WHITE PAPER

# McAfee MVISION Cloud Security: 360° Shared Responsibility Model

# Table of Contents

# McAfee MVISION Cloud Security: 360° Shared Responsibility Model

## Introduction

Shared responsibility models are important for effective security in computing. Security and compliance are everyone's responsibility and not only something delivered only by the IT group.

For cloud computing, cloud service providers (CSPs) provide some security protection. However, that doesn't mean that cloud data is fully secure. CSPs correctly point out that the responsibility isn't theirs alone, hence the concept of the Cloud Security Shared Responsibility Model. Microsoft, for example, publishes their model for their cloud computing resource, Azure. Amazon has a similar approach for Amazon Web Services (AWS). Both of these models point out that a secure infrastructure relies on the customer playing their part to make the system truly secure and compliant.

This paper acknowledges the work delivered by Microsoft and Amazon (and others) and takes those models as an initial basis, but goes into more depth on the responsibilities of the end-user community (the enterprise itself, the information and IT security teams, and the users). Cloud data can only be safeguarded if security features are well understood, switched on, and properly configured at the outset. This 360˚ Shared Responsibility Model considers who is responsible for cloud configurations, data flow between different cloud services, collaboration, access and device controls, and user behavior.

Every row in the model highlights a different set of possible risks, and every row needs attention to ensure complete security. If an enterprise addresses many rows, but not all, or assumes that someone else is responsible for all security, then security is compromised.

In fact, the analyst community has been sounding alarm bells in the IT community about the growing importance of shared responsibility in cloud security. Gartner, for example, warns that **"Through 2023, at least 99% of cloud security failures will be the customer's fault."**[1]

Gartner's statement implies that enterprises themselves, not the CSPs , need to ensure that their approach to cloud security encompasses all levels of the model.

Recognizing the inherent security pitfalls in the move to cloud services, McAfee is introducing the McAfee® MVISION Cloud 360° Shared Responsibility Model. It is designed to provide a more comprehensive and practical guide to enterprises choosing to fast track their cloud transformation. It builds on existing models

> **"Through 2023, at least 99% of cloud security failures will be the customer's fault."**
>
> —Gartner Magic Quadrant for Cloud Access Security Brokers, October 2018

Connect With Us

of shared responsibility, expanding the layers beyond a binary choice between CSPs and the customer, to all key cloud stakeholders such as the enterprise CISO teams, data owners, infrastructure teams, and users themselves.

The 360° Shared Responsibility Model is designed to help define the combination of groups that need to be aligned to ensure full cloud and data security, across all types of cloud platforms and all types of cloud use cases. The 360° Shared Responsibility Model provides a foundational security approach that should be incorporated as a key element of any organization's cloud IT strategy.

## The Cloud Security "Problem"

"Is the cloud more secure than on premises?" is often asked at conferences and in articles. The answer isn't simply "yes" or "no." It's more of a gray area because both answers could apply, depending on the level of the stack being considered. That said, most IT professionals accept that some parts of cloud security are better than on-premises approaches, since CSPs typically spend more than their customers on protecting their infrastructure and elements such as the data center, server hardware, internet connectivity, distributed denial-of-service (DDoS) defense—all delivered by the CSP.

So which areas of each cloud service are secure? Where are the gaps? And who is responsible for each function in the value chain—from hosting the data to protecting the data on the device or ensuring the service is managed correctly?

