

# McAfee SaaS Web Protection Service

## Table of Contents

Executive Summary	3
McAfee SaaS Web Protection Service—It’s Your Business Safety Net	3
Greater Threat Protection and Operational Efficiency via Managed Security Services	4
The Control Console Offers Convenient Administration and Reporting Tools	6
Innovative Technology Powers McAfee SaaS Web Protection Service	8
McAfee SaaS Web Service Capabilities	10
McAfee SaaS Web Protection Service Suites	12
Learn More	14

### Executive Summary

Armed with a mouse and unrestricted Internet access, your employees can play a dangerous game of Russian roulette with their computers, your network, and, ultimately, your organization's bottom line.

With each innocent click of the mouse, your users can expose your business to threats ranging from network-crippling viruses and information loss resulting from spyware to harassment suits arising from access to inappropriate content and hours upon hours of lost productivity.

For many organizations, Internet access is integral to day-to-day business. Left unchecked, however, the use of this powerful tool can wreak havoc in your organization. Today's web-borne threats have grown increasingly malicious, and, when combined with email threats, such as phishing attacks, the effects can be devastating to your users and your network.

Less noticeable perhaps, but just as damaging to your organization, are the effects of unauthorized web surfing and use of streaming media. Whether measured by the hours lost to non-work-related surfing or by the related usage of bandwidth and power, your business is losing money with each mouse click.

While the Internet provides quick and easy access to information related to virtually any subject you can imagine, most of it probably has no direct relationship to your business. Unfettered access to content categories like gambling, shopping, and pornography can cause trouble for your business faster than an employee can update his status on Facebook.

The McAfee® SaaS Web Protection service can help any business tap into the power and efficiency of the Internet while keeping threats—from inside and outside of the business—in check. By combining industry-leading protection against web-borne and blended threats with powerful administrative capabilities, the McAfee SaaS Web Protection service is a comprehensive Internet security solution. The fully managed service requires no hardware or software integration and offers ease of use and administration unmatched in the industry.

This overview reviews the features, functionality, and foundational technologies that power the McAfee SaaS Web Protection service and explains why choosing a Software-as-a-Service (SaaS) solution from McAfee gives you an advantage over in-house solutions and is an alternative to on-premises appliances:

- Protects businesses from unproductive web usage
- Provides protection against a wide range of web-based malware
- Provides detailed visibility into web usage
- Shields the business against workplace claims
- Aids in regulatory compliance

### McAfee SaaS Web Protection Service—It's Your Business Safety Net

The McAfee SaaS Web Protection service was developed to meet the needs of businesses with current web security solutions that cannot combat quickly evolving threats or with no solution in place because they cannot justify the cost or support the complexity of today's solutions designed for larger businesses with dedicated security professionals.

Offering robust protection against web-based threats and greater control over employee web usage, the McAfee SaaS Web Protection service is available as a convenient, feature-rich SaaS service as a stand-alone offering and is also available in multiple suites that allow for a flexible deployment method enabling the use of multiple form factors (SaaS, appliance, or virtual appliance). It is designed to offer enterprise-level service and performance without significant complexity by relying on McAfee security professional and is available at a competitive cost—including convenient month-to-month contracts.

### **Reduce overall IT costs**

The McAfee SaaS Web Protection service can help your business drastically decrease the costs associated with excess bandwidth usage and ongoing maintenance. Unlike appliances and software solutions that require integration, migration, and ongoing maintenance, our service is effortless and effective. It requires no additional hardware or software or the constant diligence needed to apply and integrate updates, new patches, and filters—McAfee takes care of all of that for you.

### **Protect networks and individual computers from infection**

McAfee SaaS services work at the network perimeter to protect all of your users, including those connected remotely, by blocking malware, spyware, viruses, and phishing attacks. Our in-the-cloud protection has been proven to be the most effective way to defend the entire enterprise infrastructure from a wide range of malicious threats, including threats from Web 2.0 environments.

