White Paper

Select a Secure Web Gateway

How to deploy comprehensive protection for your corporate network.

intel Security

Table of Contents

While the Internet has become a vital platform for enterprises of all sizes, it has also become a dangerous place, with exponential growth in both the number and sophistication of attacks against corporate networks. To guarantee stable, controlled, and secure access to the Internet and web applications, companies need technologies such as web gateways so that their unique online access requirements are met while protecting the enterprise against attacks. In this white paper, McAfee, a part of Intel Security, describes a wide range of Internet-based attack methods and explains how McAfee® Web Protection technology protects against them.

The Malware Avalanche

In a recently published report[1], Gartner analyst Dan Blum writes, "The web is indispensable for most organizations, but it's become a dangerous environment. Organizations require tools to protect their users, endpoints, and information from risks."

The danger Blum refers to comes from the explosive growth in cyberattacks against organizations of all sizes and in all industry sectors. Regardless of size, any organization with data that's profitable for attackers to obtain (financial services with banking and/or brokerage accounts, intellectual property, and personally identifiable information that can be used for identity theft) is at risk.

McAfee Labs has tracked the growth in attacks for more than a decade, and the numbers are daunting, both in terms of the sheer volume of attacks and their increasing sophistication. This information is shared with our customers and the industry and is available at the **McAfee Threat Center website**.

Malware types and threats

We define malware simply as malicious programs. Viruses, worms, Trojans, spyware, and rootkits are examples of malware. Potentially unwanted programs (PUPs), such as adware, are not necessarily malware, but are usually considered risky by security professionals.

Countless variations of new and existing malware are being launched constantly across the Internet. Originally, malware was distributed via email messages from bogus or stolen email accounts. Now, it's often hidden in websites or inserted into ad networks to be injected into the browser of an unsuspecting visitor. For instance, today's malware lurks in social media pages or messages, ready to infect users lured by offers from compromised or bogus Facebook or Twitter accounts. (For more information, read **The Hidden Truth Behind Shadow IT**, based on a survey conducted by McAfee and Frost & Sullivan.) Mobile devices, USB sticks, and other portable systems also carry malware into the network, where it propagates.

Different categories of malware behave in different ways, depending on their format, content, behavior, infection characteristics, and propagation techniques. Some newer, narrowly targeted malware types are heavily camouflaged, employing disguised or hidden behavior to avoid detection.

New threats have emerged that combine several forms of malware into one malicious payload. A single blended virus infection may include keyloggers to steal sensitive financial information, email, and corporate secrets while turning users' systems into a spam zombie in a botnet. Blended threats that enable botnets are a significant threat escalation because they offer cybercriminals a variety of opportunities to make money. For instance, a botnet sending spam can generate recurring revenue as part of a spam network, while simultaneously propagating viruses and stealing online banking, gaming, and social networking logins as well as the account information required for perpetrating fraud.

More recently, sophisticated cybercriminals are designing malware that can automatically evade detection, using techniques such as obfuscation or polymorphism. In many cases, these systems dynamically generate new run-time code or payloads (such as a PDF file). These techniques often make it possible to evade detection by traditional signature-based products.

Protecting the Enterprise

Given the variety and sophistication of recent theats, protecting the enterprise against external attack requires a multilayered approach that combines reputation analysis, proactive malware detection, application controls, data loss prevention, and more.

Reputation and traffic analysis

The best place to stop malware is at the network perimeter before it can reach a target platform (whether a server or endpoint system). There are a number of ways to do this. One is to analyze the origination point of the malware (for example, China or Eastern Europe) and collect information about a site's previous history and compute a reputation score. A particular site (IP address or domain) with a reputation for delivering malware, or a previously benign site which has become infected can then be blocked. Whitelisting/blacklisting, URL blocking and filtering, site categorization, and reputation scoring can all work together to accomplish the goal of preventing users from accessing sites that might be a source for malware.

