SOLUTION BRIEF

McAfee
Together is power.

Secure Corporate Cloud Environments

Cloud Security that Accelerates Your Business

Enterprises leverage the cloud in multiple ways, ranging from off-the-shelf Software-as-a-Service (SaaS) applications to workloads that run in Infrastructure-as-a-Service (IaaS) and private cloud environments. Beyond cost savings, a key driver of cloud adoption is the innovation that the cloud enables. The cloud can accelerate business. As a result, the cloud is increasingly the place where data—an organization's most valuable asset—is stored and shared. Securing that information is a shared responsibility between a company and their cloud providers. However, IT leaders continue to emphasize that security concerns are the greatest obstacle preventing their organizations from fully realizing the potential the cloud offers.

Connect With Us

Gartner states that "through 2020, at least 99% of cloud security failures will be the customer's fault".[1] Public cloud providers generally take responsibility for the underlying infrastructure—which leaves customers responsible for a wide range of compliance issues and security threats. Common among those are:

- Uploading of sensitive data that should not be stored in cloud services
- Sharing of sensitive data from the cloud with people who should not have access
- Downloading/syncing of sensitive data from the cloud to insecure, unmanaged devices
- Spread and execution of malware from and within cloud environments
- Access of data by third parties using compromised login credentials
- Intrusions into cloud workloads with the intent to compromise data and disrupt operations
- Misuse of data and cloud resources by malicious or careless employees

Some cloud providers have added limited, native capabilities to help customers deal with these challenges, but they are insufficient in most cases. Even the most mature native security offerings result in a new problem: they create siloes of security requiring teams to configure policies and perform remediation and reporting across each cloud service. Organizations need a central control point for cloud security to address the multitude of cloud environments they use, which span private cloud and public cloud IaaS, PaaS, and SaaS.

McAfee Cloud Security Solutions

McAfee® cloud security solutions protect corporate data, applications, and workloads in today's multicloud environment. The solutions help organizations fulfill their end of the shared responsibility model for the cloud. Specifically, McAfee cloud security solutions help organizations:

1. Understand cloud usage and risk
2. Apply persistent protection to cloud data and workloads
3. Respond to cloud security threats

Across these capabilities, McAfee continuously learns and adapts to evolving cloud risks and behaviors. Together with the native security delivered by cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Microsoft Office 365, McAfee aims to make cloud as secure or more secure than on-premises alternatives. This removes security as a barrier to cloud adoption, enabling organizations to unleash the power of the cloud to transform business.

Understand cloud usage and risk

McAfee cloud security solutions deliver comprehensive visibility into all activity in the cloud, including discovering who uses which cloud services, where sensitive data is stored, who has access, and what threats are present.

- **Identify sensitive or regulated data:** All told, 18.1% of files stored and shared in the cloud are sensitive.[2] They contain payment data, health data, personal data, or confidential corporate data. The McAfee content engine detects and categorizes a wide range of sensitive data

> "The acquisition of Skyhigh Networks by McAfee brings two cloud security leaders together. The integration of their security offerings will provide holistic data visibility, control, and protection for cloud environments while preserving policy enforcement and compliance."
>
> Ivaylo Uzunov, Manager of Information Systems, Carlson Wagonlit Travel

based on keywords, standard data patterns (example: credit card numbers), custom data patterns (example: part numbers), document fingerprints, database fingerprints, and more. You can leverage out-of-the-box policy templates or craft custom policies to match any corporate policy or regulation.