### **Reduce the risk of business disruption**

Businesses can easily increase operational efficiency and employee productivity by decreasing the threat of PC infection from spyware and viruses. The loss of productivity is severe when even one computer is infected, tying up IT resources and impacting the employee. If infections are present on multiple computers or the network itself, the effect is even more profound.

### **Protect employees from fraud and the company from IP theft and compliance violations**

With the McAfee SaaS Web Protection service, you can reduce your levels of information leakage by limiting the harmful effects of spyware or even restricting access to websites with poor reputations that may be hosting the spyware. The service not only stops new spyware from latching onto user computers, it also prevents existing spyware from sending its information payload back to its host.

### **Effectively enforce Internet usage policies**

McAfee provides a variety of tools to help administrators establish and enforce appropriate filtering policies. Every minute spent surfing or viewing a non-work-related website is a minute lost from the business. The McAfee SaaS Web Protection service can help you control on-the-job web surfing by limiting where and when your users can surf.

### **Incorporate effortless policy-setting and administration**

The McAfee SaaS Control Console, our web-based administrative platform, is intuitive and easy to use, giving administrators the flexibility to establish policies for individuals or groups, including the ability to set appropriate web threat protection levels and select which Internet content categories should be allowed or denied. Administrators can also define specific policies and filtering rules for different times of day or days of the week with scheduled policies. This feature provides greater flexibility for setting policies, enabling administrators to set different web policies during the lunch hour than for the rest of the workday, for example.

Real-time, daily, weekly, and monthly reports allow IT staff members to quickly analyze and track web traffic and usage trends to help improve overall performance and isolate issues before they become problems. Performance reports can be pushed to administrators on a scheduled basis for review.

### **Greater Threat Protection and Operational Efficiency via Managed Security Services**

Simply put, every organization with an Internet connection should implement a security solution that protects users and the business network from web-based malware. In addition, businesses that are concerned with reducing costs, increasing productivity, and limiting legal liability should also consider a solution that provides administrative oversight and control over internal web usage.

Today's smart businesses are finding that the perfect solution is one that offers robust, up-to-date protection with easy administration and use at an affordable price point. With the McAfee SaaS Web Protection service in place, your business can take a "set-it-and-forget-it" approach to web security—

### The McAfee SaaS Difference

The McAfee SaaS Web Protection service includes the following features and protection not available in competing solutions:

- *Advanced malware scanning*—McAfee Web Gateway anti-malware engine effectively detects malicious behavior and new variants of known malware families through analysis with the McAfee Global Threat Intelligence database
- *Group policy support*—Different policies for different groups, not one size fits all
- *Roaming user support*—Protection for the network from infections brought in by laptops
- *Detailed usage reporting*—Forensic-level threat, content, and usage reports provide visibility into corporate web traffic trends and use by individuals
- *Centralized administrative console*—Integrated with all other McAfee SaaS services
- *Multiple authentication mechanisms*—Login, IP, or transparent authentication in any combination
- *Flexible, scalable platform*—Plug-in architecture can easily adapt to evolving threats
- *Identical security technology as utilized in the McAfee Web Gateway*—Technologies include the anti-malware engine, McAfee Global Threat Intelligence™, anti-virus engine, and even categorization filters

without the ongoing management headaches and costs associated with certain solutions. The fully managed security service delivers a wide range of benefits over competing solutions.

#### **Prevents threats from entering the network**

All filtering is performed at the network perimeter, the outermost layer in a multilayered security strategy which prevents malware from reaching an organization's network or computers.

#### **Ensures up-to-date security**

McAfee uses global threat intelligence to continually update our system to protect against the latest threats—no need to update systems with new hardware, patches, signature files, and URL category lists.

#### **Delivers unmatched ease of administration and use**

Administration and reporting for all McAfee SaaS services is performed via the McAfee SaaS Control Console, our intuitive, easy-to-use web-based platform.