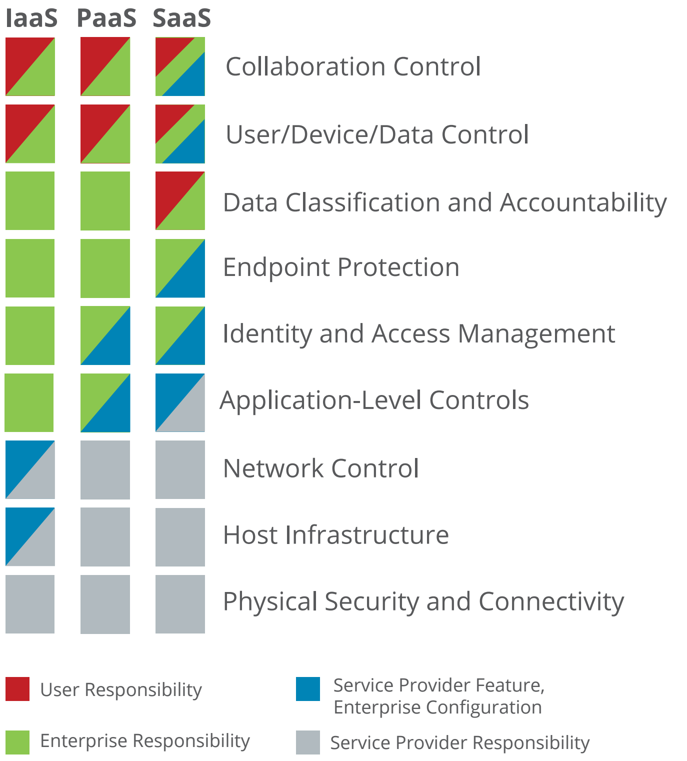
The difficulty with some older shared responsibility models is that they see the world purely from the CSP perspective—listing the security features they offer and leaving the rest up to the customer in an overly simplistic "mine" or "yours" scenario. In reality, digital transformation is making IT much more complex. We need a new model that incorporates all the key players supporting and consuming cloud services across the enterprise so that the organization can fully leverage the benefits of modern cloud IT.

Similarly, it is the responsibility of the IT professional to know all the security measures delivered by the CSP and how to enable them, including any additional security from services such as cloud access security brokers (CASBs), and also to ensure that developers and employees understand their position on the shared responsibility model. We all need to work together and know what we are responsible for.

Overall responsibility for risk belongs to the business, though many security capabilities are outsourced to the IT department and they are in a key position to lead the rest of the organization. Members of the IT team are the guardians of security and compliance for the enterprise. They need to work with the CISO; chief data officer; information security; and governance, risk, and compliance (GRC) to understand and set policies around data control, work with lines of business to help them classify data accurately, ensure compliance with regulations, help the purchasing team make buying decisions on which cloud services to allow users to access, and ensure user training is comprehensive.

## The 360° Shared Responsibility Model

The 360° Shared Responsibility model is designed to be an actionable best-practice guide. It shows which groups are either wholly or jointly accountable at each layer of the model, with a focus on those groups inside the enterprise. Cloud security requires a layered defense, where each layer in the stack of responsibility is addressed, yet they all interact together as a complete framework.



| IaaS | PaaS | SaaS | |
|---|---|---|---|
| 🟥🟩 | 🟥🟩 | 🟥🟩🟦 | Collaboration Control |
| 🟥🟩 | 🟥🟩 | 🟥🟩🟦 | User/Device/Data Control |
| 🟩 | 🟩 | 🟥🟩 | Data Classification and Accountability |
| 🟩 | 🟩 | 🟩🟦 | Endpoint Protection |
| 🟩 | 🟩🟦 | 🟩🟦 | Identity and Access Management |
| 🟩 | 🟩🟦 | 🟦⬜ | Application-Level Controls |
| 🟦⬜ | ⬜ | ⬜ | Network Control |
| 🟦⬜ | ⬜ | ⬜ | Host Infrastructure |
| ⬜ | ⬜ | ⬜ | Physical Security and Connectivity |

🟥 User Responsibility

🟦 Service Provider Feature, Enterprise Configuration

🟩 Enterprise Responsibility

⬜ Service Provider Responsibility

Figure 1. The McAfee® MVISION Cloud 360° Shared Responsibility Model.

## Dissecting the 360° Shared Responsibility Model

To explain the 360° Shared Responsibility Model and understand and describe who is responsible, the best place to start is from the bottom of the diagram and explain the responsibilities for each row.