Malware detection

Malware can be delivered in many formats, including Windows portable executable (PE) files, Microsoft Office macros and scripts, and JavaScript. The recent trend has been for the browser to be the primary delivery vehicle, and attacks often examine the browser (Internet Explorer, Chrome, Firefox) looking for specific vulnerabilities. Exploits also look for known vulnerabilities in Java, Adobe, Flash, or other browser plug-ins.

When a particular example of malware has been identified, a signature can be created. This signature operates like a fingerprint and can be shared with other computers in a network to rapidly identify and block that payload, protecting other systems against infection. Most endpoint antivirus software relies on signature detection, and that capability is also available with most anti-malware engines. Sharing malware signatures is the first line of defense, since it can be used to block known malware immediately. However, since not all instances of malware are known to all systems, signature testing—while necessary—is not sufficient for systemic protection.

The next level in malware detection is proactive scanning and analysis focused on the detection of previously unknown malware instances.

Proactive malware detection examines the software embedded in the downloaded packet (web page, email attachment) and uses various emulation techniques to trick the malware into thinking it has reached a target and then observe its behavior without actually running the malware. Behavioral observation can help determine whether or not the software is benign or malicious. Few of today's anti-malware solutions do a good job of this.

Sophisticated malware relies on new obfuscation techniques, such as dynamically generating runtime code that may enable it to slip past a malware detection engine. In some cases, detection of these advanced threats requires more in-depth analysis using two techniques: Sandboxing and static code analysis. A sandbox is an isolated runtime environment, which provides a platform where the payload code can run, rather than being emulated. Code analysis relies on reverse engineering the code and analyzing its origins and internal structures. Code analysis can often unveil similarities with previously analyzed malware, providing clues to how the malware operated and who wrote it. The combination of these two techniques is the most advanced technology for detecting and stopping malware. However, sandboxing and code analysis are more time-consuming than proactive malware detection and cannot be done in real time without negatively impacting the user experience.

Another technique that is being increasingly used by attackers to hide malware is to encrypt it in a web page using HTTPS. As a result, an effective malware detection tool must be able to decrypt and analyze a page before re-encrypting it and forwarding it to the client. With HTTPS traffic on the rise, this capability is becoming more essential.

Finally, not all malware is inbound. Most botnet agents will attempt to "phone home" and contact a master controller at some point in their lifecycle. They may then attempt to download additional malware or transmit sensitive information (such as a keystroke log or passwords) to the master system. A comprehensive malware detection solution must be able to differentiate between benign outreach (such as software application automatically downloading an update) and malicious outreach, and allow the former while blocking the later.

Application controls

Moving beyond malware detection and blockage, there are other capabilities that you should consider when evaluating a secure web gateway product.

Acceptable use policies are how an organization decides what websites and activities their employees are allowed to access and which websites or applications are off limits. URL filtering is one the most widely adopted technologies for enforcing acceptable use policies. However, many organizations desire a more granular method for implementing acceptable use policies that enables them to block specific application functions rather than the entire site. Through the use of application controls, employees or other users (contractors, students, or others) can be allowed access to a site, but specific capabilities are disabled. An example of this would be allowing access to LinkedIn but disabling the ability to send or receive LinkedIn messages.

Many cloud applications leverage HTTPS by default in order to enhance security. Application control enforcement is another instance where HTTPS scanning and decryption is essential, since you can't effectively apply application controls without the ability to decrypt the web page and determine if it should be controlled to comply with policy.

Data leakage

A major security concern of many organizations is how to protect sensitive or proprietary information against exfiltration. Data loss prevention (DLP) technology inspects data in motion and responds when it identifies sensitive data that is being improperly transferred, contrary to security policy settings. Responses can range from notification ("Do you really want to send these credit card numbers?") to active blocking. Detection of sensitive data relies on techniques such as data signatures, keywords stored in dictionaries, or regular expressions. Adding DLP to a secure web gateway enables the system to automatically scan and detect sensitive data and prevent inappropriate exportation of that data to an external site or application.