#### **Provides flexible, scalable protection**

If your organization adds new geographic locations, you don't need to deploy additional services for web filtering. The McAfee SaaS Web Protection service grows as you grow. Our operations team builds out our infrastructure to meet demand so that you don't have to add capacity as your user base or web usage grows. Additional flexibility can be found in the many bundles of security technology, including McAfee SaaS Email Protection and McAfee SaaS Web Protection which offer all form factors an organization could want: SaaS, appliances, and virtual appliances.

#### **Eliminates exorbitant up-front costs**

Our service does not require an up-front investment in hardware, software, or setup fees. Our month-to-month terms allow you to use your operating budget rather than drawing on your capital budget.

#### **Gets you up and running quickly**

Provisioning is simple and fast. Once you've purchased our solution, you don't need to wait for anything to ship. Nor do you need to install it. The setup and administration of our service is simple and is performed via a web-based console.

## Solution Guide

### Increases reliability and availability

Our web security service is hosted in fully redundant, highly reliable data centers and is managed by our operations and global threat intelligence teams.

### Simplifies the desktop

PCs can become crowded with point solutions (for example, separate software for anti-virus, anti-spyware, and URL filtering)—not only on the client systems, but at the gateway as well. These point solutions become a maintenance issue and can introduce compatibility problems. McAfee SaaS-based solutions do not rely on software installed on your users' PCs.

### The SaaS Control Console Offers Convenient Administration and Reporting Tools

Administration of all McAfee SaaS email and web security services, including the McAfee SaaS Web Protection service, is performed through the McAfee SaaS Control Console. This intuitive web-based platform is also integrated with single sign-on with the McAfee SaaS Security Platform and is designed for ease of use. It enables administrators to perform these tasks:

#### Set McAfee SaaS Web Protection service policies

- Activate threat control anti-spyware and anti-phishing filters
- Select which website content categories should be blocked
- Add trusted and blocked sites
- Create customized group policy filtering that meets the unique needs of specific user groups, including functional groups like accounts payable, sales, engineering, or even individual users

#### Set up users and groups

Users and groups can be easily set up for the McAfee SaaS Web Protection service filtering by using one of the following options:

- *Directory integration*—Customers can synchronize account information automatically through directory integration, eliminating the need to manually make changes in both the corporate Microsoft Active Directory and the McAfee SaaS system. Account information can be synchronized on an automated schedule, ranging from one to four times per day, as determined by the administrator. The administrator may also initiate a manual synchronization of account information. Directory integration is an ideal solution for organizations that make frequent changes within Active Directory and that want to simplify management of their McAfee SaaS managed security solution.
- *Explicit user creation*—Allows users to be created individually or through batch uploads and enables administrators to set specific filtering policies for individuals or groups
- Group administrators can be defined to offload the maintenance of groups and policy changes as necessary

#### Set up user authentication methods

Through the management console, administrators can determine how users will be authenticated when accessing the web. McAfee offers the following options:

- *Explicit user authentication*—With this method, users with a primary user account in the McAfee SaaS management console sign in with a username and password each time they launch a new web browser. This method is ideal for customers with roaming users and provides administrators with insight into the web activity of individual users.
- *IP address range authentication (optional)*—With the optional IP address range authentication, access to the web is granted by validating that the IP address of the user matches one of the IP addresses listed in the administration console. When using this authentication method, web activity reports will reflect usage at the IP address level.

- *WP Connector<sup>SM</sup>*—With the WP Connector, users are able to access the web with existing network credentials, eliminating the need to re-authenticate through a browser. Administrators can apply group policies and can access reporting for allowed sites, blocked sites, and threats blocked at a user level.

### Access a wide range of reports

Through the McAfee SaaS Control Console, administrators have access to a number of real-time daily, weekly, monthly, and on-demand reports, which help you to quickly analyze and track web traffic and trends. Depending on their role, administrators can review statistics for the organization as a whole or specific domains or individual users. This reporting can help you improve overall performance and isolate issues before they can escalate. All reports are available for downloading in .csv or .txt file formats and predefined reports are active in the sense that administrators can drill into the data to get more granular data at the click of a link.