### Physical security

Physical security has to do with the protection of buildings, core facilities (power, internet connectivity), employees' background/trustworthiness, servers (virtual or real), cabling, and data storage from physical harm and potentially dangerous events. This protection includes acts of God and natural disasters like earthquakes and floods, fires, terrorism, theft, and vandalism. From a compliance point of view, physical security is part of ISO 27001 and SOC2 compliance. Responsibilities are clear. The CSP needs to protect against anything mentioned above. There may be shared responsibility here, as most Software-as-a-Service (SaaS) providers do not own and run their own infrastructure, but rather, buy it from another vendor (like Amazon AWS). This is also an area where a lot of CapEx costs can be saved by moving this part of the responsibility to a service-based delivery model.

### Infrastructure

Infrastructure security covers computing hosts, operating systems and patching, load balancing, scaling, storage, and platform services configuration. If the infrastructure is not secure, it is vulnerable to attacks such as denial-of-service (DoS).

Infrastructure protection is primarily a CSP responsibility, unless enterprise customers are buying Infrastructure-as-a-Service (IaaS) services. The IaaS model offers cloud computing that provides virtual computing resources over the internet for customers, where infrastructure security is a shared responsibility between the CSP and the customer. Responsibility above the hypervisor belongs to the customer, and responsibility for the hypervisor and below belongs to the provider.

### Network security

Network security is about protecting the communications between services, including elements such as virtual networking, load balancing, name servers, and gateways.

In SaaS solutions, this is completely the responsibility of the CSP. In Platform-as-a-Service (PaaS) solutions, customers can define network-level services.

In IaaS solutions, the customer shares more responsibility with the CSP for network security. Virtual network security solutions can provide visibility into potentially risky configurations, threat protection, and micro-segmentation of virtual resources. While the customer doesn't need to connect any cables or buy switches and routers, these (now) virtual assets need to be configured as thoroughly as their physical on-premises counterparts

### Application security

Application security is ensuring applications and services are being built and run securely. This includes web services, batch processes, Internet of Things (IoT), serverless execution, analytics, and so on. The configuration settings and applications must be protected from vulnerabilities and malware.

In SaaS-based solutions, it is the responsibility of the CSP to provide application-level security. However, this is often partly delivered as a set of features that enterprises have to configure. In IaaS solutions, it is a joint responsibility between the enterprise and CSP. In PaaS solutions, it is 100% the responsibility of the enterprise, whether it is the software development (often DevOps) team, security team, or teams with shared security and developer roles like DevSecOps.

A common mistake is leaving applications open to unauthorized users, such as Microsoft Azure Blobs and Amazon AWS Simple Storage Service (S3) buckets left open to be read and written to. Both Microsoft and Amazon set the defaults to be very secure, blocking access to everyone except the owner. The enterprise engineering team needs to ensure that any changes to the security settings don't increase risk.

### Identity and access management

User or identity management is one of the core services that enterprise customers work to provide in a seamless fashion and in ways that are simple to use and easy to manage. Identity and access control let users access and use resources in their environment. It is the glue between the "who" and the "what."

Identity and access management (IAM) identifies users as employees of the company and ensures that the devices they use inside or outside the office, like laptops or mobile devices, are secure. Most enterprises have some kind of authentication technology in place. Many banks, for example, have two-factor authentication schemes in place, where a code is sent to your cell phone before it will let you log on to "the system," and makes sure the user is actually who they say they are and is using a legitimate device. Access control, in the above example, and two-factor authentication in the financial sector, go beyond simple bank policy and may even be regulated. Third-party solutions can also validate a device prior to allowing access to data. This enables enterprises to block unknown, personal devices from accessing their cloud resources. For third-party access to cloud services, such as sharing information with other organizations in the supply chain, the enterprise organization needs to decide how to authenticate these users.

An example of the problem of ignoring this row in the model is where a cloud service is considered "non-core" and administered by a single department that doesn't integrate it with the global IAM such as the webinar system administered by marketing). If a user leaves the company, they may still have a login to this service and subsequently access to the data contained therein.

