SaaS

(Software as a Service)

2012 Product Guide

Thank You for your interest in Excel Micro!
We are a premier distributor of market leading Software-as-a-Service solutions that help your company migrate to a more reliable, more secure and more cost efficient model.

Call Us at (877) 4NO-SPAM (466-7726)
Or
Visit http://www.excelmicro.com

Excel Micro, Inc.

ABOUT US

Founded in 1991 in the Philadelphia-area's technology corridor, the company's mission is to consistently be: The most reputable distributor of SaaS "Software as a Service" solutions.

Excel Micro is the largest Authorized Distributor of the complete suite of Google Message Security & Compliance Solutions and are responsible for the worldwide reseller channel, managing over 3,500 resellers and close to a million licenses sold. In addition, Excel Micro has built relationship with industry leaders in the SaaS marketplace to be able to offer clients dynamic hosted solutions for very low minimum commitments.

You will have the ability to purchase the market leading SaaS solutions, for Spam/Virus Filtering, Email Encryption, Email Archiving, Office Collaboration, and Web Protection.

Our product brands include Google, Postini, McAfee, ZixCorp, YouSendIt, and other industry leaders. As an Excel Micro reseller you will have access to marketing and training materials, webinars, presentations, fully-functional trials, as well as, Excel Micro's Product Support Specialists. We invite you to join the thousands of companies moving toward SaaS solutions everyday.

PRODUCTS

EMAIL SECURITY
- Google Message Security, powered by Postini
- McAfee Email Protection & Continuity

EMAIL ARCHIVING
- Google Message Discovery, powered by Postini
- Archiving & Discovery, powered by Postini
- McAfee Email Archiving & Security Suite

EMAIL ENCRYPTION
- Google Message Encryption
- McAfee Email Encryption
- ZixCorp Email Encryption
- Cisco IronPort Email Encryption

EMAIL CONTINUITY
- McAfee Email Security & Continuity
- EXM Email Continuity

WEB-BASED EMAIL, CALENDAR, & DOCUMENTS
- Google Apps for Business
- Google Apps for Government

WEB SECURITY
- McAfee Web Protection

EMAIL INGESTION
- Excel Micro Historic Message Journaling
- McAfee Historical Data Storage

SECURE FILE SENDING & SHARING
- Workstream by YouSendIt

Built on industry standards, Excel Micro's suite of products and services brings your business:
- Cost Savings
- Improved Network and Desktop Security
- Administrative Ease

Industry professionals and editors are raving about the Excel Micro solution as:
- Comprehensive
- Cost Effective
- Easy to Install and Maintain

The SaaS model is on track to become the standard that will replace everything you're currently using. It's more effective and less expensive protection.

Google Postini Services

What is Google Message Security?

Google Message Security, powered by Postini, provides highly effective inbound and outbound email security for organizations of all sizes. Google Message Security is always on and always current, so organizations are assured of having effective and reliable protection for their email at all times. Google Message Security blocks spam, phishing, viruses, and other email threats before they reach your organization, reducing load on your email servers, conserving bandwidth and improving the performance of your existing messaging infrastructure.

Google Message Security conserves IT resources by eliminating the constant patching and updates that are required by other appliance or software solutions. End-users manage their own message quarantines and settings with an easy-to-use, web based interface.

What's Included?

- **Real-time** threat identification
- Automatically identifies and tracks internet protocol (IP) addresses that are issuing attacks such as **spam, viruses, denial of service (DoS), etc.**
- Patented real-time anti-spam technology examines thousands of elements of an email message in order to determine if it is spam
- Extremely effective spam filtering, and **exceptionally low false positive rates**
- Multiple commercial anti-virus engines
- **Content management & attachment management** allows you to define policies for both inbound and outbound email that provides an additional layer of protection against external threats

Industry Leader

Google Message Security is the industry leading 100% hosted spam & virus filtering solution. Processing over 3 billion connections per day in real-time keeps clients protected from the latest email security threats. With a simple MX record change you do not need to worry about costly hardware, updates, maintenance, patches, or unexpected downtime. By having email security hosted you are freeing up IT resources to focus on more strategic projects and not worry about time consuming spam & virus filtering.

Requirements & More Information

Google Message Security requires a registered domain and an active email account. For more information on Google Message Security and a helpful video visit www.excelmicro.com/services/spam-virus-filtering. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

FEATURES & BENEFITS

- Comprehensive message security to stop spam, viruses, phishing, denial of service (DoS), directory harvest attacks (DHA), and other email attacks
- **Zero-hour anti-virus** protection with multi-layered protection, including heuristic and signature-based detection
- Extensive and detailed **quarantine summary reporting** to end users through a convenient web console
- Built-in **lexical analysis** for social security and credit card
- Real-time processing with scale & reliability
- Patented real-time, pass-through architecture ensures that there are no delays, message loss or disruptions to email service, regardless of how high spam volumes climb
- **99.999% availability** for message processing and capacity to handle billions of transactions a day
- Policy enforced domain to domain messaging encryption using standard **SSL or TLS** protocols
- **SAS 70 Type II** certified and **WebTrust** seal validates Google's stringent standards for physical and operational security, assuring the safety of your communications

GOOGLE POSTINI SERVICES AUTHORIZED DISTRIBUTOR Google

EXCEL micro

Google Postini Services

What is Google Message Discovery?

Google Message Discovery, powered by Postini, goes beyond the functionality of our security offering to give customers maximum control and flexibility over your electronic records archive, meeting discovery, and compliance objectives.

In addition to the security provided by Google Message Security, powered by Postini, Google Message Discovery provides archiving, discovery, and compliance functionality. Whether you must respond to a discovery situation or want to prepare in advance for an eventual request, Google Message Discovery can help you find and manage the right information quickly and painlessly.

What's Included?

- **All features & benefits of Google Message Security**
- Centralized Message Center for each user to manage their individual archive
- Unlimited storage space
- Email Retention anywhere from 1 to 10 years
- Messages cannot be rewritten or deleted
- Detailed reporting and message holds for audit and other investigations
- Administrator full search & discovery access over the entire domain
- Export search results to PST or MBOX format for further review and analysis

Why Archive?