The McAfee SaaS Web Protection service reports include:

- *Traffic overview*—The reports in this section provide an overall understanding of the traffic and bandwidth trends, including the number of content requests that were allowed and blocked in the selected reporting period and the data volume utilized
  - » *Data volume in/out*—Displays inbound/outbound bandwidth usage
  - » *Allowed/blocked content requests*—Displays the aggregates of allowed requests by users over a specified time period. These numbers include one or more hits on a single visit to a web page.
- *Threat filtering*—These reports provide an overview of the threats that the McAfee SaaS Web Protection service filters for the specified time period. The threats monitored include Trojans, spyware sources, spyware effects/privacy concerns, phishing, and viruses.
  - » *Threat distribution*—Displays the overall percentage for each threat type detected
  - » *Threat trends*—Shows the aggregates of blocked requests over a specified time period, grouped by threat type
  - » *Top sites and top protected users*—Lists the top sites and top protected users for the particular threat selected on the main view of threat filtering
  - » *Top viruses*—Displays the top viruses for the specified time period
- *Allowed content*—These reports contain data relevant to all allowed requests for the specified time period, organized by category, helping customers to continually hone their policy sets
  - » *All categories/traffic*—Lists the most requested content categories
  - » *All categories/data volume in*—Shows the categories taking up the most network bandwidth. In some cases, a category may not be the most heavily requested, but it may be requiring an inordinate amount of bandwidth
  - » *Top sites and top users*—Lists the top sites and top users for the particular category you selected on the main view of allowed content
  - » *Top viruses*—Displays the top viruses for the specified time period
  - » *Traffic trends*—Displays the aggregates of traffic trends over a specified time period
  - » *Traffic summary by category*—Displays the aggregates of allowed requests, by category, for the specified category
- *Blocked content*—These reports contain data relevant to all blocked content requests for the specified time period, organized by category
  - » *Top categories*—Displays a ranked list of all web categories blocked by the service
  - » *Traffic trends/all categories*—Displays the aggregates of blocked requests for the specified time period
  - » *Top sites and top users*—Lists the top sites and top users for the particular category you selected on the main view of blocked content
  - » *Top viruses*—Displays the top viruses for the specified time period

## Solution Guide

- » *Traffic trends*—Displays the aggregates of traffic trends over a specified time period
- » *Traffic summary by category*—Displays the aggregates of blocked requests, by category, for the specified category
- *Audit trail*—The McAfee SaaS Web Protection service audit trail reports display the audit log items for all actions performed by service administrators, including configuration and policy changes
- *Performance reports*—Performance reports provide customers with greater insight into the ongoing performance of their email and web security services. These reports will allow not only the easy manipulation and comparison of data, but also the ability to send these reports automatically to a distribution list. Administrators can opt for weekly and/or monthly delivery of performance reports, which include:
  - » Data volume in (KBs)
  - » Data volume out (KBs)
  - » Total traffic requests
  - » Allowed traffic
  - » Blocked content
  - » Blocked threats
- *Forensic reports*—Customers who need greater detail than is provided in the standard McAfee SaaS Web Protection reports can drill down into log data to create their own special reports. Authorized administrators can view, sort, filter, and download data using a variety of search criteria that include:
  - » Date/time range
  - » User name
  - » Group name
  - » Requested host
  - » Requested path
  - » Category
  - » Result
  - » Server-to-client bytes
  - » Client-to-server bytes
  - » Source IP
  - » HTTP action
  - » Virus

### Innovative Technology Powers McAfee SaaS Web Protection Service

Businesses that are protected by the McAfee SaaS Web Protection service quickly realize the advantages of utilizing a fully managed security service. Our advanced technologies never grow obsolete, are continually updated to protect against the latest threats, and don't require the ongoing management and maintenance necessary with certain appliance-based or other in-house solutions. Year over year, multiple publications have ranked the McAfee Gateway anti-malware engine as the leading engine on the market.

