SECURE CLOUD-BASED COMMUNICATIONS

Manage risk while embracing cloud services
Manage risk while embracing cloud services

The Situation

Use of the cloud for business-critical services continues to increase as corporate and government networks de-perimeterize. We now tunnel nearly all traffic over port 80. Our services edge is extending to every possible type of virtual and small form factor device. This migration is changing our security paradigm.

“The Cloud” is roughly defined as the services being delivered from remote sites, and the infrastructure that runs these services. Whether a public, private, hybrid, or community cloud, the physical location of the devices—endpoints, servers, storage, routers, security systems—that we interact with has moved. When our security universe relies on interactions with devices we don’t own, the puzzle of risk management is confounded.

Driving Concerns

The hallmark characteristics of Cloud Computing—multi-tenancy, autonomous and ubiquitous access on demand, and broad availability to and from any standard web-enabled device—make the role of the IT security professional almost impossibly difficult. When a business unit can use a corporate credit card to enroll itself in cloud storage applications in five minutes, it is not always possible to even determine the entire list of cloud providers your company is using!

Cloud services come together in ways that stretch our existing protection technologies: email messages can contain HTML elements and links to URLs, and websites like Gmail and Yahoo are also messaging portals. Any data loss reporting capability must incorporate both of these vectors to be useful. Protections for any of these areas fail if unauthorized users are granted access to sensitive data via correct access controls incorrectly applied. Protections must be comprehensive and operate enlightened to the way we use technology today.

What factors do risk management professionals need to consider in looking at managing cloud communication risk? Some of them are:

- **Compliance.** Compliance is complex, and the costs are significant, for many reasons. The laws governing cloud computing are evolving; data flows quickly and easily across political borders; and eDiscovery is hindered when the consumer of a web service has no physical access to the system that houses the data. When a court order stipulates furnishing email or other data, it might not be possible for an IT administrator to produce the data if cloud services were involved. This failure could happen because cloud provider contracts do not always define data portability, and cloud products do not always make data extraction simple.

  Government organizations share with each other in varied amounts, and companies offering cloud services cooperate with government data requests in varied amounts. And the Internet has of course enabled even small and medium-sized businesses to be global organizations. All these dynamic issues and players make understanding and implementing a cloud services compliance strategy very difficult—and almost guarantee you will have to review and refresh terms and conditions annually.

- **Identity and access management.** Before moving key data into the cloud, you need to ensure that your control framework does not break in the cloud. The authentication and identity services used on your corporate network may not use Internet routable protocols and additional authentication factors may be relevant for the cloud. Your team may lack the necessary skills to effectively and securely employ Security Assertion Markup Language (SAML) and other measures present in many cloud resources today. You may have to embrace Open ID, federate your identity beyond your physical perimeter, and manage credential brokering to third parties from a centralized point. You will have to rely on your provider to correctly manage role-based access to resources. When an employee leaves,
Understanding these concerns is central to managing the risk cloud computing introduces, but also harnessing its opportunities and potential benefits.

Solution Description
Extracting organizational value out of the cloud without expanding the risk surface requires excellent coordination, and a holistic collection of people, process, and technology. Cloud-based communications include a complex web of ports and protocols, but typically at least 85 percent of the traffic flowing in and out of an organization is web and email. So start there! Getting a handle on cloud computing begins with knowing your data and ensuring that your fabric of existing IT security controls extends well into cloud models. Once you identify your data, plan your cloud use deliberately, and define what acceptable use looks like. It is essential to put the correct users in contact with the authorized data in explicit ways. Plan carefully, balance scrutiny with risk exposure, and circle back for audit and review often. Technologies evolve quickly and so do the needs of the business. These steps can help secure your bridge to the cloud.

Key requirements for securing cloud-based communications include:

- **Compliance.** Know your data. Understand your regulatory implications. Monitor your email and web-based communications with content inspection, watching for HIPAA, PCI, or SOX-implicated data exfiltration like authorization data, financial performance disclosure, or PI. Enforcing a policy that ensures the auditors will be happy means mapping control statements to web and mail filtering policies. It is counterintuitive, but sometimes it is easier to prove compliance to auditor-approved levels when a third party houses the data, and all interactions with it are logged by the cloud service provider. Audit trail and file integrity have built in assurance with cloud applications.

Sometimes the biggest job of a risk manager is simply documenting the risk exposure! While not an easy task, if a complete catalog of websites visited by the organization can be built, a complete list of cloud service providers in use by the company can be built. Explore opportunities for cloud services to reduce the complexity or costs of compliance. Just getting all the data into one place is the first step of supporting a subpoena and in most cases automatically part of a cloud service by design.