In today's world, electronic communications are both increasingly critical and growing in volume. Businesses know that they need to archive this critical communications data but struggle with keeping this data from clogging primary communications systems. Google Message Discovery helps companies accomplish both objectives at once.

Offered as a hosted service, Google Message Discovery includes everything you need to get started with an online digital archiving and discovery strategy. No need to worry about hardware, software, upgrades, maintenance, high availability and scalability. What could be easier than a simple, all-inclusive per-user fee? No more complicated math to put together hardware, storage, redundancy and labor costs! It's easy to budget and plan for archiving and discovery costs now with Google Message Discovery.

Requirements & More Information

Google Message Discovery requires companies to have their own mail server. If an ISP hosts your email, we suggest you consider Google Apps for Business, which doesn't require that you own your mail server. For more information on Google Message Security and a helpful video visit www.excelmicro.com/services/archiving. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

FEATURES & BENEFITS

Manage Archives
Centralize storage of message data into a single company archive to offload data from mail servers, enforce a standard retention policy, and provide an easily accessible repository for discovery efforts.

Discover Evidence
Effectively manage multiple investigations, inquiries, and discoveries with enhanced search, save, and restore capabilities. Place records on hold, such as necessitated by litigation notice, which temporarily discontinues automatic message deletion.

Best of all, it's hosted by Google. So there's no hardware or software to download, install or maintain. Google Message Discovery simplifies mailbox storage management, eases IT administration burdens, and lowers the total cost of ownership compared to software or appliance based solutions.

ADDITIONAL SERVICES

hMJ
Historic Message Journaling

Historic Message Journaling is now available. HMJ is an additional solution offered through Excel Micro that will ingest historic emails into you new Google Message Discovery account. This will eliminate the needs to manage two separate archive solutions and have everything now searchable within your Message Center.

GOOGLE POSTINI SERVICES AUTHORIZED DISTRIBUTOR Google

EXCEL micro

Google Postini Services

What is Google Message Encryption?

Google Message Encryption, powered by Postini, provides on-demand message encryption for your organization to securely communicate with business partners and customers according to security policy or on an "as needed" basis.

Without the complexity and costs associated with legacy on-premises encryption technologies, Google Message Encryption service makes encrypting email messages easy and affordable. The policy-based solution enables your organization to send encrypted email to any recipient.

What's Included?

- **Secure messaging** between business partners, customers, or individuals without any additional software, hardware, or technical training
- **Automatic enforcement** of organizational email encryption policies based on individuals, groups, or specific message content
- User-initiated encryption for confidential messages to **any email recipient**
- Auditable protection of emails containing regulated or company proprietary information
- Centrally-managed security policies and reporting

How Does It Work?

Google Message Encryption service secures outgoing email to the Postini data center using a secure SSL/TLS encrypted connection. At the data center, messages are scanned for viruses and messaging policy compliance. Based on centrally managed policies, messages are encrypted for each intended recipient. Encrypted messages are either delivered directly to the recipients' inbox or stored on a web-based portal for secure pickup.

Requirements & More Information

Google Message Encryption requires a Google Message Security or Google Message Discovery account. You must have the ability to redirect your outbound mail on your internal email server or have a Google Apps for Business account in order to use this solution. For more information on Google Message Encryption visit www.excelmicro.com/services/encryption/gme. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

DELIVERY METHOD

Inbox Delivery
The inbox delivery method delivers email directly to the recipients' email application as an encrypted attachment. Recipients can view their messages by opening the attachment and providing their password. If the recipient does not have an existing password, the recipient is stepped through a simple, one-time registration. No additional software is required.

Portal Delivery
Using the secure portal delivery, email notifications are sent to intended recipients letting them know a message is waiting for them. The notification message includes a link to the portal and instructions on how to view the encrypted message using their web browser. Clicking on the link directs recipients to the secure portal. Using the full-featured messaging console, recipients can view, reply to, and compose new messages securely.

GOOGLE POSTINI SERVICES AUTHORIZED DISTRIBUTOR Google

EXCEL micro

Google™ Apps for Business

What is Google Apps?

Google Apps is a suite of applications that includes Gmail, Google Calendar (shared calendaring), Google Talk (instant messaging and voice over IP), Google Docs & Spreadsheets (online document hosting and collaboration), Google Page Creator (web page creation and publishing), Start Page (a single, customizable access point for all applications) and Google Security & Compliance.

Google Apps for Business gives you the communication and collaboration tools to manage electronic communication, information sharing, and stay connected anywhere. Whether your business is moving everything to the cloud, just wants an affordable email solution or struggles to give employees access to critical information, Google Apps will help you stretch resources and work smarter. Google Apps for Business is 100% hosted by Google, so there is no hardware or software to download or maintain.

What's Included?

- **Google Mail** - 25GB storage, less spam, and a 99.9% uptime SLA, mail search tools, integrated IM, and enhanced email security
- **Google Docs** - Create, share and collaborate documents, spreadsheets, and presentations in real-time
- **Google Calendar** - Agenda management, scheduling, shared online calendars and mobile calendar sync
- **Google Sites** - Secure, coding-free web pages for intranets and team managed sites
- **Google Talk**- Instant messenger with free PC-to-PC voice calls worldwide
- **Security**- Spam and virus filtering powered by Postini

Access Anytime Anywhere?

With Google Apps you can access your email, documents, calendars, contacts, and more anywhere you have an internet connection.

Ready To Go Google?

Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email sales@excelmicro.com.

HOW SECURE IS GOOGLE APPS?

Having your mail, documents, and other information hosted in Google's **SAS70 Type II** and **FISMA Certified** data centers is more secure than using your own in-house mail server like Exchange.

Google is the first major cloud provider to offer **2-step verification**, default https encryption, attachment viewing and mobile device management in the browser, along with many other security & administrative capabilities. You can view more of Google's security and data protection measures outlined in their Security Whitepaper.

Google operates on of the most robust networks of distributed data centers worldwide. The data centers are protected around the clock and monitored by a **dedicated security team**, the facilities are held to **extremely high standards of scrutiny** every moment of the day.