As soon as your service is activated, your business is immediately backed by the full range of McAfee SaaS technologies and threat expertise. Working outside of your network to ensure that threats are kept safely at bay, our service allows your organization to use the Internet efficiently, safely, and productively.

### Advanced technologies eliminate web-based threats

Once your web traffic is routed through our web proxy servers, which are housed in redundant data centers, we begin to filter the traffic according to policies you've determined in the McAfee SaaS Control Console.

- Content and phishing policies are applied that prevent users from accessing inappropriate websites. A customizable per-policy "access denied" web page is displayed when access to the undesirable web page is blocked.
- The McAfee SaaS Web Protection service helps you to limit unauthorized web surfing with the help of McAfee Global Threat Intelligence, which contains more than 100 content categories. Our technology looks for content clues within previously unseen websites and blocks those that conflict with your allowed content policies. Content controlling features also use safe search, which prevents users from accessing prohibited content via search engine results.
- Unclassified websites are identified and automatically submitted for classification by the McAfee SaaS system. Users can also nominate websites for prioritized classification by clicking the feedback button on the control console.
- In addition to policies covering content, proactive anti-malware controls can understand the intent of different programs, executables, and actions to understand if the information should be allowed or not
- Phishing attempts are effectively blocked to protect your employees from identity theft and fraud. Should an employee receive a phishing email and attempt to click on a fraudulent link, the suspect URL is immediately compared with our extensive database of known phishing URLs and, if found, incoming web traffic is blocked. Because phishers may keep their fraudulent sites up for a limited amount of time, the McAfee SaaS Web Protection service works to detect phishing "fingerprints" in incoming web traffic and blocks previously unseen websites that appear suspicious.
- If spyware is brought into the environment (from USB drives and other devices) payloads are blocked at the network perimeter as spyware tries to "phone home"
- Finally, web traffic is scanned by McAfee Web Gateway anti-malware technology for malicious code, including spyware, viruses, and Trojans

### McAfee Labs™ monitors the global state of web threats

McAfee Labs delivers the core technologies and threat intelligence that power the suite of endpoint, web, email, and network security products from McAfee. With a research footprint that covers the globe, McAfee Labs provides accurate and predictive global threat intelligence. A team of approximately 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation. Support from the McAfee Labs 24/7 emergency response team ensures the highest level of insight into emerging risks.

### Guaranteed, around-the-clock availability

Our multiple, redundant data center production environments and the McAfee SaaS Network Operations Center (NOC) provide 24/7/365 operational support and automated monitoring of all service components. Our production facilities provide for carrier-grade infrastructure, and our architecture design lends itself to a low-cost and highly distributed environment. Network and application monitoring provides remote operations personnel visibility into suspect or trouble alerts and alarms. McAfee data centers have been ISO/IEC 27001:2005 certified for the following:

- Management and change control for the hardware infrastructure and software applications after deployment
- Network configuration and traffic management
- Network and data security
- Incident responses
- Problem identification and remediation

### Reduced latency provided through innovative architecture and technologies

Because our proxy servers cache local copies of popular web content, as popular web accelerators do, some users will experience faster browsing performance than if they bypassed our filtering service. By keeping your PCs free of spyware and other malicious programs, the McAfee SaaS Web Protection service helps PCs run faster, which also improves web browsing performance.

### McAfee also helps minimize HTTP latency in a number of ways, including:

- *Content caching*—Popular content is cached on our proxy servers, so that it can be sent to the client more quickly than retrieving it from the target website, which is commonly done by popular “Internet accelerators”
- *Parallel processing*—Web pages are often a collage of elements retrieved from multiple locations. Our servers accelerate webpage loading by retrieving webpage elements in parallel.
- *Excess capacity*—Our operations team ensures that our network and servers have sufficient capacity to handle spikes in web traffic
- *Intelligent malware scanning*—Our process streamlines resource-intensive virus/spyware/Trojan scanning by remembering objects that have been scanned previously and only scanning unknown objects. Small objects (like images typically embedded in a webpage) are processed separately and with higher priority than large objects (like file downloads). This ensures that users doing large file downloads don’t negatively affect the time-sensitive web browsing of other users.
- *Fewer network hops*—We minimize network latency by locating our web filter servers just one hop away from multiple tier-one network providers. This means fewer hops for your traffic to reach our proxy servers and fewer hops for our proxy servers to reach your target websites.