- **Identity and access management.** When data is moving outside the company’s four physical walls, the authorization framework used inside the company for access control needs to operate outside the company’s physical perimeter as well. This coverage will enable secure use of the data. A central identity service that allows portability and facilitates secure connections to business partners is becoming a business imperative. Many data sharing relationships between enterprises and cloud providers are starting to support data tokenization, encryption, and single-sign-on capabilities. Ensure identity transactions are brokered securely, authentication controls in place are adequate, and data is published only to properly authenticated actors.

- **Availability.** Architecture changes of any sort affect resource availability and uptime expectations. It’s important to evaluate the uptime performance of cloud providers. It’s also valuable to consider ways cloud models can increase availability. Multi-tenancy usually makes it easier for you to leverage cloud services to meet your business requirements for resilience, availability, and scale. For example, cloud mail filters will typically buffer inbound message flows if a mail server becomes unavailable. This service could be useful in ensuring email delivery if you need to bring down your email server for maintenance.
The cloud can help both services and data to be more available. Especially important for data that must be retained for long periods or processed for eDiscovery, the data archived in clouds—including archived email traffic—is often more highly available and easily searched than locally stored data.

- **Incident response.** Cloud models can lower the risk of infection by protecting web and email traffic vectors from malware. When you are infected or attacked, the logging performed by most cloud applications can be an effective tool in forensic investigations and incident response. Make sure the right data is logged and available to you without elaborate processes or paper trails.

**Technologies Used in the McAfee Solution**

Any security ecosystem is only as strong as the weakest link; a comprehensive approach is needed. The best way to start managing cloud-enabled risks is to evaluate your exposure at your network gateway, your first connection to the cloud. Design logical controls and mechanisms to extend your existing processes past the physical gateway. By thinking through the issues that create risks, you will be in a strong position to identify the concerns that matter to your business, specify relevant responses, and get the implementation support required from both cloud providers and your business unit partners.

Most networks interact with the cloud through email, web, and identity services. Properly securing these routes is a strong starting point. The number one priorities of the security team should be preventing content leakage, protecting against exposure to service interruption, minimizing the risk surface as identity services are exposed beyond the physical network boundary, and maintaining your resilience to malware and web-borne threats.

Securely brokering identity and managing authorizations is a business imperative. While most of us remember the failures of PKI from the early ‘90s, it is broadly accepted that now is the time to build a layer for authentication and rights management to external services.

McAfee helps you establish a framework to securely communicate identity to external parties and manage correct provisioning of user accounts. The McAfee® Cloud Identity Manager centrally brokers identity and secures identity validation transactions. Authentications to external sites are tokenized and securely brokered, prohibiting identity leaks and data loss that occur through legitimately authorized but illicit access. Users gain a simplified login experience for external sites, while the solution adds a credential management capability to the security team’s tool chest. If the entire set of company credentials needed a refresh because the provider had a breach, no user interaction at all would be required to establish a new service password for each web service used. McAfee Identity Manager would process these requests.

McAfee offers reinforcing protections layered at each service tier to help you ensure sufficient and appropriate protection. Our web and email protections include all the deployment options you need: on-premises, virtual, in the cloud, or any hybrid combination. With this flexibility, you can move to the cloud as quickly or painstakingly as you prefer, or architect a mix of systems that offers the ideal combination of control, flexibility, and cost savings.

The first layer to consider is content security at your “gateway,” which could be an appliance on your site or a SaaS-based service in the cloud, or layers in both places. McAfee helps secure your gateway with network-level protection for web traffic, email services, and content inspection (data loss prevention) across both channels.

McAfee leverages cloud-based intelligence from many McAfee products to bi-directionally share the latest breaking threat and protection information, as part of the McAfee Global Threat Intelligence™ (GTI) fabric. Threat protections are more complete when nodes reference the most current information in the cloud, and compare details on threats with other nodes. While GTI is not a product, it is an enabling piece of many McAfee products, including the web and email protections described below.
McAfee can help you extend email, web, and identity services to take full advantage of the cloud.

These essential gateway systems protect against inbound malicious content and spam and help you manage outbound content to match business use and compliance requirements. With this baseline in place, you can focus on the communication paths, isolate typical use cases, and extend your security systems and policies across the broad, cloud-enabled business and compliance ecosystem.