Adding Postini services such as **Archiving & Discovery** will help you limit exposure to spam and virus, and will provide you with SAS70 compliant email archiving.

COMPATIBLE PRODUCTS

EMAIL SECURITY
- Google Message Security, powered by Postini

EMAIL ARCHIVING
- Archiving & Discovery, powered by Postini

EMAIL ENCRYPTION
- Google Message Encryption
- ZixCorp Email Encryption
- Cisco IronPort Email Encryption

EMAIL INGESTION
- Excel Micro Historic Message Journaling

WEB SECURITY
- Webroot Web Security SaaS

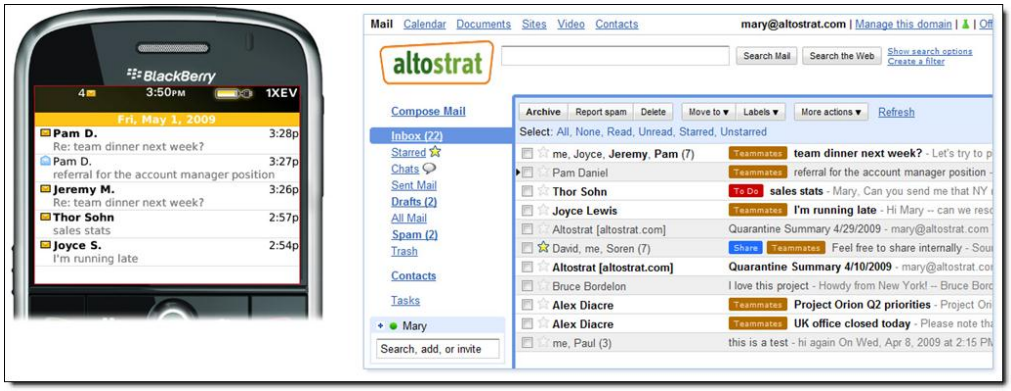


Google APPS PREMIER SMB RESELLER

EXCEL micro

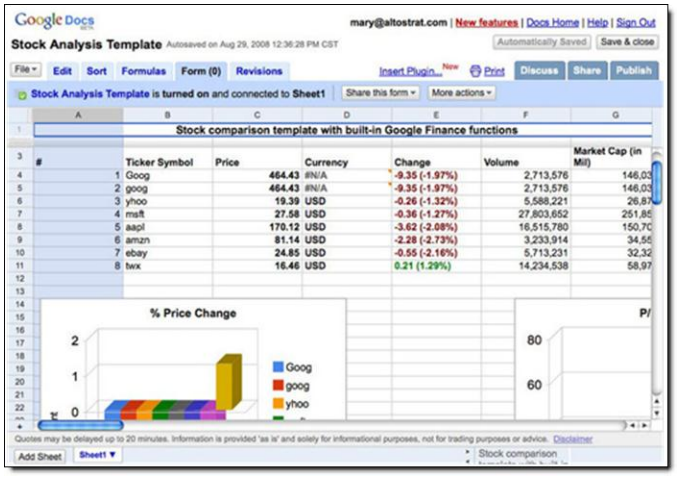
Google™ Apps for Business

Google Apps for Business gives you the communication and collaboration tools to manage electronic communication, information sharing, and stay connected anywhere. Whether your business is moving everything to the cloud, just wants an affordable email solution, Google Apps will help you stretch resources and work smarter

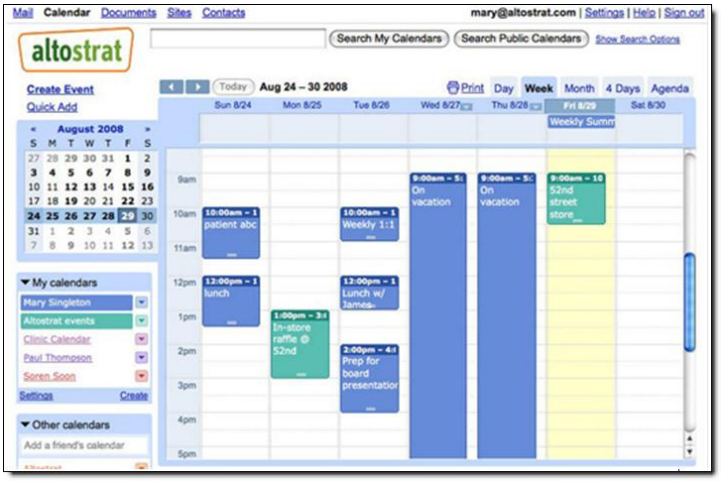


Google Mail- 25GB storage, less spam, and a 99.9% uptime SLA, mail search tools, integrated IM, mobile sync, and enhanced email security

Google Talk- IM with free PC-to-PC voice calls worldwide



Google Docs- Create, share and collaborate documents, spreadsheets, and presentations in real-time



Google Calendar- Agenda management, scheduling, shared online calendars and mobile calendar sync

McAfee SaaS Email Protection & Continuity

Email protection, availability, and compliance for a productive business

Tackle email security the easy way with McAfee® SaaS Email Protection and Continuity. Beyond blocking spam, phishing scams, malware, and inappropriate email content before it reaches your network, this cloud-based service enforces outgoing mail policies to protect you from data loss. Count on always-on email continuity so that your organization has around-the-clock access to email. With no hardware to buy, no software to install, and automatic updates to protect against the latest threats, you can focus on securing your business, not running applications.

Why McAfee Email Protection & Continuity?

- Perimeter IP filtering to **block threats before they reach your network**
- Advanced **spam and fraud protection**
- Layered virus and worm scanning to **block 100 percent of all known viruses**
- Email attack protection
- Filtering and **policy enforcement for outbound** messages and attachments
- **Complete messaging continuity**
- **Group policies** management
- Message audit message tracking and disposition tool
- Optional McAfee SaaS Email Encryption

Low-Cost, Easy-to-Manage Email Protection

A snap to deploy, McAfee SaaS Email Protection and Continuity prevents inbound and outbound email threats from impacting your network and end users, while maintaining continuous access to email, no matter what. This security Software-as- a-Service (SaaS) is always on, is always up to date, and requires no additional investment in time and resources to maintain it. Because the service stops spam and email-based threats before they infiltrate your network, the load on your email servers is greatly reduced, saving you valuable bandwidth and server storage.