In today's collaborative, cloud-based environment there may be instances where you will want to share files with others using a file-sharing website such as Box, Dropbox, or Google Drive. These applications have the ability to add encryption capabilities, typically at an additional cost, but if an account with access to the file is compromised, the file will be at risk of unauthorized access. If you need to share files containing sensitive data using a file-sharing site, you should configure your secure web gateway to encrypt the file as part of the upload process. That way, anyone who attempts to access the file without going through the gateway will be unable to read it. Only authorized users who have been authenticated by the gateway will be able to retrieve and decrypt the file.

Mobile user protection

Another consideration is how to protect mobile systems such as laptops, tablets, or smartphones. When a remote or mobile user accesses a website or Software-as-a-Service (SaaS) application outside the protection of the enterprise firewall, the potential for malware exposure and compromise is significantly elevated. If the user subsequently brings an infected device into the corporate network, the result may be widespread malware infection.

To forestall this capability, you should be able to deploy a secure, tamperproof client agent on all end-user mobile devices which can determine if the device is protected by a secure web gateway and, if it isn't, redirect all web traffic requests to either a DMZ-resident or SaaS-based gateway. This ensures that all the protections provided by the gateway are applied to all inbound and outbound web traffic from the mobile device in a way that is completely transparent to the user, and that doesn't require the user to log onto a VPN. Some mobile security solutions require the user to deploy a browser-specific plug-in. However, this approach is not secure, since the user can bypass the protection by using an unsecured browser.

McAfee Web Protection

McAfee Web Protection is McAfee's web security solution. It includes both on-premises (McAfee Web Gateway) or cloud-based (McAfee SaaS Web Protection) solutions. The on-premises solution can be deployed as a dedicated appliance (with a scalable family of appliances) on a VMware virtual machine or on a blade in a blade server. Customers also have the ability to deploy a hybrid model. The hybrid deployment option gives customers the flexibility to mix-and-match on-premises and cloud-based deployments to meet specific requirements. For example, customers can use the on-premises system for controlling users at corporate headquarters and the SaaS system for managing remote users. Or, they can configure the SaaS option to deliver additional capacity.

The following are some of the main features of McAfee Web Protection.

McAfee Global Threat Intelligence

McAfee Web Protection delivers enhanced web filtering functionality and security through a combination of both reputation and category-based filtering. McAfee Global Threat Intelligence (McAfee GTI) powers McAfee Web Protection's web filtering technologies. McAfee GTI creates a profile of Internet entities—websites, DNS servers, and IP addresses—based on hundreds of different attributes gathered from the massive global data collection capabilities of McAfee Labs. It then assigns multiple reputation scores based on the security risk posed and shares this data with McAfee client systems so that administrators can apply very granular rules about what to permit or deny—and continue to monitor those entities over time. Rapid dissemination of reputation scores closes the gap between initial malware discovery and customer notification, ensuring that McAfee customers are protected against newly discovered malware as early as possible.

McAfee Gateway Anti-Malware Engine

Known malware can be blocked as soon as its signature is identified by one of the multiple signature engines available from McAfee. However, unknown (zero-day) malware is an increasingly serious problem. In fact, McAfee Labs identifies more than 100,000 unique examples of malware every day. To combat this problem, the McAfee Gateway Anti-Malware Engine conducts proactive behavioral analysis of payloads using a patent-pending technique and determines if they are safe. By scanning a web page's active content, emulating and understanding its behavior, and predicting its intent, the McAfee Gateway Anti-Malware Engine defends against zero-day attacks. Web-based traffic that passes through the gateway is subject to this analysis, including HTTP/HTTPS (SSL encrypted), FTP, instant messaging/chat, and more. The McAfee Gateway Anti-Malware Engine scans not just web content for hidden malware (HTML/HTML5 and JavaScript), but also downloaded files, such as Windows executables and Windows libraries, JavaScript, Flash, Java applets and applications, ActiveX controls, Visual Basic script and Visual Basic for applications, ZIP files, Adobe PDFs, graphics and media, Microsoft Office macros, and other types of files.

HTTPS scanning is particularly important as more websites/SaaS applications rely on encryption to secure content. Many cybercriminals use HTTPS to hide malicious content from examination. McAfee Web Gateway includes the ability to decrypt and examine these pages.