### McAfee SaaS Web Protection Service Capabilities

Whether your organization is looking to strengthen its defense against web threats or to gain greater insight and control over non-business-related Internet usage, or both, the McAfee SaaS Web Protection service is designed to meet your needs.

### McAfee SaaS Web Protection service threat protection

Each trip taken on the Internet is an open invitation for malware to attach itself to users’ computers and your network. As malware writers increasingly turn their attention from email to web-based and blended threats, it has become imperative for businesses to shield their users and networks from harm.

The McAfee SaaS Web Protection service leverages the McAfee Web Gateway anti-malware engine to enable businesses to protect their employees—including those connected remotely—and network assets from harmful Internet-based threats. The McAfee SaaS Web Protection service works outside of your network to block spyware, Trojans, and viruses, including those embedded in webmail messages, before they reach your networks or computers. Spyware that is already installed or introduced through another medium is prevented from “phoning home” to deliver its payload of secretly collected data. Phishing attacks are also blocked to protect users from fraud and identity theft.

- *Advanced spyware protection*—Spyware is rampant on the Internet and poses a wide range of threats to computers on your network. This malicious code spies on your computer activity and reports back to anyone willing to pay for the information. Spyware ranges from the benign type, which merely tracks the websites you visit, to the dangerous keystroke loggers that can capture PINs, passwords, and credit card numbers. Spyware is not just prevalent on questionable websites—it’s also embedded in thousands of legitimate websites, waiting for the next unsuspecting visitor.

The threat protection capabilities help protect against all spyware, whether it’s embedded in downloads, ads, or web pages. The service works in both directions, preventing spyware from entering your network and blocking the outgoing information payload from malicious code already installed on user computers.

The threat protection capabilities help protect against all spyware, whether it's embedded in downloads, ads, or web pages. The service works in both directions, preventing spyware from entering your network and blocking the outgoing information payload from malicious code already installed on user computers.

- *Powerful anti-virus scanning*—The widespread use of web-based email has given virus writers the opportunity to enter your business through the browser, instead of the more common email client. These destructive worms and viruses can cost your business thousands of dollars each year in lost productivity, IT drain, network bandwidth overload, and general corporate cleanup efforts. The McAfee SaaS Web Protection service features powerful anti-virus protection that is outstanding at identifying Trojans, a favorite method for hackers to distribute spyware via the web. Our systems automatically update their virus definitions within minutes of publication.
- *Effective fraud-fighting capabilities*—The increase in the number and complexity of fraudulent phishing scams each year is causing unsuspecting users to become victims of identity theft and organizations to be faced with the potential for unintended financial and security disclosure. Your users are protected from falling prey to fraud and identity theft. Should a user click on a link to a fraudulent website (usually via a phishing email or Instant Message), McAfee blocks access to the site if it is known. Multiple sources of phishing site data help ensure that users are protected by these evolving, transient threats.

### McAfee SaaS Web Protection service content protection

Whether you're looking for news, weather, sports, music, entertainment, or just random information, the Internet has it all. However, it's a good bet that most of what's available on the Internet has nothing to do with your business. For many of your users, the Internet is the world's biggest distraction and is sapping your business of productivity, consuming bandwidth, and potentially putting your business at risk.