Simplified Web-based Administration

With a single, intuitive web-based management console, best practices come built in, and email policy updates are simple to manage across all your domains and locations, freeing up IT resources and lowering your total cost of ownership. Administrators can configure and enforce policies, including content-filtering and attachment content rules. Policies may be applied globally to user groups or individuals for ultimate flexibility. Extensive reports, logs, and quarantines provide ultimate visibility.

Robust Infrastructure You Can Rely On

Our SaaS data center strategy includes maintaining multiple data centers across four continents. Each data center is ISO 27001 certified and provides full redundancy with active-active redundant hardware at all network layers: firewall, router, and load-balancer switch. Within each data center, we also provide automated network and application monitoring, which provides remote operations personnel visibility into suspect or trouble alerts and alarm and 24/7 security experts vigilantly overseeing the systems.

AFFORDABLE & MANAGEABLE

- No hardware or software to buy, maintain, manage, or update
- No upfront capital outlay
- No setup or upgrade fees
- Automatic continuity activation and synchronization for seamless continuity
- Simple web-based administration
- 24/7 customer support at no extra charge
- ISO 27001 certified

McAfee SaaS Email Protection & Continuity

Email protection, availability, and compliance for a productive business

Superior Spam Protection

Our Stacked Classification Framework® spam detection system, powered by a patented technology, applies multiple layers of analysis to determine the probability that an email is spam, regardless of language. McAfee Global Threat Intelligence™ message reputation inspects each message to detect known and emerging message-based threats such as spam, even if these messages come from a reputable source, such as an infected system within a whitelisted company.

Block Viruses & Worms

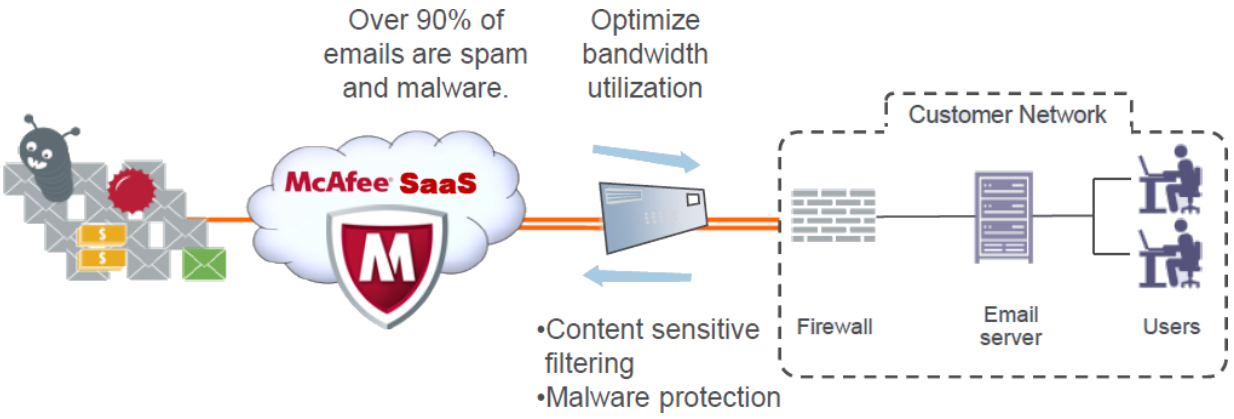
McAfee SaaS Email Protection and Continuity includes our proprietary WormTraq® detection technology. It also scans for malware, in both the message body and all attachments, using our industry-leading, signature-based antivirus engine powered by McAfee Global Threat Intelligence. Just as important as blocking inbound attacks, outbound emails are filtered to protect your clients against malware.

Always-on Email Continuity

Business doesn't stop when email networks experience an outage. Whether the network is inaccessible due to natural disasters, power outages, or even regular maintenance, McAfee SaaS Email Protection and Continuity keeps employees, customers, partners, and suppliers connected 24/7. The secure, easy-to-use web interface allows users to send and receive messages with continued protection, search for and retrieve stored messages, and manage quarantines and message stores. The service retains all messages sent or received during the outage, intelligently synchronizing an accurate record of all outage-period message activity when your own email servers come back online.

SEAMLESS EMAIL CONTINUITY

- Automatic service engagement when an outage is detected
- Access to email received during an outage via a secure web interface
- Full email functionality, including read, compose, reply, forward, and delete
- Intelligent post-outage email activity synchronization
- Outage notifications and system updates
- Inbound and outbound message filtering



McAfee SaaS Email Archiving

Reliable, in-the-cloud email archiving with your choice of one or multiple years of message retention

McAfee® SaaS Email Archiving is your answer to reducing email storage and management costs, satisfying e-discovery and compliance needs, and protecting your business and employees. By adopting a software-as-a-service (SaaS) model, you virtually eliminate management burdens while ensuring safe, simple, cost-effective retention of inbound, outbound, internal, and even historical email. Anytime you need to find a particular message—or even thousands of messages—the precise information you're looking for can be at your fingertips in just seconds.

Email volumes are soaring, and email has become a primary medium for communicating all kinds of information. Reliable storage and quick access to that information is essential to business operations. At the same time, government and industry regulations require you to keep paper trails for myriad decisions and processes—whether or not any actual paper is involved. Businesses of all sizes, therefore, need a way to safely store and rapidly retrieve the massive volumes of email they generate every day.

Why McAfee Email Archiving?

