



McAfee Cloud Security Platform

Building a secure bridge between the enterprise and the cloud

Build a Secure Bridge to the Cloud

- **Data loss prevention**—Discover and classify data in the organization before it leaves to the cloud. Create and enforce robust policies to secure sensitive data.
- **Identity and access management**—Comprehensive access control for cloud applications using enterprise identities
- **Email security**—Email remains the single biggest source of data leakage. Protect your critical data by securing the incoming and outgoing email traffic that flows through the cloud.
- **Web security**—Whether accessing cloud applications or storing data, secure all web traffic in one place
- **Mobile web security**—McAfee Web Security allows enterprises to extend and enforce their security policies on mobile devices
- **Services gateway**—Offload application-level security and authorization to a gateway at the network edge or in the cloud

“Nine out of 10 businesses cite security as the top obstacle for cloud adoption.”

—IDC

The McAfee® Cloud Security Platform, a key component of the Security Connected framework, helps businesses safely and confidently take advantage of cloud computing by extending and applying their own security practices and policies to data moving to and from the cloud. This suite secures email, web, and identity authentication traffic, leveraging McAfee Global Threat Intelligence™ for real-time protection against the latest threats.

According to industry analysts, the two most common concerns that companies have when considering cloud computing are the possibility of data loss and how to restrict access to information. More simply, how do businesses protect the data they send, receive, or store in the cloud. Also, how do they make sure that only the right people have access to that information?

Although cloud providers do their best to reassure customers, they've failed to help businesses fully overcome these concerns. As a result, businesses are either forgoing using cloud computing or are building private clouds that minimize the cost and efficiency benefits.

McAfee has taken a unique approach to this problem by securing the data and traffic moving between the business and the cloud. McAfee achieves this through the industry's first and only comprehensive cloud security platform that helps secure the primary forms of cloud traffic: email traffic, web traffic, and authentication traffic.

Of course, cloud traffic is not limited to the data shared from a single entity or headquarters. It also includes the traffic being sent and received by remote offices and on-the-go employees with mobile devices. Therefore, security needs to be everywhere that data is moving, regardless of channel or location.

The McAfee Cloud Security Platform offers a variety of deployment options to cover all workers regardless of location, ranging from traditional on-premises solutions, Software-as-a-Service (SaaS) solutions, and even a hybrid combination of both.

So how does a business go about building a secure bridge to the cloud?

Securing the Cloud Starts with Data

Before even beginning to consider what type of data should or should not be moved to the cloud, a business must first understand what data it has, where it resides—and more importantly, the value or sensitivity of the data. Only when there is a complete inventory of the data, can an organization begin to classify the data to build the appropriate policies to protect it and then enforce policies while data travels both within and outside the organization.

Protecting Primary Cloud Channels

The primary channels of traffic that move data to and from the cloud include:

- Email traffic
- Web traffic (mobile and application services)
- Authentication traffic

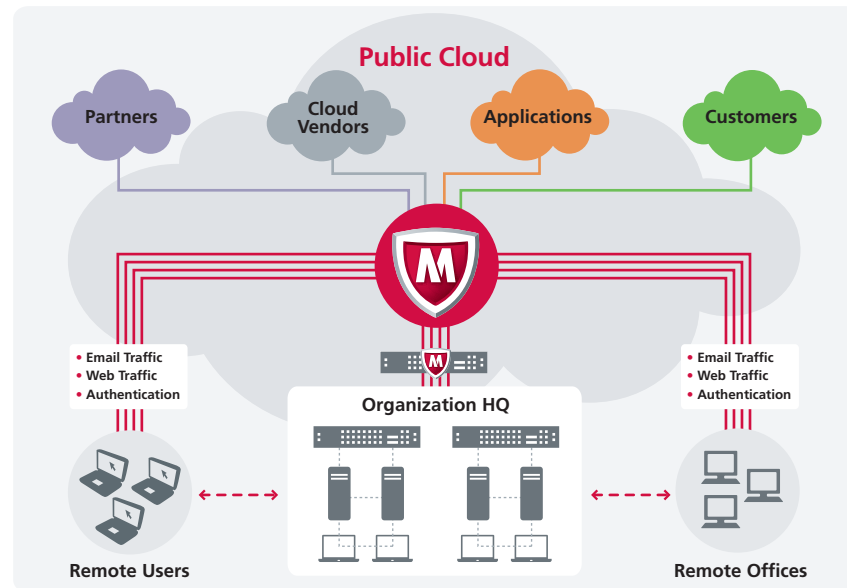


Figure 1. McAfee protects key cloud traffic channels.

This includes all application and protocol data traversing over port 80 or 443, including traffic between social media sites, instant messaging, blogs, and web email.

