McAfee® SaaS Web Protection

Solution Guide

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Table of Contents

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 due to 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, as in 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 the related usage of bandwidth and power, your business is losing money with each mouse click. And 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, SaaS Web Protection 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 SaaS Web Protection, and explains why choosing a Software as a Service (SaaS) from McAfee gives you an advantage over in-house solutions or 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 – It's Your Business Safety Net

McAfee® SaaS Web Protection was developed to meet the needs of businesses whose current web security solutions cannot combat quickly-evolving threats or who have no solution in place because they cannot justify the cost or support the complexity of today's solutions designed for larger businesses.

Offering robust protection against web-based threats and greater control over employee web usage, SaaS Web Protection is available as a convenient, feature-rich SaaS service. Designed to offer enterprise-grade service and performance, without enterprise-level complexity and cost, SaaS Web Protection can help your organization to:

Reduce overall IT costs

The SaaS Web Protection service can help your business to drastically decrease the costs associated with excess bandwidth utilization and on-going maintenance. Unlike appliances and software solutions that require integration, migration and a significant amount of ongoing maintenance, our service is effortless and highly effective – requiring no additional hardware or software or the constant diligence needed to apply and integrate updates, new patches and filters.

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 spyware, viruses and phishing attacks. Our in-the-cloud protection has proven to be the most effective way to defend the entire enterprise infrastructure from a wide range of malicious threats.

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 gets 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 SaaS Web Protection service, you can reduce your levels of information leakage by limiting the harmful effects of spyware. The service not only stops new spyware from latching onto user computers, but 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 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 setting appropriate web threat protection levels and selecting which Internet content categories should be allowed or denied. Real-time, daily, weekly and monthly reports also allow IT staff members to quickly analyze and track web traffic and

usage trends in order to improve overall performance and isolate issues before they become problems.

The McAfee SaaS Difference

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

- **Multi-level malware protection**
  - Proactive category filters and malware scanning of returned content
- **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**
  - Threat, Content, and Usage Reports provide visibility into corporate web traffic trends
- **Centralized 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

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, while offering easy administration and use at a price point every business can afford.

With the SaaS Web Protection service in place, your business can take a "set it and forget" approach to web security, without the ongoing management headaches and costs associated with certain on-premises solutions. The fully-managed security service delivers a wide range of benefits over competing solutions, which include:

Preventing threats from entering the network

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

Ensuring up-to–date security

McAfee Labs® Global Threat Intelligence keeps pace with quickly-evolving web threats and continually updates our system to protect against even the latest threats. Administrators aren't forced to continually update systems with new hardware, patches, signature files, and URL category lists.

Delivering 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.

Providing flexible, scalable protection

If your organization adds new geographic locations, you don't need to deploy additional services for web filtering. The SaaS Web Protection service automatically grows as you grow. Our Operations team builds out our infrastructure so that you don't have to add capacity as your user base or web usage grows.

Eliminating exorbitant upfront costs

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

Getting you up and running quickly

Provisioning is simple and fast. Once you've purchased our solution, you don't need to wait for hardware or software 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.

Increasing reliability and availability

Our web security service is hosted in our fully-redundant, highly reliable data centers and is managed by our Operations and Global Threat Intelligence teams.

Simplifying the desktop

PCs can become crowded with point solutions (e.g. separate software for anti-virus, anti-spyware and URL filtering). These point solutions become a maintenance issue and can introduce compatibility problems. McAfee does not rely on software installed on your users' PCs.

McAfee SaaS Control Console – Convenient Administration and Reporting Tools

Administration of all McAfee SaaS email and web security services, including SaaS Web Protection, is performed through the McAfee SaaS Control Console. This intuitive web-based platform is designed for ease-of-use and enables administrators to:

- **Set SaaS Web Protection policies:**
  - Activate Threat Control anti-spyware and anti-phishing filters
  - Select which website content categories should be blocked by Content Control
  - Add trusted and blocked sites
  - Create customized group policies filtering that meet the unique needs of specific user groups, including functional groups like accounts payable, sales or engineering, or even individual users
- **Set up Users and Groups**

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

- **Directory Integration** - Customers can synchronize account information automatically through Directory Integration, thereby eliminating the need to manually make changes in both the corporate Active Directory and the McAfee SaaS system. Account information can be synchronized on an automated schedule, ranging from 1 to 4 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.