McAfee SaaS Web Protection content protection capabilities can help you to manage how the Internet is used in your organization by enabling effective monitoring and limiting employee web surfing. With this convenient package, businesses can limit liability and promote a wholesome work environment by defining policies that limit where users can surf (for example, no pornography or gambling). Productivity can increase and network bandwidth conserved by minimizing or controlling access to online distractions such as personal webmail, gaming sites, or media downloads. Furthermore, you can also increase organizational security, as many unsavory websites are used to propagate malware, and blocking access to these sites reduces exposure to such threats.

- *Broad URL filtering capabilities*—McAfee SaaS Web Protection draws on the extensive McAfee TrustedSource™ URL categories list, which includes more than 100 content categories. Administrators can easily select and block the content categories deemed inappropriate for on-the-job surfing.

### SaaS Web Protection Service website content categories

The SaaS Web Protection service content category list is continually updated as unclassified websites are identified and automatically submitted for classification. Users will see an "access denied" message if they attempt to visit web pages that violate the policy set by administrators. In the event that approved websites are included within a prohibited content category, administrators can include the site on a trusted sites list.

Administrators are provided with the tools they need to block use of bandwidth-robbing streaming media sites, including those that sell, deliver, or stream music or video content in any format and those that provide downloads.

Safe search closes the surfing loophole. Safe search helps reduce corporate liability by preventing users from accessing sexually explicit content via leading search engines such as Google, Yahoo!, and MSN. A feature of leading search engines like Google, Yahoo!, Ask, and MSN Live, safe search enables users to set search preferences to filter results for sexually explicit content. The McAfee SaaS Web Protection service forces the search engines to use the safe search filters, regardless of the user's settings. By selecting the safe search option for a user or group of users, content control will automatically block all websites categorized as pornography.

McAfee TrustedSource™ URL categories list

Adult topics	Historical revisionism	Public information
Alcohol	History	Real estate
Anonymizers	Humor/comics	Recreation/hobbies
Anonymizing utilities	Illegal software	Religion and ideology
Art/culture/heritage	Incidental nudity	Remote access
Auction/classifieds	Information security	Residential IP addresses
Blogs/wikis	Information security news	Resource sharing
Business	Instant messaging	Restaurants
Chat	Interactive web applications	School cheating information
Computing Internet	Internet radio/TV	Search engines
Content server	Internet services	Sexual materials
Controversial opinions	Job search	Shareware/freeware
Criminal activities	Malicious sites	Social networking
Cult/occult	Marketing/merchandising	Software/hardware
Dating/personals	Media downloads	Spam email URLs
Dating/social networking	Media sharing	Sports
Digital postcards	Messaging	Spyware/adware
Drugs	Mobile phone	Stock trading
Education/reference	Moderated	Streaming media
Entertainment	Motor vehicles	Technical information
Extreme	Nonprofit/advocacy groups	Technical/business forums
Fashion/beauty	Nudity	Text translators
Finance/banking	Online shopping	Text/spoken only
For kids	P2P/file sharing	Tobacco
Forum/bulletin boards	Parked domain	Travel
Gambling	Personal network storage	Usenet news
Gambling related	Personal pages	Violence
Game/cartoon violence	Pharmacy	Visual search engine
Games	Phishing	Weapons
General news	Politics/opinion	Web ads
Government/military	Pornography	Web mail
Gruesome content	Portal sites	Web meetings
Hacking/computer crime	Profanity	Web phone
Hate/discrimination	Professional networking	
Health	Provocative attire	

McAfee SaaS Web Protection Service Suites

Businesses can increase their overall online security with one of our service suites, which combine the power and protection of our industry-leading email security, web security, and email archiving\* SaaS services. The service suites are backed by live 24/7 support, innovative technology, and our experienced team of threat experts. You can choose the following service suites as an alternative to the standalone McAfee SaaS Web Protection offering to meet the unique needs of your organization:

- *McAfee SaaS Email and Web Protection Suite*—This economical suite includes complete email protection combined with McAfee SaaS Web Protection service
- *McAfee Web and Email Security with Archiving*—A comprehensive bundle that protects your business from spam, viruses and worms, email attacks, fraud, and spyware while enabling you to efficiently store and retrieve all inbound, outbound, and internal emails
- *McAfee Web Protection*—For any organizations that needs the flexibility of multiple deployment form factors and the option of mixing SaaS, virtual appliances, and even hardware appliances to increase their web security profile, the McAfee Web Protection bundle is the choice for them. This offering allows customers to deploy virtual or hardware solutions at corporate offices and deploy SaaS technology for remote users, home office users, or even smaller offices where IT staff may not be available.