Where you already have on-premises gateway protections in place, look for opportunities to save money or increase security using cloud services. A popular use case is moving spam filtering to a SaaS model. With 85 percent or more of worldwide message volume being unwanted, removing spam in the cloud before it consumes corporate Internet bandwidth, power, or disk space becomes very attractive economically. Spam filtration is also an ideal cloud service because it can be filtered based on reputations and malware, areas where experts and automation are crucial factors. Implementation is simple, as well, by redirecting traffic at the gateway.

Similarly, a popular use case for SaaS web filtering is rapid protection of a network after an acquisition event. Basic policy-based protection can be enabled for an acquired company in minimal time. Another common service offers protection for mobile users, who are the front line for experiencing malware infection and bringing these infections onto the corporate network.

Below are the specific solutions that will help you achieve the flexibility and control you need as you move into the cloud at your pace.

**McAfee Cloud Identity Manager**
McAfee Cloud Identity Manager relieves the pain that end users experience managing multiple passwords for cloud applications. Cloud Identity Manager, a gateway appliance, is a simple to deploy framework for building and managing authorization services for these cloud application connections.
It allows you to enforce corporate standards for cloud application access and improves productivity for IT and end users by relieving password reset requests.

This solution gives you control over the cloud access security lifecycle. Cloud Identity Manager provides single sign-on (SSO), automated provisioning, strong authentication, authorization, and consolidated auditing. We provide plug-and-play cloud connectors for out-of-the-box integration with popular cloud-based applications, including Salesforce.com and Google Apps. No coding or separate purchases of toolkits required. Simply pick your cloud application from the console menu and you are ready to go. Quick implementation means a better return on your investment and a faster time to value.

**McAfee Web Protection**

HTTP is the cornerstone protocol of the Internet and the primary mechanism of user interaction with remote entities. Most end-user enabled cloud applications use web browsers to enable customer interactions.

McAfee Web Protection solutions—enabled as on-premises or VMware appliances, SaaS services, or your preferred hybrid combination—help improve your cloud services compliance posture by ensuring http and https dialogs with remote sites and applications are correctly logged and policy enforced, while risky content is blocked. Non-compliant and unauthorized data use is blocked by web gateway protections (either at your site or at our hosting facility), even when a user attempts to post the information to a micro-blogging site like Twitter.

Advanced filtering of web traffic for security threats keeps Trojans and other malware off user devices to preserve system availability. The powerful combination of both reputation and category-based filtering from McAfee Global Threat Intelligence (GTI) powers McAfee Web Protection’s web filtering technologies. McAfee GTI creates a profile of all Internet entities—websites, email, and IP addresses—based on hundreds of different attributes gathered from the massive, global data collection capabilities of McAfee Labs. It then assigns a reputation score based on the security risk posed, enabling administrators to apply very granular rules about what to permit or deny—and continues to monitor those entities over time.

McAfee Web Protection includes proactive, behavioral analysis that opens content in real time for deep inspection and intent analysis. By scanning a web page’s active content, emulating and understanding its behavior, and predicting its intent, McAfee Web Protection proactively protects against zero-day and targeted attacks as they occur. Real-time lookups to the McAfee Global Threat Intelligence file reputation service allows McAfee technology to close the gap between virus discovery and signatures being available.

McAfee Web Protection customers can take advantage of McAfee SiteAdvisor® Enterprise software with Web Filtering for Endpoint, included in McAfee Web Protection, to both protect and control web access for mobile users. This integrated, gateway-aware solution intelligently enforces the appropriate policy, whether the end user is at a corporate office and behind an on-premises solution or outside the network.

Web protections also provide valuable log data to support forensic investigations and incident response. Much of what a user does on the host is ultimately recorded in their Internet and web communications, which McAfee gateway protections can capture and report.

The integrated McAfee Web Reporter aggregates data, regardless of delivery platform. It provides instant information and forensic tools to illuminate how organizations use the web, helping to comply with regulations, identify trends, isolate problems, document inappropriate web activity, and tailor filtering settings to best enforce web usage policies.
McAfee Email Protection

Protecting your users from malicious elements also requires protecting email, the other widely open gateway from your organization to the Internet. Email is fundamentally a cloud service, since it enables remote hosts to exchange messages, so it needs protection. McAfee recommends a security focused mail gateway solution that goes beyond spam protection and truly validates the security posture of email messages, before allowing them to reach the user machine.