The McAfee Gateway Anti-Malware engine evaluates a suspect payload using in-line emulation to examine the code's behavior. One big advantage of this approach is that it can perform the evaluation without introducing significant latency. When the suspicious types of behavior are identified, web objects showing this behavior are blocked. Some examples include keylogger, password stealer, code execution or browser-specific exploit, code injection, obfuscated code, potentially unwanted adware or spyware, cross-site scripting, direct kernel communication, and more.

McAfee Advanced Threat Defense

To provide even deeper protection, McAfee released McAfee Advanced Threat Defense, which combines dynamic analysis using sandboxing technology with static code analysis. The sandbox uses a virtual machine to create an environment equivalent to the customer's endpoint—including operating system and specific applications, including browsers—where the payload under analysis runs. Static code analysis reverse engineers the code and examines it for patterns consistent with malicious intent. The combination of these features, in conjunction with McAfee ePolicy Orchestrator® (McAfee ePO™) software and endpoint protection solutions, enables McAfee Advanced Threat Defense to find, freeze, and fix malware that may have entered your network. Sandboxing and static code analysis are both CPU-intensive and may result in a delay before the content is delivered to the user. Therefore, McAfee recommends combining a web (or email) gateway with the sandbox, where suspicious content that is not identified by the gateway can be forwarded to the sandbox for additional, in-depth examination.

Web application controls

Popular websites such as YouTube or Facebook contain a wide variety of information, some of which may be considered inappropriate for business environments or provide little business value and therefore require controlled access. And while much of the site may be deemed inappropriate, there may be certain channels that should be accessed. A legacy web gateway solution would typically prevent access to a page or an entire site by blocking all sites in a URL category. Other solutions may apply media type filtering, such as blocking a Flash video. However, both methods do not really solve the original business problem with a policy like: "Non-business-related Flash videos on YouTube should not be viewed on the corporate network during primary business hours."

A state-of-the-art solution allows access to acceptable content while removing unwanted content, along with a clear message to the user. For example, let's say you wish to allow access to approved YouTube channels for training, but want to block other videos. The McAfee Web Protection policy engine only requires two rules to block inappropriate videos and display a message that the content has been blocked to meet business requirements.

The flexible rules-based policy engine built into McAfee Web Protection also enables application-level availability during high network loads or spikes in traffic. This can be used to guarantee that all business-critical applications are available and non-business-related traffic is deprioritized or blocked until traffic levels normalize again.

McAfee Web Protection includes more than 1,000 discrete controls for popular web applications. A complete list is available on the McAfee **Web Application Control page**.

Outbound protection
McAfee Web Protection protects outbound traffic in three ways.

It uses McAfee Data Loss Prevention (DLP) technology to protect against loss of confidential information through social networking sites, blogs, wikis, and SaaS applications. Key McAfee DLP modules, including the core DLP engine and dictionaries, monitor outbound content (using all relevant web protocols, such as HTTP/HTTPS, FTP, IM, and others) and enforce policies for information leaving the network. Upon encountering a policy violation, it can take a variety of actions, including applying encryption or blocking the data, or ensuring compliance with regulations and policies governing the privacy of sensitive information.

The McAfee Gateway Anti-Malware Engine can determine when outbound communication via the Internet may be a botnet client attempting to connect to its command-and-control home server to transmit stolen data or receive further instructions. The aggressiveness of heuristics and proactive detection is adjusted dynamically, based on whether it's a human user surfing, a background process accessing the web (such as an application downloading an update), or an unknown potential bot client.

The third way McAfee Web Gateway protects outbound traffic is through transparent file encryption. This feature encrypts files before they are uploaded to an external file-sharing site, such as Box or Dropbox. This protects the file in the event the file-sharing site is compromised by a malicious outsider who steals credentials to an account with access to the file. Without the ability to retrieve the file through the gateway, the attacker is unable to decrypt the file.

Mobile support
In an increasingly mobile world, customers are concerned that a computer may be infected by accessing the Internet from an insecure access point, such as a public Wi-Fi hotspot.