- **Understand access and sharing of sensitive data:** The sharing tools in cloud services that enhance collaboration can also result in data being shared with the wrong people. The McAfee cloud context engine understands granular permissions on files and folders. It discovers users that have access rights, along with their level of access (examples: viewer, editor, owner, and others). When users log in to cloud services, the solution also understands the context of access, including the device type, device management status, user location and network, and the user's role.
- **Discover shadow SaaS and IaaS usage:** Employees today routinely use cloud in ways that are unknown to IT. In fact, the average organization uses 1,427 distinct cloud services. McAfee cloud security solutions discover all cloud services in use by an organization and assign a 1-to-10 risk score to each service based on a 261-point assessment. You can also identify all workloads running in public and private cloud environments. Once known, cloud applications and workloads can be brought under management by IT to ensure they are secured.
- **Audit IaaS security configurations:** Even a single misconfiguration can have serious security ramifications if exploited by an attacker. Recognizing that there are dozens of critical settings for each object (service, instance, container, and others) within infrastructure platforms and, potentially, many thousands of objects, McAfee cloud security solutions audit configurations to discover weaknesses in a security posture. You can then assess a wide range of settings across identity and access management, network configuration, and administrator access that can make organizations vulnerable to attack.
- **Detect user behavior threats:** Enterprises today must contend with malicious or careless employees as well as malicious third parties. The use of cloud amplifies the potential damage of each. Machine learning analyzes user behavior and pinpoints activity that indicates an insider threat (example: an employee taking data to a competitor) along with account compromise that can lead to the theft of sensitive data or exploitation of infrastructure (example: a third party uses employee credentials compromised in a phishing attack to access payment card data).
- **Detect advanced threats:** Today's sophisticated zero-day threats mask their attributes to evade signature-based detection tools increasingly found in cloud environments. McAfee cloud security solutions deliver multilayer detection of malware, whether present in cloud workloads or cloud applications. As a first layer, a scan runs for known malware signatures. Additionally, advanced threat capabilities leverage a combination of sandboxing, dynamic behavioral analysis, and machine learning across the host and network to detect threats that have not been encountered before.

Apply persistent protection to cloud data and workloads

McAfee cloud security solutions take real-time action to protect data, enforcing policies on what data can be stored in the cloud and who can access that data, and apply protection to data that persists inside or outside the cloud.

- **Enforce policies across data stored in the cloud:** For organizations that have internal policies or regulations governing what data is permitted in the cloud, McAfee cloud security solutions can automatically quarantine or remove files that contain sensitive data from cloud services. Security analysts can also choose to manually take remediation action to remove data when reviewing incidents. Finally, user-centric remediation can coach end users after detecting policy incidents and, once the end user removes the sensitive data from the file, it can automatically resolve the alert.
- **Build sharing and collaboration guardrails:** Twenty-one percent of files and folders are accessed within five minutes of being shared from the cloud.[4] Therefore, timely enforcement is critical to preventing inappropriate access. McAfee cloud security solutions enforce sharing policies in real time—before the event is fully executed in the cloud service and an invite sent. You can also enforce sharing controls across pre-existing data already stored in the cloud. The McAfee policy engine can remove a user's access permissions, downgrade permissions (example: from editor to viewer), and revoke shared links.
- **Prevent data movement to insecure, unmanaged devices:** Many organizations want to enable anywhere, anytime access to cloud-based collaboration tools but limit the risk of data being stored on devices that lack corporate security software. McAfee cloud security solutions can enforce controls that allow users to view and collaborate on data within cloud applications but prevent users from downloading data when they access from an unmanaged device. Device management status can be defined using existing endpoint security solutions or device certificates.
- **Encrypt structured data using encryption keys:** Some regulations require that certain types of data—such as payment card data—be encrypted. In these cases, encryption by cloud service providers may be insufficient because the cloud provider has access to the encryption keys. McAfee cloud security solutions enable encryption of data in structured applications using encryption keys under control that are not accessible to the cloud provider. At the same time, authorized users can transparently access encrypted data and perform operations such as search and sort.
- **Apply rights management protection to files:** Files containing certain types of sensitive data may need to be encrypted. McAfee cloud security solutions integrate with information rights management (IRM) solutions to apply IRM protection to files. Policies can be based on the content a file contains, as well as end-user actions, such as downloading the file to a device where it could be shared or forwarded to a third party. Depending on the rights management solution, IRM protection can be used to encrypt files, manage access, and limit end-user functions, such as copy and print.

Respond to cloud security threats

McAfee cloud security solutions respond to cloud threats by proactively strengthening infrastructure configuration, hardening workloads against attack, taking action to mitigate high-risk cloud usage, and stopping malware.

