



# McAfee SaaS Web Protection

**Cloud-based web security for a safe, secure network**

## Key Advantages

- Continuous updates protect all users, even off-network, against fast-changing and zero-day malware attacks.
- Enforces Internet usage policies and provides visibility to web usage through detailed reports by user or group.
- More than 100 content categories allow flexible content control to help protect your business against legal liability.
- Enables control over hundreds of online media types and applications, including social media sites, which can drain productivity.
- Replaces escalating on-premises capital equipment costs and staffing demands with a predictable, seamlessly scalable subscription service.
- Proven protection—McAfee SaaS Web Protection already safeguards web usage for thousands of customers and hundreds of thousands of users around the globe.

The web has opened the door to infinite business opportunities for both your business and the business of cybercrime. Each web connection provides a potential entry point for infection, malicious infiltration, and corporate risk. McAfee® SaaS Web Protection offers easy, feature-rich, vital defenses against dynamic web-based malware attacks using extensive, up-to-the-minute threat data from McAfee Global Threat Intelligence. Managed 24/7 by McAfee web and cloud security experts leveraging industry best practices, McAfee SaaS Web Protection helps you gain control over threats and undesired Internet access effectively and economically.

The dynamic content and interactivity of the web has increased the delivery of sophisticated web-borne threats that can evade detection by traditional security measures. To protect your employees, customers, network, and intellectual property, your organization needs proactive web security. That means a solution that doesn't just block known bad URLs, but also unknown and hidden attacks, blended threats, and spyware. By understanding the behavior of web content and the context in which it operates, McAfee SaaS Web Protection can predict malicious intent using its McAfee Gateway Anti-Malware Engine, blocking threats that other security solutions let into the network.

Unfettered use of the web can also lead to unproductive users and legal issues. Managing safe, appropriate Internet access can, but shouldn't have to be, a resource drain. Setting policy rules with our cloud-based console

is simple and provides granular control over online content, media types, applications, and even the time of day specific web services can be accessed.

With no hardware or software to install, McAfee SaaS Web Protection is a reliable, cost-effective solution for comprehensive web security. Built on a proven Software-as-a-Service (SaaS) platform, this global service features near-zero latency, industry-leading uptime and enterprise-class scalability to ensure the performance needed for the most demanding and distributed environments. If you already have on-premises web filtering, our service is a low-risk, low-cost solution that can increase your protection profile with advanced anti-malware or simply protect branch offices and mobile users.

**Key Motivators**

- Desire to lower the maintenance overhead of your existing web security technology.
- Increased issues with malware.
- Requirement to provide enterprise-class security for remote or mobile users.

**McAfee Global Threat Intelligence Gathers Worldwide Threat Data**

Web threats and malicious content span the globe, and so does McAfee research. The McAfee Global Threat Intelligence network collects, analyzes, and distributes real-time data from more than 100 million sensors in more than 120 countries:

- In North America, spam URLs make up 41% of all web threats, followed by malicious sites and suspected malicious sites.
- In Europe/Middle East/Africa, spam and phishing URLs each make up 31% of the total, with malicious sites filling out another 29%.
- In Latin and South America, 36% of malicious URLs are associated with spam hosting, while 30% host phishing sites, and 25% host other sorts of malicious websites.
- In Asia/Pacific, 31% of the total is made up of questionable sites—those servers registered in such a way that the site should be closely monitored. Spam URLs make up the next largest group at 29%, followed by malicious sites at 24%.

(Source: McAfee Labs)

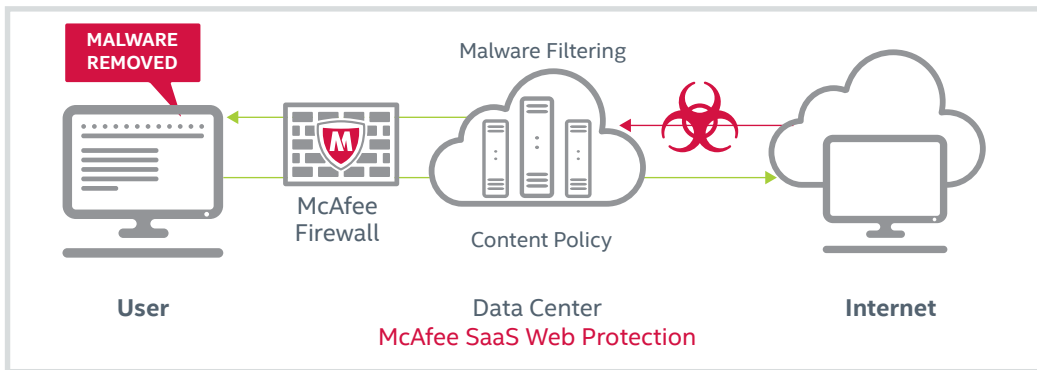


Figure 1. McAfee SaaS Web Protection web request flow.