- **Total protection** for your email-based **data assets**
- Powerful e-discovery features to retrieve information in seconds
- Full support for **industry and regulatory compliance** requirements
- No hardware or software to install or manage
- **Unlimited storage** at no extra charge
- Retention for one or **multiple years**

Fast, Affordable, Simple

McAfee SaaS Email Archiving takes care of all your email storage, management, and retrieval needs with a cloud-based service that eliminates the need to manage backup media and onsite storage. It's an easy-to-use, fully integrated, and economical service that:

- Automatically and safely stores email for future review and e-discovery
- Offers users powerful, precise, and rapid search capabilities without the need for IT assistance
- Replaces cumbersome, costly, and unreliable tape backup
- Requires no hardware or software purchases

Complete Protection for Your Business

McAfee SaaS Email Archiving is offered as a standalone service or bundled as part of the McAfee SaaS Email Security and Archiving Suite, which includes inbound email filtering and email continuity. When you choose the suite, you gain complete confidence that your massive email volumes will be safely stored and easily searchable, at any time.

AFFORDABLE & MANAGEABLE

- More effectively manage email retention without adding more resources
- Minimize business risk, satisfy compliance needs, and reduce legal liabilities/litigation
- Incorporate business continuity with complete email backup protection
- Increase email security by preventing message tampering

McAfee SaaS Email Archiving

Reliable, in-the-cloud email archiving with your choice of one or multiple years of message retention

Archiving & Document Compliance

McAfee SaaS Email Archiving offers more than data protection for employees and management. It also supports industry and regulatory retention and compliance requirements. Whether you need to recover a stored email message in response to an e-discovery request, to demonstrate compliance, or simply as an accurate record of "who said what to whom," you want to produce the message as quickly as possible.

With McAfee SaaS Email Archiving, you can easily access one message—or thousands of messages— in seconds, using either simple or advanced search criteria, including user, date range, metadata, message content, and even attachment content. You can also save multiple searches to simplify the task of documenting compliance over time.

Complete Set of Compliance Features

Today's strict compliance requirements often go far beyond document retention and retrieval, McAfee SaaS Email Archiving provides a complete set of compliance features, including:

- Tamperproof read-only storage—Messages and message metadata are protected in their original state
- Dual data centers—Eliminates the threat of a single point of failure, ensuring that no message is ever lost
- Automatic quality verification—Verifies that stored message copies are identical to the originals
- Dual commit message capture—Messages aren't deleted from your email server until accurate copies have been made and verified
- Auditable message serialization—Adds a unique numeric identifier to each message to comply with SEC requirements that prohibit tampering or deletion of messages
- Transport and storage encryption—Messages are transported securely via TLS or SSL, and are stored using 256-bit encryption

Bring Your Historical Data Onboard

Archiving your email in one location makes it easier to search and retrieve all relevant data quickly when you need it.

Businesses with large historical mail store can transfer their data more efficiently with our custom email services. We provide you a secure offline method for transferring historical data for priority import, which offers several advantages to businesses with very large historical mail stores. Our archiving solution:

- Doesn't impact Internet bandwidth
- Eliminates the need to load historical data onto an Exchange server for online import
- Automatically de-duplicates data using an MD5 checksum process
- Includes a dedicated portable hard drive and all other features needed to securely execute the transfer

COMPLETE SECURITY SUITE

- Bundle together McAfee Email Protection Archiving, Continuity, and Web Protection for a complete suite. Manage your account from one overall administrative dashboard

McAfee SaaS Email Encryption Service

Security-as-a-Service protects your classified data

McAfee® SaaS Email Encryption Service safeguards your confidential data and enables you to maintain compliance with regulations requiring encryption of sensitive data. A cloud-based solution, McAfee SaaS Email Encryption delivers unparalleled scalability, eliminates the burden of managing a solution, and empowers your mobile workforce to send and receive encrypted emails ubiquitously from any email client. And, with advanced pre-built data loss prevention (DLP) rules and advanced content scanning, establishing and enforcing policies are easier than ever before.

The irony of email is that it's so critical yet so vulnerable. With one innocent click, years of product research, valuable intellectual property, and billions of dollars in account data can be lost through a simple email message.

With today's online and mobile society, confidential data is always on the move and always at risk. Mitigate the risks by encrypting your mail messages with McAfee SaaS Email Encryption. Our Security-as-a-Service solution helps organizations protect valuable information easily and economically, maintain a stronger business, and comply with privacy regulations.

Why McAfee Email Encryption?

- No hardware/software to install or manage
- No key management
- No upfront capital outlay
- No setup or upgrade fees
- Unlimited encryption
- ISO 27001 certified data centers

Secure Your Email Communications Easily

Protect your confidential outbound email without disrupting the day-to-day workflow of your employees with McAfee SaaS Email Encryption. The simple, cloud-based encryption secures confidential information delivery and helps your organization:

- Encrypt outgoing email with minimal administration
- Ensure compliance with data privacy and retention regulations
- Integrate data loss prevention strategies

Avoid Severe Consequences

The consequences of innocently forwarding confidential information can be severe—from significant fines to substantial business losses. You can avoid these consequences by implementing the document registration features of McAfee to fingerprint and monitor the movement of critical files without any upfront investment in additional hardware or software to:

- Scale to meet the needs of your business
- Keep your workforce agile; send and receive encrypted messages ubiquitously from any email client, including mobile devices

PRE-BUILT DATA LOSS PREVENTION (DLP)

Advanced prebuilt DLP rules help businesses comply with industry and government legislation, including, but not limited to:

- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standards (PCI DSS)
- EU Data Privacy Protection Directive

McAfee SaaS Email Encryption Service

Security-as-a-Service protects your classified data

Email Encryption Technology Made Simple

McAfee SaaS Email Encryption is built with trusted and proven standards-based encryption technologies. It removes the difficulty of installing and managing current solutions and is easy to use. Encryption technologies used include: PKI, S/MIME, X.509 certificates (including the ability to enforce certificate authorities), 3DES, AES-256, and 1024- bit RSA keys (with MDS and SHA-1 encryption algorithms). The encrypted message web portal utilizes 128-bit secure sockets layer (SSL).

DID YOU KNOW?

"Email is the second most common source of data leakage-storage behind portable storage."
—Forrester Research

"One in five outgoing emails contains content that poses a legal, financial, or regulatory risk."
—Forrester Research

Another Critical Layer of Protection

At McAfee, our philosophy is that a layered approach to email and network protection is the most secure and effective. McAfee SaaS Email Protection is the foundation required for McAfee SaaS Email Encryption.