Protecting against inbound email based security risks and spam frees hosts from overhead involved in unwanted mail. Filtering out the spam in the cloud also keeps this email from occupying resources and threatening availability of your on-premises email infrastructure. Inspection for malware needs more than a virus scan. McAfee uses reputation and email fingerprinting powered by Global Threat Intelligence (GTI) to detect and block risky email communications. Full file type and media verification help prevent spoofed content from getting through.

McAfee Email Protection includes email continuity services, so that inbound email can be queued and accessed if your email infrastructure is disrupted—for scheduled maintenance or accidental downtime. During this period, users can access and send messages over the web instead. Once service is restored, the email synchronizes message activities.

McAfee also encourages filtering outbound messages. This control is important because sometimes configuration errors allow spam to leave your network. This traffic can make your company look like a spammer, and reputation-based filters will block traffic from your company IP addresses and locations. Your legitimate mail will not get through, and these blocks can affect network availability.

McAfee email protection solutions can also evaluate email and email attachments for sensitive and regulated data. Since audit compliance relies on being able to report on key phrases that are important to SOX and financial reporting, disclosure laws like CA SB1386, and industry and country specific legislation, McAfee email protection solutions include built-in content dictionaries and fingerprinting to help reliably identify confidential data. We also make compliance documentation straightforward to provide the crucial evidence auditors require. The message inspection can look into myriad different attachment types and inspect them for compliance with custom and configurable DLP policies.

For example, an effective compliance control for preventing personally identifiable information (PII) leaks is to configure McAfee email protection layers to identify sensitive information like social security numbers automatically. Based on policy, McAfee Email Protection can perform automated protection actions to quarantine, block, encrypt the message, or send the message content via secure web delivery.

As your email infrastructure includes more cloud services, McAfee recommends having a central capability to report on your global email infrastructure, effectively manage quarantines and notifications, and inspect content for security and content implications. This unified operation will assist with compliance, especially in the event of eDiscovery. Being able to perform effective, timely, and affordable eDiscovery is often a matter of centralizing message stores. McAfee SaaS Email Archiving is an option that will allow you to store and protect your data for up to seven years. Optional SaaS Email Encryption can encrypt cloud email according to policy.

Whether you are looking for email security onsite, in the cloud, or a hybrid of both, McAfee Email Protection delivers email security the way you need it to enable your path to the cloud.

Additional McAfee Cloud Products

- **McAfee SaaS Endpoint Protection.** Block a full range of threats, including viruses, spyware, and hacker attacks. Easily deployed and managed through the web-based McAfee SecurityCenter™, SaaS Endpoint Protection helps to automate endpoint defenses and lower security costs.

- **McAfee SaaS Vulnerability Management.** Quickly activate vulnerability scanning and actionable reporting, helping you to rank risks and gauge compliance against industry standards such as PCI.
Impact of the Solution

Deploying McAfee technologies to secure your cloud based communications will:

• Enable the business to transact business more safely via web and email channels
• Protect your brand with a risk-based approach to considering and selecting cloud services
• Reduce the support cost of mitigating infected host machines
• Reduce audit costs with demonstrable security controls in place
• Protect against data leakage, intellectual property loss, and their legal and revenue implications
• Help demonstrate due care in the event of a breach
• Establish a security review process before clouds are deployed, rather than down the road, lowering costs and eliminating rework
• Enable your business to explore and embrace new options for using the cloud, knowing the business is prepared and the services can be secured

Through predictable user-based subscription pricing, regardless of solution deployment, McAfee web and email security solutions provide the ultimate flexibility. Identity management will help you add on other cloud services while reducing authentication complexity and risks. You can meet your current business requirements and adapt easily as you move forward into greater cloud use—public, private, community, government, and hybrid cloud models.

Additional Resources

www.mcafee.com/cloud-identity-manager
www.mcafee.com/web-protection
www.mcafee.com/email-protection

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author

Quinton Jones leads a solution business development effort for McAfee SaaS products and cloud services. He is engaged in product strategy, business process enablement, training, and evangelism. Quinton is an ardent security professional with 10 years experience designing security architectures, security metrics, security program management, engagement, and project management. He has held roles in business development, sales management, technical account management, audit and advisory, and technical consulting at eEye Digital Security, Qualys, and Breakwater Security Associates.

Quinton speaks at security conferences and briefings on network and application security domain topics. Quinton holds an MBA from the UCLA Anderson School of Management, a BA from the University of Washington, and maintains a CISSP certification. He is involved with University information security curriculum development, is an early adopter of the Cloud Security Alliance CCSK certification, and is a board member of the Source Seattle conference.