**Complete Web Protection**

McAfee SaaS Web Protection secures all inbound and outbound web traffic. It enforces your organization’s Internet use policy by automatically applying access rules to all policy-controlled users. Traffic that violates your policy is blocked before it can enter your network. For permitted traffic, McAfee SaaS Web Protection uses sophisticated techniques to analyze the nature and intent of all content and active code on the requested web pages with an advanced anti-malware engine, layered on top of antivirus and global threat reputation filters. This provides immediate protection against malware, viruses, and other exploits by blocking malicious pages and stripping out threatening elements, delivering safe content so users can continue to get their work done.

**Content Analysis Detects Changing Malware**

Malware on websites can download silently to unsuspecting visitor devices, resulting in data exfiltration of intellectual property or customer information. By scanning a web page’s active content and understanding its intent or predicted behavior, we proactively protect against zero-day malware, blended threats, phishing sites, and targeted attacks that are trying to steal your information, all powered by our award-winning McAfee Gateway Anti-Malware Engine.

**Flexible, Comprehensive Control**

Web usage in a business environment is a double-edged sword: it is often both the center of productivity and a convenient, sometimes costly, platform for inappropriate activity. Protecting users from malware is essential—but not your only priority. Stopping data loss and keeping employees productive can save money and prevent potentially debilitating legal liabilities.

With comprehensive web filtering options including approximately 100 site categories, hundreds of media types, more than 1,000 online applications, and even encrypted SSL traffic, you can ensure web access is free of offensive, undesired, or unproductive activity. Users can still experience the freedom of the web without time-wasting distractions. At the same time, you gain the ability to:

- Drill down to specific web applications and allow employees to access social media sites at specified hours.
- Keep data in-house by disabling the upload function or enforcing file encryption before uploading files to online file-sharing sites while allowing the download of files from external collaborators.
- Allow remote or mobile employees to access the web at their own discretion while continuing to enforce enterprise-class security.

Granular controls like these are more effective than indiscriminate blocking of Internet access and allow you to foster a productive and secure online experience.

### **Simplified Transparent Authentication, Plus Protection on or off the Network**

Routing your employees' web traffic couldn't be easier with McAfee SaaS Web Protection. You can utilize standard routing technologies, such as a browser proxy setting or a proxy auto configuration (PAC) file, or make it even easier with the McAfee Client Proxy. With this free, optional client software technology, you can implement seamless authentication and redirection without having to manage a browser plug-in or cookies, backhaul traffic to a central hub, or write PAC files. The tamper-proof McAfee Client Proxy enables web protection policies and web security to be applied to off-network, roaming users, even if their Internet access is being provided through a public portal, such as at a coffee shop, hotel, or other Wi-Fi hotspot.

### **Convenient Administration and Reporting**

Customizable dashboards help each administrator monitor trends and gain a better understanding of how the organization uses web and email resources. From any browser, you can isolate problems, document inappropriate activity, comply with regulatory reporting, and fine-tune filtering settings to enforce web-usage policies. Tailored notifications alert users of policy violations and blocked web content. Administrative alerts provide instant knowledge about important security events.

### **Learn More**

Securing your business is simple and affordable with McAfee cloud-based security services. Use **McAfee SaaS Web Protection** in addition to our **McAfee SaaS Endpoint Protection**, **McAfee SaaS Email Protection**, and **McAfee SaaS Email Archiving** services to cover all digital threat and compliance vulnerabilities.

In addition to SaaS offerings, McAfee provides all-in-one product offerings that include appliance, virtual, and SaaS form factors for anyone looking for the most flexible solutions.

For more information, visit [www.mcafee.com/saas](http://www.mcafee.com/saas) or [www.mcafee.com/webprotection](http://www.mcafee.com/webprotection).