McAfee SaaS Email Protection is a cloud-based service that prevents inbound and outbound email threats from impacting your network and end users:

- Your email network is safe—We block billions of spam, viruses, worms, and phishing threats from our customers' business environments every month
- Your employees are more productive—Our service effectively blocks more than 99 percent of spam with industry-leading low false positive rates
- You automatically filter outbound email—It's just as important to filter what goes out as what comes in. McAfee SaaS Email Protection provides outbound content filtering, protecting your business from malicious or accidental loss of sensitive data. The addition of McAfee SaaS Email Encryption further protects your data via deep content inspection as it travels between sender and receiver in the open Internet.
- You can focus on more priority projects— Because the solutions are fully maintained by McAfee, you can keep your IT staff focused on strategic projects to drive your business forward

McAfee SaaS Web Protection

Comprehensive cloud-based web security for a safe, secure network

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. By applying advanced data correlation and the most extensive threat data available updated 24/7 by McAfee® Global Threat Intelligence™, McAfee SaaS Web Protection offers easy, feature-rich, vital defenses against dynamic web-based malware attacks. Managed by McAfee professionals in web and cloud security and leveraging best web security practices, McAfee SaaS Web Protection helps you gain effective and economical control over threats and undesired Internet access.

Why McAfee?

- **Reduces capital requirements**, ongoing expenses, and maintenance time, enabling IT to focus on business-enabling projects
- **Real-time scanning** of web content to defend against both known and unknown threats
- Seamless and automatic enforcement of policies that can leverage user **synchronization with Active Directory**
- **Reduces bandwidth** requirements and **improves throughput**
- Customized rules based on employee needs and requirements
- Dynamic query engine with the **ability to export data** for use in external business intelligence tools and records management systems

Complete Inbound & Outbound Protection

McAfee SaaS Web Protection secures all aspects of Web 2.0 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. It provides immediate protection against malware and other exploits by stripping out the threatening aspects and delivering the safe content so users can continue to get to the information they need to complete their tasks.

Automatic Protection Updated in Real Time

Websites and content change frequently, and cybercriminals have learned how to disguise their locations and actions. Traditional static URL blocking isn't enough. The McAfee Global Threat Intelligence network collects real-time data from more than 100 million sensors in more than 120 countries and correlates activities across key threat vectors, including email, web, vulnerabilities, and host and network intrusions. With hundreds of dedicated threat researchers, McAfee Labs develops advanced analytics and reputation services to infer intent and risk and protect you from the latest threats.

FEATURES & BENEFITS

- Continuous updates protect the whole network, even roaming users, against fast-changing malware, spyware, and phishing.
- 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.
- Substitutes a predictable, seamlessly scalable subscription for escalating on-premises capital equipment costs and staffing demands.
- Replaces uncertainty with proven protection: McAfee SaaS Web Protection already safeguards web usage for thousands of customers and hundreds of thousands of users.
- Robust protection: in North America, spam URLs make up 41 percent of all web threats, followed by malicious sites and suspected malicious sites.

McAfee SaaS Web Protection

Comprehensive cloud-based web security for a safe, secure network

Content Analysis Detects Changing Malware

Malware on websites can download silently to unsuspecting visitor machines, resulting in keyloggers that "phone home" with logins and customer data, or a zombie that joins a global botnet. By scanning a web page's active content and understanding its intent or predicted behavior, we proactively protect against unknown malware, blended threats, phishing sites, and targeted attacks. We can also strip out objectionable or regulated content, such as pornography.

Flexible Control Based on Category & User

Categories make it easy to set policies against offensive, undesired, and unproductive use of the web. With approximately 100 categories to choose from, our web filtering is unmatched in flexibility, accuracy, and security. It provides easy control over inappropriate Internet use that saps productivity and can present legal liability. In addition, categories can be matched to content and user communities for more targeted control. For instance, bandwidth-intensive video-sharing sites might be blocked during peak business hours for everyone except the marketing staff. Customer care teams can be allowed to access news and shopping sites—but not gambling portals—during the lunch hour.

Savings Are Standard with Web Security

In addition to the savings gained by using our proactive control to strip malware and restrict risky sites, you will reduce the costs and IT overhead associated with clean-up and replacement of infected PCs. Surfing and access controls also free up network bandwidth for legitimate work, putting off network upgrades while reducing time-wasting online activities by employees.

FEATURES & BENEFITS

- Continuous updates protect the whole network, even roaming users, against fast-changing malware, spyware, and phishing.
- 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.
- Substitutes a predictable, seamlessly scalable subscription for escalating on-premises capital equipment costs and staffing demands.
- Replaces uncertainty with proven protection: McAfee SaaS Web Protection already safeguards web usage for thousands of customers and hundreds of thousands of users.
- Robust protection: in North America, spam URLs make up 41 percent of all web threats, followed by malicious sites and suspected malicious sites.

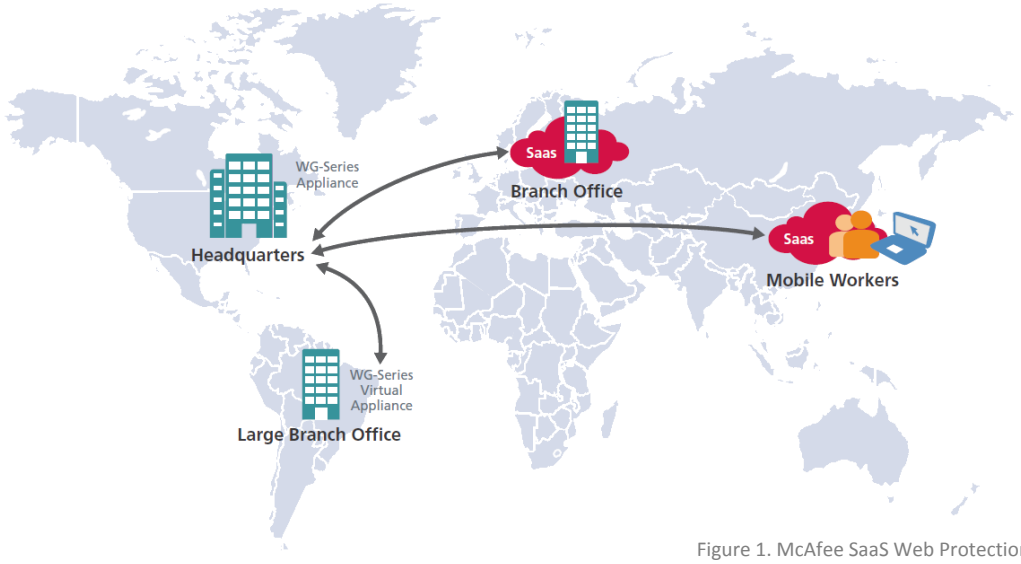


Figure 1. McAfee SaaS Web Protection at work

zixcorp®

What is ZixCorp Email Encryption?