McAfee Client Proxy, a tool which is available at no extra cost for all McAfee Web Protection customers, protects laptop users working outside the corporate network. McAfee Client Proxy is location-aware and recognizes whether it is inside the corporate network, connected to it by VPN, or on an external network, such as a hotel or café hotspot. To determine location, McAfee Client Proxy attempts a TCP connect to the address of the web gateway or other network device. During the connect phase, McAfee Client Proxy initiates a test or a SYN directed to the web gateway. If the web gateway responds, McAfee Client Proxy remains passive. If there is no response, McAfee Client Proxy determines it is outside a corporate network and automatically directs web traffic to the designated McAfee web protection solution, which can either be McAfee SaaS Web Protection or McAfee Web Gateway in an Internet-accessible DMZ. The client is tamperproof, works transparently to the user, and is browser-independent.

Cloud application single sign-on
A key component of any web access security strategy is user authentication. McAfee Web Gateway includes authentication features, which can be synchronized with Microsoft Active Directory or other LDAP-enabled directories. In addition, McAfee Web Gateway includes SaaS application single sign-on (SSO) features. The SSO function includes a launch pad, where the user can click on an icon representing a target cloud application and be signed onto the application without entering another user ID or password. This feature enhances end-user convenience, improves security (by controlling or eliminating passwords), and reduces expensive help desk calls.

Hybrid flexibility
McAfee Web Protection includes licenses for on-premises, cloud-based, or hybrid configurations. On-premises options include a scalable family of appliances, which can be clustered for high availabity or configured with a load balancer for performance optimization; a VMware virtual machine; or a blade server. McAfee SaaS Web Protection, on the other hand, is a complete multitenant SaaS solution, which requires no on-premises components.

Customers can also deploy hybrid configurations, where some users use the on-premises version and others use the SaaS version. For example, a highly distributed company with many field offices can use the on-premises version for corporate office protection and the SaaS version for other offices, or a smaller business may choose the SaaS-only option to reduce the need for an operations staff. Or, as indicated earlier, a company can use the SaaS version to protect mobile user laptops that are accessing the Internet from any non-corporate location.

Security Connected

Security Connected is our vision and architecture for a comprehensive end-to-end system that protects your enterprise from the cloud to the data center to the client. McAfee Web Protection is part of this environment, which also includes the following products:

- **McAfee Advanced Threat Defense:** Finds advanced malware and zero-day threats, and seamlessly integrates with McAfee network security solutions to freeze the threat while Real Time for McAfee ePO software initiates a fix or remediation actions.
- **McAfee Endpoint Suite:** Delivers anti-malware, device control, and fundamental email and web protection in a single solution that is integrated with the McAfee ePO security management platform.
- **McAfee ePolicy Orchestrator:** The only enterprise-class software to provide unified management of endpoint, network, and data security. With end-to-end visibility and powerful automations that slash incident response times, McAfee ePO software dramatically strengthens protection and drives down the cost and complexity of managing risk and security.
- **McAfee Next Generation Firewall:** Lets you add network security capabilities when and where you need them to get maximum value out of your investment. Innovative evasion prevention, centralized management, and built-in high availability and scalability meet the complex, high-performance needs of demanding data centers and distributed enterprises, both today and tomorrow.
- **McAfee SiteAdvisor® Enterprise Software:** A web browser plug-in that allows you to surf and search the web safely, avoiding online threats such as spyware, adware, and phishing scams.

Conclusion

McAfee Web Protection is part of the Security Connected architecture that delivers the industry's leading web security solution:

- Reputation analysis, media filtering, and URL filtering.
- Inbound security protection with signature-based and zero-day malware detection and blocking.
- Outbound data protection with integrated DLP, file encryption, and botnet "phone-home" detection.
- More than 1,000 web application controls for granular acceptable-use policy enforcement.
- Built-in SSL scanning to uncover hidden malware and enforce application controls for encrypted web sessions.

For more information, or to arrange for a free McAfee Web Protection trial, visit **www.mcafee.com/webprotection**.

About McAfee

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

1. Selecting and Deploying Secure Web Gateway Solutions, Gartner, December 10, 2012

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

60940wp_secure-web-gateway_0214B_ETMG