- **Set up User Authentication Methods**
  Through the McAfee SaaS Control Console, administrators can determine the manner in which 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 Control 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 McAfee SaaS Control Console. When using this authentication method, web activity reports will reflect usage at the IP address level, and not the user level. In addition, Group Policies cannot be applied when using this method and all filtering is based on a single default policy for all Users.
  - **WP Connector℠ –** With the WP Connector, users are able to access the Web with existing user 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 a number of real-time daily, weekly, monthly and on-demand reports, which help 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 to improve overall performance and isolate issues before they can escalate. All McAfee SaaS Control Console reports are available for downloading in CSV or text file formats. The SaaS Web Protection 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 SaaS Web Protection filters for the specified time period. The threats monitored include Malware Trojans, Spyware Sources, Spyware Effects/Privacy Concerns, Phishing and Viruses. (Total Control and Threat Control packages only).
  - 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. (Viewable with Total Control and Threat Control packages only.)
  - 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. (Viewable with Total Control and Threat Control packages only.)

- 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 –**SaaS Web Protection 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 on-going 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

Innovative Technology Powers SaaS Web Protection

Businesses that are protected by SaaS Web Protection 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 on-going management and maintenance necessary with certain appliance-based or other in-house solutions.

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 Control and phishing policies are applied, which prevent users from accessing inappropriate websites. If the user tries to visit an uncategorized site, our Dynamic Realtime Rating engine attempts to classify the site on the fly, which is essential, as many new inappropriate websites come online each day. An "access denied" web page is displayed when access to the undesirable web page is blocked.
- SaaS Web Protection helps you to limit unauthorized web surfing based on a database of over 60 content categories, with 15 million websites and billions of web pages. Our technology looks for content clues within previously unseen websites and blocks those that conflict with your allowed content policies. Content Control also uses 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 SaaS Web Protection console. Uncategorized websites (usually new or visited infrequently) are scanned in real time by our Dynamic Realtime Rating service, which does an exceptional job of identifying inappropriate content.

- In addition to policies covering content, Content Control can be configured to block incoming file types, including .exe, .ftp, and streaming media, which helps you to reduce risk and bandwidth utilization.
- 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, SaaS Web Protection works to detect phishing "fingerprints" in incoming web traffic, and blocks previously un-seen websites that appear suspicious.
- Spyware payloads are blocked at the network perimeter as spyware tries to “phone home.”
- Finally, web traffic is scanned for malicious code, including spyware, viruses and Trojans.

McAfee Labs monitors global state of Web threats

McAfee Labs delivers the core technologies and threat intelligence that power McAfee’s suite of endpoint, web, email, and network security products. With a research footprint that covers the globe, McAfee Labs provides accurate and predictive Global Threat Intelligence. A team of 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 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 Email and Web Security Network Operations Center (NOC) provide 24x7x365 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 "pod" environment. Network and application monitoring provides remote operations personnel visibility into suspect or trouble alerts and alarms.

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, SaaS Web Protection helps PCs to run faster, which also improves Web browsing performance.

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

- **Content caching:** Popular content is cached on our proxy servers, so 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 Package Options and Descriptions

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. The service protects users on the entire corporate network, including remote users, and is available in three packages, including:

- **Threat Control** – Our powerful web filtering technologies protect employees and network assets from harmful Internet-based threats like spyware, viruses and phishing attacks.
- **Content Control** – This package offers service administrators the tools they need to effectively monitor and limit non-work related web surfing by employees.
- **Total Control** – A comprehensive web security solution, Total Control combines Threat Control and Content Control.

McAfee® SaaS Web Protection - Threat Control

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 SaaS Web Protection Threat Control package enables businesses to protect employees – including those connected remotely– and network assets from harmful Internet-based threats. Threat Control 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 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 benign, by merely tracking the websites you visit, to the dangerous keystroke loggers that can capture PINs, passwords and credit card numbers. Your users don't have to go looking for spyware on questionable websites – it's embedded in thousands of legitimate websites, waiting for the next unsuspecting visitor.

Threat Control helps to 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 clean-up efforts.

  Threat Control features powerful anti-virus protection that is outstanding at identifying Trojans, which are a favorite method of distributing spyware via the Web. Our systems automatically update their virus definitions within minutes of publication.

- **Effective fraud fighting capabilities:** The increase in 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 financial and security disclosure. Furthermore, fraud is damaging the reputation of email as a safe and secure way of collaborating.

  With Threat Control, 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), we block access to the site if it is known. Multiple sources of phishing site data help ensure that your users are protected by these evolving transient threats.

McAfee® SaaS Web Protection - Content Control

Whether you're looking for news, weather, sports, music, entertainment or just random information from any and all corners of the globe, 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 its time-wasting allure is sapping your business of productivity, eating up bandwidth and potentially putting your business at legal risk.

SaaS Web Protection Content Control 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 (e.g. no pornography, gambling). Productivity can be increased, 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 the threat.