ZixCorp is the leading provider of policy-based email encryption as a service for privacy and regulatory compliance.

As the largest hosted email encryption service provider, ZixCorp protects millions of email addresses, including those of some of the nation's most influential institutions. This easy-to-use service connects organizations with their customers and partners to protect and deliver sensitive information in healthcare, finance, insurance and government.

Features & Benefits

- **Ability to send secure email to anyone**
- Built-in content scanning
- No training for end users
- No software to install
- Policy management for regulatory compliance
- Automatic retrieval and distribution of encryption keys
- Full content scanning of subject line, messages and attachments
- S/MIME, OpenPGP and TLS support

ZixGateway

ZixGateway provides a secure and private channel for email communications between an organization and its customers and business partners. With ZixGateway, companies leverage the policy-based email encryption to **automatically scan outbound emails** for sensitive information, preventing security breaches caused by user errors and **meeting compliance requirements**. ZixGateway is the only enterprise email encryption solution to offer fully transparent email communication for the sender and recipient. When a ZixGateway customer sends encrypted email to another ZixGateway customer, the email is delivered securely without any additional effort from the sender or the recipient.

ZixGateway provides company-wide security with automatic content filtering and management of outbound corporate email. ZixGateway automatically encrypts sensitive data and determines the most efficient way to deliver messages using the **ZixCorp Best Method of Delivery.**

Requirements & More Information

You must have the ability to redirect your outbound mail to use ZixCorp Email Encryption. It is also required to have a version of Google Message Security & Compliance Solution (Postini) to use ZixCorp Email Encryption. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

ZixDirectory

ZixCorp's unmatched Email Encryption Service allows customers to **communicate seamlessly and securely**. Each ZixCorp customer is enrolled in the ZixDirectory, our global repository with more than **23 million members.** With ZixDirectory, customers eliminate the need to build their own directory of encryption keys to communicate securely with their partners and customers. ZixCorp's Email Encryption Service is easy-to-use and is the leading encryption service in the industry today.

ZixCorp provides email encryption services to WellPoint, Humana, the US Securities and Exchange Commissions (SEC), and more than 1,200 hospitals and 1,300 financial institutes.

SAS 70 Type II CERTIFIED · SysTrust · PCI DSS COMPLIANT

zix partner

EXCEL micro

IRONPORT®

What is IronPort Email Encryption?

Cisco IronPort Email Encryption overcomes the problems of earlier encryption technologies by providing a solution that meets compliance requirements for email encryption, while delivering powerful new email control features. The advanced technology allows organizations to improve their security and transparently protect users from the latest Internet threats.

Cisco takes the burden out of encryption key management through a hosted key management service. The Cisco Registered Envelope Service provides secure and transparent management of encryption key creation, distribution, and retention. Operating from multiple Cisco data centers, this service has high availability and 10-year key retention.

Cisco IronPort Email Encryption technology revolutionizes email encryption – satisfying compliance requirements while providing opportunity to extend into areas that can add tangible business value. Cisco provides the only email encryption technology that combines universal accessibility (send and receive on any email platform) with ease-of-use (no client software or PKI), and is proven in mission-critical deployments of up to 30 million recipients.

POWERFUL EMAIL CONTROL

Flexible Sender Encryption
The sender can initiate encryption through a wide variety of means, including installing an email client plug-in that allows them to encrypt a message with the click of a button, marking the message as urgent, or using a keyword (such as "encrypt") in the subject line. Emails can also be encrypted automatically through administrator-configured policies or Lexicons.

Support for All Email Platforms
Messages encrypted using Cisco IronPort Email Encryption can be opened by any AOL, Yahoo!, Gmail, or Hotmail user, as well as by traditional enterprise email clients such as Outlook, Lotus Notes, and Groupwise.

SAS 70 Type II CERTIFIED

Features & Benefits

- Administrator Configured Policies (lexicons)
- Keywords or Phrases
- Email Client Plug-In (encryption on-demand)
- Meet regulatory requirements such as PCI, HIPAA, SOX, GLBA, as well as state privacy regulations and European directives.
- No training for end users
- No software to install

Opportunistic TLS

Servers attempt to negotiate a TLS connection with recipient servers but resort to a non-TLS connection if they are unable to make a secured TLS connection. If they are able to establish a TLS connection message are sent completely encrypted but arrive in the recipient's inbox in plain text with no further action needed to decrypt.

Requirements & More Information

You must have the ability to redirect your outbound mail to use ZixCorp Email Encryption. It is also required to have a version of Google Message Security & Compliance Solution (Postini) to use ZixCorp Email Encryption. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

EXCEL micro

workstream™ by yousendit

What is Workstream?

Workstream by YouSendIt simplifies the way businesses manage and share content online. Workstream provides the first business content collaboration service to offer a secure and integrated approach for sending, sharing, storing and signing files online. Workstream meets and exceeds IT's mandate for security that is often missing from many cloud-based collaboration alternatives. Secure, easy-to-use, and accessible from anywhere on nearly any device, Workstream enables your company to be more productive and reduce costs associated with collaborating. By tightly integrating with the most commonly used productivity applications, business users send, share and access files with the ease of email. Workstream allows organizations of any size to collaborate easily, intuitively and instantly.