### Client and endpoint protection

Endpoint devices that access the cloud need to be kept secure and access must be controlled if device status is unknown. Risk can be introduced, for example, if a device has write access to an organization's cloud services and inadvertently uploads a file containing ransomware. Without even accessing the cloud itself, modern malware can steal login credentials from target groups of users "on demand" and use the stolen credentials to exfiltrate data from anywhere. The customer organization is primarily responsible for endpoint protection and for traditional end-user training about safe usage. CSPs may provide capabilities that define endpoint devices and provide secure device management, mobile application management, and PC management. However, using a mobile management solution will still require customer accountability for their users.

Client and endpoint protection will protect the user and their devices from attack. If criminals want only to steal compute cycles, as in when they turn client devices into internet bots or run processes unbeknownst to their "host" (such as cryptomining), that's one thing. Spam may just bombard the user with unsolicited information. Viruses (unwanted processes running on your PC) slow things down, and that may be the extent of the damage. Some exploits may be driven by pure mischief. But more sinister infections may involve spam or malware running on the users' PCs or laptops for criminal purposes. That's another level altogether. Modern malware is smart enough to steal login credentials from target groups of users "on demand." Even innocent-sounding spam has the potential to spy on the user and steal login credentials or address books. Client and endpoint protection is that suite of antispam and virus protection that slows down your fast laptop or blocks you from doing the things you want do to run your business. The IT group normally installs the software and sets the definitions of what constitutes spam or attacks on users' devices.

## Data classification and accountability

Defining data classification and accountability requires surveying the enterprise's own data to categorize it as sensitive or otherwise (the categories will determine how the data is handled) and who can access this data based on regulations or commercial requirements. DLP systems typically start with classification scanning. Data classification is in the domain of the line-of-business (LOB) manager. Third-party solutions also exist to enable users to self-classify their own data. Lines of business own their data and need to collaborate with security teams to assist with classification. Guidance is available here.

Data classification is often thought to be the ultimate solution to data protection requirements. However, experience has shown that automated tools for data classification and overly enthusiastic data classification programs and rules often lead to a negative user experience. Over-classification and misclassification can impact business agility.

## User, device, and data controls

User, device, and data controls need to work together with cloud computing as data moves to clouds, from clouds, and between clouds. The data part is subtly different than protecting it, as outlined in previous sections. This isn't so much about protection from attacks, but rather controlling how data—especially sensitive data—is monitored and managed.

For "from the cloud traffic," security team needs to define policies for areas such as whether particular data can be downloaded to unmanaged devices or shared with specified parties or all third parties.

For "to the cloud" services, the IT team should check files for malware and ransomware as they are being uploaded to the cloud, especially when third parties are allowed to access and upload files to the company's cloud. Some sensitive classifications of data may also need to be blocked from entering the cloud or directed to approved cloud services only.

Data between clouds also should be controlled. When it is possible for a user to join two cloud services together, the IT team needs to manage data transfer. The cloud service provider may have controls allowing and disallowing between cloud transfers, but it is the responsibility of the enterprise to set up the policies.

## Collaboration behavior

Many cloud services provide the ability to collaborate between people. The user has the ultimate responsibility to ensure that data is not shared in an unsafe manner, though they will need training to understand the risks and engage in only safe activities.

## How McAfee Technology Can Help

A summary of who does what—who is responsible for what security function—is offered in the diagram below. Use this diagram to explore solutions from McAfee that can address the 360° Shared Responsibility Model.

Below, we'll look at potential use cases for McAfee technology, where McAfee as a CSP fits in this model, and how these use cases can provide practical help.

The enterprise IT team has to ensure an intuitive and powerful set of sanctioned tools and apps for the LOB user. In practice, this provides a way to control the link. A CASB can help by providing an approved set of web services that can be accessed via the cloud. A CASB provides insight into cloud app use across cloud platforms and identifies unsanctioned use, which is particularly important to regulated enterprises like banks. The MVISION Cloud uses autodiscovery to audit the apps LOB users are using and identifies risky apps (and risky users), sensitive data, and other risk-related categories. MVISION Cloud autodiscovers all cloud apps in use and provides detailed risk ratings for each service, enabling you to quickly understand the risk to your organization and how it compares with your peers in the industry. Also, when a user visits a web page, domain checks can use these to resolve the host dynamic name server (DNS) name rule objects (which are friendly for users) to IP addresses (which are not). The IT team can configure the DNS server details at a domain level or at a device level.