- **Broad URL filtering capabilities**: Content Control draws on broad, industry leading URL databases, which contain over 15 million website ratings, representing billions of web pages, more than 60 content categories, in 50 languages. Websites are categorized into one or more categories which have been specifically chosen to aid you in defining relevant filtering policies. Administrators can easily select and block the content categories deemed inappropriate for on-the-job surfing.

Adult/Mature Content	Games	Real Estate
Pornography	Government/Legal	Society/Daily Living
Sex Education	Military	Blogs/Personal Pages
Intimate Apparel/Swimsuit	Political/Activist Groups	Restaurants/Dining/Food
Nudity	Health	Sports/Recreation
Extreme	Computers/Internet	Travel
Illegal/Questionable	Search Engines/Portals	Vehicles
Gambling	Spyware/Malware Sources	Humor/Jokes
Violence/Hate/Racism	Spyware Effects/Privacy Concerns	Software Downloads
Weapons	Job Search/Careers	Pay to Surf
Abortion	News/Media	Peer-to-Peer (P2P)
Hacking	Personals/Dating	Streaming Media/MP3s
Phishing	Reference	Web Applications
Arts/Entertainment	Open Image/Media Servers	Proxy Avoidance
Business/Economy	Chat/Instant Messaging	For Kids
Alternative Spirituality/Occult	Email	Web Advertisements
Alcohol	Newsgroups/Forums	Web Hosting
Tobacco	Religion	Suspicious
Illegal Drugs	Social Networking	Alt. Sexuality/Lifestyles
Education	Online Storage	LGBT
Cultural/Charitable Organizations	Remote Access Tools	Non-viewable
Financial Services	Shopping	Content Servers
Brokerage/Trading	Auctions	Placeholders

The Content Control URL list is continually updated, as unclassified websites are identified and automatically submitted for classification. Users can also nominate websites for prioritized classification by clicking the Feedback Button on the SaaS Web Protection console. Uncategorized websites (usually new or visited infrequently) are scanned in real time by our Dynamic Realtime Rating Service, which does an exceptional job of identifying unsavory content.

With Content Control in place, users will see an “access denied” if they attempt to visit web pages which violate the policy set by your administrator. In the event that approved websites included within a prohibited content category, administrators can including the site on a Trusted Sites list, thereby opening access.

Content Control also gives administrators the tools they need to block the increasing 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 for such viewers.

Safe Search Closes Surfing Loophole: Safe Search helps to 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. SaaS Web Protection forces the search engines to utilize 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 SaaS Web Protection Service Suites

In addition to SaaS Web Protection-only - service packages, 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 24x7 support, innovative technology and our experienced team of threat experts. You can choose the following Service Suites to meet the unique needs of your organization:

- **Email and Web Security**[SM] - This economic suite includes complete email protection combined with SaaS Web Protection - Total Control.
- **Complete Security**[SM] - 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. In addition to SaaS Email Protection & Continuity, Complete Security includes SaaS Web Protection- Total Control and SaaS Email Archiving with retention periods of 1, 3, 5 or 7 years .

SaaS Email Protection	SaaS Web Protection	SaaS Email Archiving
• Advanced spam blocking • Triple virus and worm scanning • Content and attachment filtering • Email attack protection • Fraud protection • SaaS Email Continuity • SaaS Control Console • Sophisticated, 14-day spam quarantine • Group policies management • Enforced TLS security • 24x7 threat monitoring and protection • (Optional) Outbound filtering • (Optional) Email Intelligent Routing	• Anti-spyware scanning • Anti-virus scanning • Anti-phishing protection • URL filtering • Safe Search protection • Peer-to-peer site blocking • Streaming media site blocking • Group policies management • IP and user-level authentication • SaaS Control Console • 24x7 threat monitoring and protection	• Unlimited storage • Advanced search options • Definable retention for 1, 3, 5 or 7 years • Secure data transport and storage • Transactional data acquisition • Parallel Search Technology • Outlook 2003/2007 integration • Saved searches capabilities • Mail source health monitoring • SaaS Control Console • 24x7 online or phone Customer Support Services • (Optional) Additional historical data storage (25GB increments) • (Optional) Managed Import Service

All McAfee SaaS stand-alone packages and Service Suites include complimentary phone, email and online Customer Support Services, and all are available through convenient month-to-month terms, with no setup fees.

About McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, 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. http://www.mcafee.com.

McAfee SaaS Email & Web Security Sales Team
9781 South Meridian Blvd., Suite 400
Englewood, CO 80112 USA
T +1.877.695.6442
F +1.720.895.5757
E sales@mcafeesaas.com