Securing these channels is vital to protecting both outbound and inbound cloud traffic. Bidirectional controls ensure that your outbound traffic is secure, while also protecting your organization's perimeter from spam, malware, and other cloud-borne threats.

Consolidate with Next-Generation Cloud Protection

The McAfee Cloud Security Platform represents the natural evolution from traditional, disparate email and web security gateways to consolidated cloud gateways, providing a single, integrated solution to manage all data moving between the business and the cloud.

The McAfee Cloud Security platform consists of key products and technologies from McAfee. These solutions help establish consistent controls that work throughout the extended enterprise infrastructure, transparently enforcing security and compliance policies on mobile and remote users as well.

Modular in design, the McAfee Cloud Security Platform allows users to easily consolidate and integrate various protections.

McAfee Cloud Identity Manager

McAfee Cloud Identity Manager enables organizations to provide comprehensive access control for cloud applications using enterprise identities. This solution provides cloud account provisioning, de-provisioning, identity synchronization, single-sign on connectors to common SaaS application, and two-factor authentication using one-time password soft tokens.

Cloud connectivity for applications and data is delivered through SAML, OAuth, OpenID, and XACML standards—all connected to existing identity management infrastructure.

McAfee Data Loss Prevention

McAfee Data Loss Prevention (DLP) delivers data security and unrivaled, actionable insight about data at rest, in motion, and in use across your organization. With non-invasive network technology, McAfee Data Loss Prevention discovers data no matter where it resides or what format it is in, giving the enterprise rich data mining tools to classify data and create effective policies that protect better and more quickly. Organizations leverage centralized management and reporting through McAfee ePolicy Orchestrator® (McAfee ePO™) software.

McAfee Email Protection

McAfee Email Protection delivers total email protection for organizations, integrating comprehensive inbound threat protection with outbound data loss prevention, encryption, robust reporting, and simple administration. McAfee Email Protection helps businesses prevent data leakage through email by leveraging the same McAfee Data Loss Prevention technologies deployed to protect data within the organization. The enterprise can leverage McAfee Email Protection integration with the McAfee ePO platform for centralized management and reporting.

McAfee Web Protection

McAfee Web Protection enables enterprises of all sizes to facilitate secure communications and safe, productive access to business applications—anywhere and from any device. Bidirectional web security protects enterprise users who use a browser to access applications hosted in the cloud. Through proactive reputation- and intent-based protection, it meets the needs of today's evolving threat landscape. McAfee Web Protection also enables enterprises to fine-tune controls over functionality enabled on interactive web applications, exerting policies by application and down to the user level.

McAfee Web Protection also extends security to mobile devices accessing content that is traditionally available on internal corporate servers such as intranets, wikis, Microsoft Sharepoint servers, and other web-based solutions. Smartphones and tablets, including BlackBerry, Apple iPhone, Apple iPad, and Android, can direct web traffic to McAfee Web Security solutions through standard device management and security controls, ensuring that mobile devices are secured with advanced anti-malware protection and corporate web filtering policies.

McAfee Services Gateway

McAfee Services Gateway provides a layer of security, control, and management for application-to-application traffic. McAfee Services Gateway offloads application programming interface (API) security, data transformation, representational state transfer (REST) to simple object access protocol (SOAP) mediation, and identity token exchange to a high-speed gateway at the network edge or in the cloud. McAfee Services Gateway simplifies services delivery, acting as a proxy that offloads security policy enforcement from applications. It accelerates, secures, integrates, and routes legacy data within a single, easy-to-manage software appliance.

Real-Time Protection with McAfee Global Threat Intelligence

The McAfee Cloud Security Platform leverages McAfee Global Threat Intelligence, providing real-time protection against known and emerging threats. With visibility across all key threat vectors—file, web, email, and network—and a view into the latest vulnerabilities across the IT industry, McAfee correlates real-world data collected from millions of sensors around the globe to deliver the most comprehensive protection in the market.



On-Premises, SaaS, or Hybrid

Because security needs vary greatly, the McAfee Cloud Security Platform is form factor agnostic. Businesses have the freedom to deploy their cloud security as an on-premises solution, SaaS, or a combination of both. Customers are also free to transition between form factors as their business or security needs change.

An Open Platform for Freedom with Control

McAfee Cloud Security Platform is modular by design and leverages McAfee ePO software for management and reporting. The open architecture and the built in APIs of McAfee ePO allows customers and partners to add on complementary security services and solutions to the McAfee Cloud Security Platform.

Easy to Buy

McAfee Cloud Security platform is easy to buy and license. All solutions can be purchased on a subscription basis, allowing organizations to mix SaaS and on-premises deployment options.