- Improve Business & Tem Performance
- No email bounce backs
- Eliminate the need to FedEx or even FTP sites
- Eliminate faxing, printing, and scanning by using e-signatures
- Reduce costs by eliminating FTP Servers and reduce your email and server storage costs.
- No additional hardware, software or maintenance.
- Improve security with access permissions and policies and file expiration settings

Access Anytime Anywhere

You can send a receive files securely anywhere you have an internet connection. Workstream will also sync your desktop folder with your mobile devices automatically.

YouSendIt Express

YouSendIt Express is a desktop application that gives you the ability send files without having to use an email client or the web interface.

Outlook Plugin

Outlook users have the ability to install a plugin which will give you the choice to send a file using Workstream anytime.

More Information

For more information on the different editions of Workstream by YouSendIt and which is best for your company, contact Excel Micro anytime at 877-466-7726 or email us at sales@excelmicro.com.

Meets Your Needs

- **Do you share large files with co-workers, customers, and vendors?**
  - Workstream makes it easy to upload content and share with others.
- **Do you send large files and get bounce backs because of email size limits?**
  - With Workstream you can upload files and folders up to 2GB.
- **Are you email server costs increasing?**
  - By offloading your large files to Workstream you will reduce your server costs and will free up IT.
- **Do you need contracts signed on the road and don't have access to a printer, fax machine, or scanner?**
  - With the e-signature feature of Workstream you can sign docs directly on your computer or mobile device.

Real-Time Logging & Reporting

Workstream will give you the control to track any file you send to a recipient. You can see when the file was opened, updated, and synced to your folder. Administrator can also set files to expire after a certain amount of days or number of times the document can be downloaded.

EXM CONTINUITY

What is EXM Email Continuity?

Email continuity guarantees you that you will have 24x7x365 instant access to your email, even during a server outage. All inbound emails that you receive are stored on our backup server so in the event of a server outage, you will have a webmail portal that you can log into and send & receive new emails. As soon as your primary server comes back online, all new emails that were received during the outage event will sync up with your server so that all received emails will be available on your primary server. Continuity will work with most email environments. It is always on, always current & you will not lose productivity while your primary server is offline.

EXM Email Continuity Allows You To...

- Develop a complete email continuity and disaster recovery solution for your organization
- Maintain constant email access for users round the clock, even if your Exchange server is not available
- Minimize the risk of data loss due to on-premise server failures

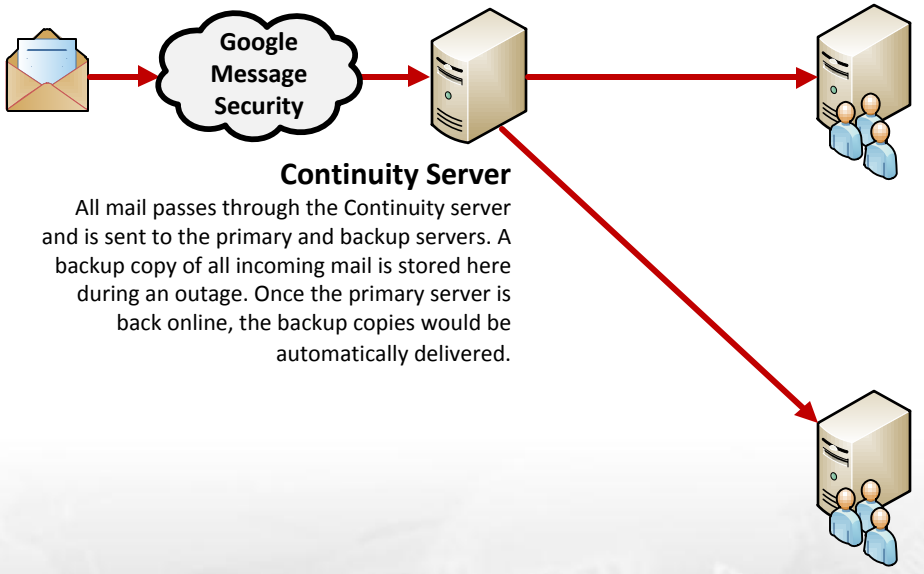
AVAILABLE EDITIONS

Enterprise Edition

Enterprise Edition of email continuity will give you the same functionality as the Standard Edition, but it will also give you 20 days of email retention on the backup server. During a server outage you will be able to access the previous 20 days worth of received emails on the backup server. All emails are purged from the backup server 20 days from the date received.

Standard Edition

Standard Edition of email continuity will give you 24/7/365 access to your email during a server outage. Email will only be stored on the backup server while your server is offline. As soon as your server comes back online, all new received emails will sync with your server and be purged from the backup server.



Continuity Server

All mail passes through the Continuity server and is sent to the primary and backup servers. A backup copy of all incoming mail is stored here during an outage. Once the primary server is back online, the backup copies would be automatically delivered.

Primary Mail Server

While your server is online, all emails bypass queuing server and are delivered to your primary mail server.

Backup Server

When your server is down, you will log onto this server to send and receive new emails.

Requirements & More Information

Excel Micro's EXM Email Continuity requires either a Google Message Security or Google Message Discovery account. Contact Excel Micro anytime to activate a free full functioning trial at 877-466-7726 or email us at sales@excelmicro.com.

Contact Us

www.ExcelMicro.com – Visit us on the web anytime for product information, our live webinar schedule, and to see what is new and exciting at Excel Micro.

www.MSPSupport.com – Our Resource Website with; Product Information, Screenshots, Datasheets, & Demo Logins.

https://Portal.ExcelMicro.com – Our Partner Portal where you can view Actual Usage Reports, Agreement Details, & Place New Orders.

www.twitter.com/ExcelMicro – Follow Us on Twitter for industry news, product updates, and promotions.

www.linkedin.com/in/excelmicro – Join our network on LinkedIn.

Sales Department
sales@excelmicro.com
877-4No-Spam (466-7726) ext. 6300

Support Department
support@excelmicro.com
877-4No-Spam (466-7726) ext. 6400

Marketing Department
news@excelmicro.com
877-4No-Spam (466-7726) ext. 6320

Billing Department
billing@excelmicro.com
877-4No-Spam (466-7726) ext. 6500