Cloud Security

By Ian Clements

Introduction
McAfee fully understands the definition of cloud computing and the security implications associated with the cloud model. Security is a priority, and protecting our own operations is key. McAfee works closely with relevant cloud service providers (CSPs) to leverage different service models, best practices, and architecture frameworks.

This document outlines the McAfee approach to cloud security as a cloud customer. It focuses on the security of our organization and the technical controls we have implemented to protect our data and services within multicloud environments.

McAfee and Its Cloud Security Culture

Security training for all employees
McAfee provides an opportunity for all employees to attend in-house or third-party cloud security training. This training enables developers and operational users that interact with cloud resources to gain relevant skill sets and knowledge. Recurring, refresher, and updated training opportunities are made available to all employees. As a security company, we are fully aware of the ever-evolving threat landscape in cloud computing, and we continually transform in order to improve our security posture and raise awareness among all employees. Within the McAfee organization, there are regular Tech Talks that are focused on security and privacy. Employees are provided with opportunities to keep their knowledge fresh by attending webinars and cloud provider conferences or by reading industry publications. This also enables them to earn Continuing Professional Education (CPE) credits for relevant certifications.

Our security team
McAfee has a dedicated security team of highly skilled, industry-certified professionals. These professionals work closely with all software engineering and operations teams to provide best practice guidance, frameworks, and security tool sets that can be used in all phases of the cloud data lifecycle. The team is also responsible for providing and maintaining the company’s defense, developing the company’s security review processes, and reviewing all cloud-based services. In addition, the security team is actively involved in operational and application threat modeling, along with assessments of application programming interface (API) security.

Operational security and management
The McAfee security team oversees the system and application vulnerability management process that actively scans for security threats using a combination of tools. They are responsible for providing the framework that is used to identify, understand, track, and follow up on vulnerabilities and service misconfigurations. They follow vendor guidance and identify vulnerabilities or misconfigurations. They then log this data, prioritize threats according to severity, and assign an owner. The vulnerability...
management team tracks all issues and follows up frequently until these issues are fully remediated. The company has predefined security policies with service level agreements (SLAs). Log capture and log management capability is provided using various tools from our own product portfolio and cloud native services. Continual perimeter assessments are done to identify any control, data, or management plane misconfiguration using various tools that have the ability for auto-remediation. These assessments include identity and access management assessments, such as two-factor authentication, login IP ranges, VPN configurations, single sign-on (SSO), and corporate password policies.

**Cloud Data Security**

McAfee understands that cloud data security is critical. Our security team works closely with the legal and engineering teams to understand and implement the required security controls for the relevant frameworks associated with cloud computing. We take data ownership seriously and have policies around data categorization and data classification. We implement asset discovery tools and relevant data security technologies to protect customers, employees, and McAfee data in all environments. Technologies implemented include data loss prevention (DLP), encryption (client and server side), obfuscation, anonymization, tokenization, and masking. Continuous auditing pinpoints and prevents possible data exposures.

**References**


https://github.com/CloudSecurityAlliancePublic/CSA-Guidance