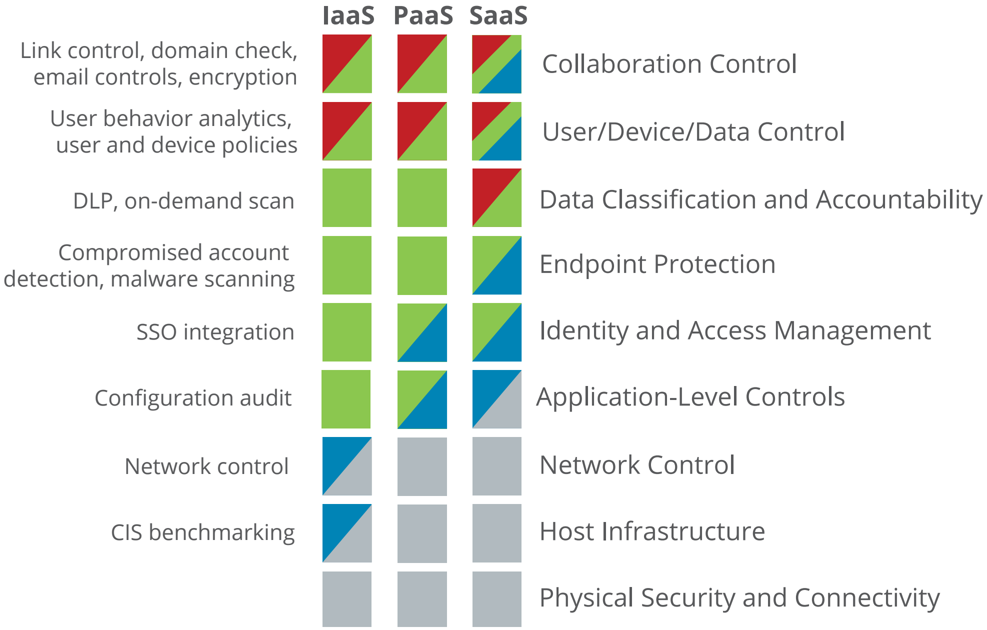

IaaS
PaaS
SaaS
Link control, domain check, email controls, encryption
Collaboration Control
User behavior analytics, user and device policies
User/Device/Data Control
DLP, on-demand scan
Data Classification and Accountability
Compromised account detection, malware scanning
Endpoint Protection
SSO integration
Identity and Access Management
Configuration audit
Application-Level Controls
Network control
Network Control
CIS benchmarking
Host Infrastructure
Physical Security and Connectivity

Figure 2. Technologies that support the 360° Shared Responsibility Model.

McAfee® Security for Email Servers provide in-memory and incremental on-demand scanning to remove viruses, worms, Trojans, phishing, and other threats from incoming and outgoing email. These risk ratings can be applied too. Encryption is a technique that can be used to control user behavior by encrypting outgoing messages so that only the intended recipient can decrypt it.

User behavior analytics is available to apply big data principles to rapidly process massive volumes of data, extending detection and correction through behavioral analytics and on to endpoint detection and response, enabling remediation to the endpoint in real time. User and behavioral analytics give us a snapshot of how users are using devices and cloud apps. Policies that run on MVISION Cloud protect data by taking actions deep within the cloud with services that correct policy violations and stop security threats. It's cloud-native data security. Armed with analytics, you have data on how users are using cloud services and you can make sure that data in the cloud is being handled properly and protected in keeping with your own and regulatory requirements and with national and international mandates.

DLP scans give you a good idea of what your enterprise considers as sensitive and non-sensitive data. McAfee® DLP Discover runs on premises or on virtual cloud servers and scans network file systems and databases to identify and protect sensitive files and data. This can be done when the system is installed (known as in transit) or on demand whenever your enterprise needs to.

