and policies to all users regardless of location, but the enterprise must select an SWG that will integrate with its existing infrastructure. With an on-premises SWG, a proxy architecture must be used so that all Web-bound traffic is processed. By forcing all Web traffic to terminate at the proxy, the gateway can ensure no traffic flows to or from the Internet without inspection or control. Alternative SWG deployments, such as TAP deployments, have the gateway observing traffic as it passes by because it's sitting off to the side of the network. If the gateway doesn't detect the threat in time because the traffic isn't being intercepted as an inline appliance would, malware or other threats can slip onto the network unnoticed. This method might be fine for enforcing organizational policy, but it's definitely not a reliable safeguard against Web-borne threats.

Finally, as with most Web security technology, the marketing materials for secure Web gateway products are full of superlative blurbs, such as *unique*, *the best* and *industry-leading*. Enterprises should attempt to ignore these largely baseless claims when assessing how a certain device can best meet organizational requirements. Instead, narrow down a list of finalists on how well each product measures up against a pre-defined list of must-have features, and then use price, performance testing and advice from other customers to guide the final decision.

There's no question secure Web gateway technology has evolved considerably in recent years with many impressive new capabilities, but advancement alone is no guarantee of success. A careful, thoughtful review of what today's products can do and how they match up against an enterprise's needs is an essential precursor to secure Web gateway success.

About the author:
Michael Cobb, CISSP-ISSAP, is a renowned security author with more than 15 years of experience in the IT industry and another 16 years of experience in finance. He is the founder and managing director of Cobweb Applications Ltd., a consultancy that helps companies to secure their networks and websites, and also helps them achieve ISO 27001 certification. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. Michael is also a Microsoft Certified Database Administrator and a Microsoft Certified Professional.

Web Browser Security Features Make Attacks Harder

By: Robert Westervelt, News Director

Security capabilities built into popular browsers are making it more difficult than ever for cybercriminals to carry out attacks using browser vulnerabilities, according to security experts. While the security improvements don’t make browsers bulletproof, recent hacking contests demonstrate the overall enhanced state of browser security.

Microsoft, Mozilla and Google have all been developing support for substantial security capabilities in recent years that isolate critical components and help prevent attackers from using the browser as a stepping stone to a more substantial attack, says Chris Valasek, senior research scientist at Accuvant Labs.

“It’s accepted that users will click on links and browsers will be exploited, but if you have something to contain the attack you are going to be much better off,” Valasek says. “As long as there are smart attackers out there with time on their hands they’re going to take vulnerabilities and create something to exploit them, but we’re seeing that it’s taking more time and more effort.”

At RSA Conference 2012, Valasek and his team, which includes researchers Joshua Drake and Paul Mehta, talked about Web browser security features and the results of their browser security analysis of Mozilla Firefox, Microsoft Internet Explorer and Google Chrome. The analysis found all three browsers contain capabilities that make an attacker’s job much harder. The Accuvant Labs researchers praised Google’s implementation of sandboxing in Chrome for making it an extremely difficult browser to crack. Sandbox technology – also implemented in Internet Explorer – is intended to contain certain actions, such as code execution.

“While not perfect, sandboxes do provide a huge barrier of entry of any persistence on anyone’s machine,” Valasek says. “It might make an attacker look for lower hanging fruit.”

Both IE and Chrome also support JIT hardening, a function that reduces the impact of vulnerabilities in other software. The browser JIT engine is among the favorite targets of attackers.

All three browsers use address space layout randomization (ASLR) and data execution prevention (DEP), technologies designed to prevent an attacker from using well-known locations to begin exploitation and from exploiting

Contents

code in certain regions of memory. The browsers also contain a stack cookies function, which is designed to prevent stack-based buffer overflows, a common component to a successful attack.

“We can beat up on Firefox or Internet Explorer and even Chrome, but all of these browsers improved drastically since where they were at four years ago,” Drake says.

However, as with any security technology, there is no silver bullet, he adds. All of the security features contain weaknesses that can be exploited by a skilled attacker. Still, the increasingly difficult nature of carrying out an attack targeting the browser vulnerability was put on display in March at the CanSecWest security conference in Vancouver BC, where Google and HP TippingPoint held their annual browser busting contests. While several winners were crowned, the contestants reportedly admitted that it took long hours to string together an attack scenario that enabled them to break out of the browser and onto the machine.

A team of researchers from VUPEN Security strung together multiple vulnerabilities in a complex exploit to garner $60,000 from Google. Other white hat hackers in the contest failed to pull off a complete attack. This year’s contest stood in stark contrast to years past when multiple security researchers took mere minutes to demonstrate a vulnerability and compete a successful browser attack.

For the Pwn2Own contest run by HP’s TippingPoint Zero Day Initiative, the research team from VUPEN demonstrated a successful attack against Chrome and Internet Explorer, while independent researchers Vincenzo Iozzo and Willem Pinckaers teamed up to successfully exploit a Firefox zero-day flaw.

Despite the improvements in browser security, spear phishing and other email attacks targeting browser vulnerabilities and browser components like Adobe Flash and other plugins, are almost constant and a serious problem for enterprises says Anup Gosh, founder and chief technology officer of hardened-browser maker Invincea. Gosh, who received funding from DARPA to create a virtual sandbox browser environment that supports Internet Explorer and Firefox, says a lot of organizations are still using outdated browsers with fewer security features to support custom applications.

“When you talk to people who clean up networks and the incident response guys, it’s all spear phishing right now,” Gosh says. “It’s not hard to get a user to click on a link and exploit a browser component vulnerability. The weaknesses are still there.”

About the author:
Robert Westervelt is news director of SearchSecurity.com.

TechTarget

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

- SearchCloudSecurity
- SearchSecurityChannel
- SearchFinancialSecurity
- SearchMidmarketSecurity