## Solution Guide

- *McAfee Content Security Suite*—This suite of products includes all of the McAfee Web Protection security technology in addition to the McAfee Email Protection technology, and even McAfee DLP Prevent and McAfee Device Control to protect all major storage devices and media within your organization

All McAfee SaaS standalone packages and service suites include free phone, email, and online customer support services, and all are available through convenient month-to-month terms, with no setup fees.

### McAfee SaaS Solutions Feature Comparison

McAfee SaaS Web Protection	McAfee SaaS Email Protection	McAfee SaaS Email Archiving*
<ul style="list-style-type: none"> <li>• McAfee Global Threat Intelligence and the McAfee Web Gateway anti-malware engine (consistently the number one-ranked engine on the market)</li> <li>• McAfee anti-virus engine</li> <li>• Anti-phishing protection</li> <li>• URL filtering</li> <li>• Safe search protection</li> <li>• Predefined drill-down reporting</li> <li>• Forensic-level reporting</li> <li>• Peer-to-peer site blocking</li> <li>• Anonymization site blocking</li> <li>• Streaming media site blocking</li> <li>• Group policies management</li> <li>• Scheduled policies</li> <li>• IP and user-level authentication</li> <li>• Microsoft Active Directory synchronization</li> <li>• Batch processing of larger data sets</li> <li>• Custom notification pages</li> <li>• McAfee SaaS Control Console</li> <li>• Distributed administration</li> <li>• 24/7 threat monitoring and protection</li> <li>• Global data center availability</li> <li>• ISO/IEC 27001: 2005-certified data center management</li> <li>• Engines managed by McAfee security professionals</li> </ul>	<ul style="list-style-type: none"> <li>• Advanced spam blocking</li> <li>• Triple virus and worm scanning</li> <li>• Content and attachment filtering</li> <li>• Email attack protection</li> <li>• Fraud protection</li> <li>• McAfee SaaS Email Continuity</li> <li>• McAfee SaaS Control Console</li> <li>• Sophisticated, 14-day spam quarantine</li> <li>• Message audit</li> <li>• Group policies management</li> <li>• Enforced transport layer security (TLS) security</li> <li>• 24/7 threat monitoring and protection</li> <li>• (Optional) Outbound filtering</li> <li>• (Optional) Email intelligent routing</li> <li>• (Optional) McAfee SaaS Email Encryption</li> </ul>	<ul style="list-style-type: none"> <li>• Unlimited storage</li> <li>• Advanced search options</li> <li>• Definable retention for one, three, five, or seven years</li> <li>• Secure data transport and storage</li> <li>• Transactional data acquisition</li> <li>• Parallel search technology</li> <li>• Legal hold</li> <li>• Outlook 2003/2007/2010 integration</li> <li>• Saved searches capabilities</li> <li>• Configurable system status alerts</li> <li>• Mail source health monitoring</li> <li>• McAfee SaaS Control Console</li> <li>• 24/7 online or phone customer support services</li> <li>• (Optional) Additional historical data storage (25 GB increments)</li> <li>• (Optional) Managed import service</li> </ul>

## Solution Guide

### About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. <http://www.mcafee.com>

### Learn More about McAfee SaaS Web Protection Service

McAfee SaaS Sales Team  
9781 South Meridian Blvd., Suite 400  
Englewood, CO 80112 USA  
Phone: 1.877.695.6442  
Fax: 1.720.895.5757  
Email: [sales@mcafeesaas.com](mailto:sales@mcafeesaas.com)