- **Implement defensive measures for workloads:** Workloads running in public or private cloud environments are vulnerable to malware and targeted attacks. McAfee cloud security solutions can whitelist trusted applications that are approved to run on the host while preventing all other code from executing. You can also use network micro-segmentation to limit communication to trusted resources. These capabilities prevent malicious payloads from operating and spreading, whether known or not, thereby hardening workloads in the cloud against sophisticated zero-day threats.
- **Require additional authentication for high-risk access:** In response to high-risk cloud access scenarios, McAfee cloud security solutions can introduce the requirement for a user to authenticate with an additional identity factor in real time. This capability leverages existing identity providers and identity factors already familiar to end users. By confirming the user's identity with another factor, such as a hard token, a mobile phone soft token, or text message, you can significantly reduce the risk of account compromise.
- **Govern shadow cloud usage with closed-loop remediation:** New cloud applications come online frequently, and the risk of cloud services evolves rapidly, making manual cloud policies difficult to create and keep up to date. McAfee cloud security solutions enforce policies based on the 1-to-10 risk rating of a cloud service or any combination of 261 distinct cloud service attributes tracked for each cloud service. The solution integrates with an existing firewall or web gateway to automatically update and enforce policies without disrupting the existing environment.
- **Neutralize and remove malware:** Malware and ransomware can infect workloads running in public and private cloud environments. Cloud-based file sync-and-share applications can also spread malware from one infected user's device to another user's device through a shared folder that syncs automatically. Whether malware is detected on a workload host or in a cloud application, McAfee cloud security solutions quarantine or remove the malware, safeguarding sensitive data from compromise and preventing corruption of data by ransomware.

Adapt to evolving cloud risks

McAfee cloud security solutions continuously adapt and learn as cloud services change, user behavior changes, and as attacks and threats evolve. The solutions proactively adapts to changes in:

- **The risk attributes of cloud services:** McAfee Cloud Service Intelligence continuously tracks and updates 261 risk attributes across thousands of cloud services.
- **Cloud provider APIs and data models:** As cloud providers evolve, McAfee cloud security solutions stay in sync, offering continuous visibility and control over cloud services and applications.

> "We use McAfee® Skyhigh Security Cloud to layer security controls like data loss prevention and access control for Box so that the easy path to collaboration is also the secure path."
>
> Tim Tompkins, Senior Director of Security Innovation, Aetna

- **User behavior patterns:** Machine learning continuously analyzes behavior changes to refine threat detection models.
- **Security analyst input:** As analysts mark false positives or adjust detection sensitivity, supervised machine learning updates behavior models.
- **Threat patterns:** The threat landscape is constantly changing, and McAfee cloud security solutions leverage our Global Threat Intelligence network to stay up to date on the latest threats.

Security for the Entire Cloud

McAfee cloud security solutions deliver comprehensive security for an organization's part of the cloud shared responsibility model, providing complete coverage for all cloud assets.

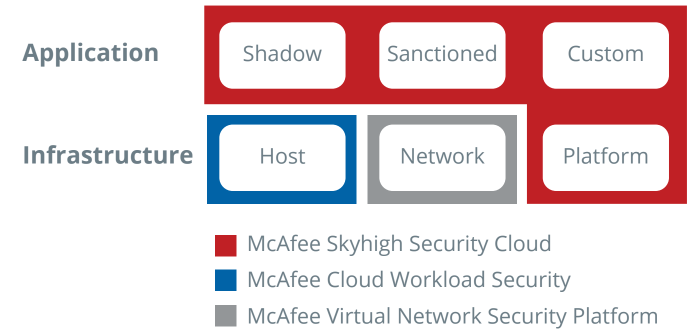
Application
Shadow
Sanctioned
Custom
Infrastructure
Host
Network
Platform
🟥 McAfee Skyhigh Security Cloud
🟦 McAfee Cloud Workload Security
▨ McAfee Virtual Network Security Platform

Figure 1. McAfee cloud security solutions protect all aspects of the cloud—both applications and infrastructure.

McAfee® Skyhigh Security Cloud

- Shadow SaaS applications introduced by employees
- Sanctioned SaaS applications procured by IT
- Custom in-house developed applications that run in the cloud
- IaaS platforms on which hosts and custom applications run

McAfee® Cloud Workload Security

- Hosts that run on private and public IaaS platforms such as VMware, AWS, and Azure

McAfee® Virtual Network Security Platform

- Network traffic going to, from, and between cloud workloads

Learn More

For more information, visit: www.mcafee.com/cloudsecurity.

1. Gartner, Magic Quadrant for Cloud Access Security Brokers, November 30, 2017, Steve Riley, Craig Lawson
2. Skyhigh Cloud Adoption & Risk Report
3. Ibid.
4. Ibid.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com