Malware is malicious executable software that is designed to steal data from your enterprise. MVISION Cloud uses a combination of signatures and running executables to identify malware in the cloud and to stop threats. Cybercriminals are keen to collect every piece of information they can about you and potentially sell them online or use them for their own nefarious purposes. Even internal resources may maliciously or inadvertently compromise their own accounts or a co-worker's account. The LOB manager should be able to spot hacked accounts or insider threats. Malware scanning is used to identify which login credentials have been compromised and flags malware in real time to detect criminally compromised accounts and even insider threats in MVISION Cloud.

IAM and single sign-on (SSO) integration allows the IT team to work with the LOB manager to connect access methods like Microsoft Active Directory (AD) and integrate it with McAfee IAM and SSO. Users are no longer required to remember multiple, complex passwords. And your enterprise saves time and money while significantly increasing the security of data in the cloud.

The McAfee® Virtual Network Security Platform technology expands network protection across virtualized environments like Microsoft Azure. It delivers network security solution designed for public clouds and clouds made up of a combination of private and public clouds. It includes a virtual instance of intrusion prevention system (IPS) with network visibility and inspection techniques. Cloud workload protection (CWP) provides automatic workload management and detection, along with blocking of malware in the cloud.

All CSP security features—whether they come from Salesforce or Box—are configurable via registry entries in MVISION Cloud. This allows IT professionals to view and make potential security configuration choices and apply security attributes. McAfee leverages its proven expertise to bring security to the apps and services LOB users use every day by augmenting the security capabilities of your preferred app provider.

## Summary

Everyone involved has some responsibility when it comes to security, especially cloud security. Responsibility is shared across different constituencies, depending on the systems in use.

The CSP is responsible for providing the baseline level of security measures and for offering additional security features, but it is the responsibility of the customer's IT teams to configure these properly. If the CSP doesn't host its own systems, the CSP needs to ensure that the lowest layers in the model are delivered by the hosting outsourcer they've chosen—SaaS, PaaS, or IaaS vendors.

Governance, risk, and compliance (GRC) teams need to define which regulations and standards the enterprise aspires to adhere to. GRC defines and executes a strategy for the enterprise's overall governance, enterprise risk management, and compliance with regulations and needs to work hand in hand with IT security and content owners to define what data needs to be protected and define appropriate secure processes, such as DLP, access control, and which third parties are trusted with the enterprise's content. In practical terms, GRC will set the enterprise's security policy. IT interprets the policy and compliance needs of the enterprise—as articulated by the compliance group—doing their own due diligence and choosing the best partner and technology to enforce the security features they've sourced.

All LOB users need to be trained to understand their part in cloud security, with regular reviews of their knowledge and technology. McAfee can help by intercepting potentially dangerous actions and reminding LOB users (the most important consumer) of their responsibilities.

Ultimately, cloud security is a shared responsibility. All enterprises need to assemble a cloud security steering committee, drawn from multiple disciplines, to share knowledge and define appropriate policies for the security team to enforce.

## Family Car Rental: The Ultimate in Shared Responsibility

Perhaps the ultimate shared responsibility model in our daily lives is best illustrated by renting a car for a family vacation.

First, the manufacturer has the responsibility that the car is roadworthy when it comes off the assembly line. It needs to have good brakes, tires, and functioning airbags. The manufacturer needs to ensure that the car will not fall apart when it turns the first corner. During the lifetime of the car, the rental company and the renter hopefully won't need to test the airbags—they typically just assume that they will work as originally installed.

Once the car gets older, the owner (the rental company) is responsible for checking the tires and the brakes, servicing the car, and keeping it roadworthy. The renter assumes that this is simply the case. The renter needs to have the appropriate license for the vehicle, and this is checked by the rental company before the car is handed over.

The car includes seat belts, installed by the manufacturer, but it is the driver's responsibility to wear seat belts and ensure that all the family members wear them too.

For young children, it is the driver's responsibility to ensure that they have appropriate child seats. The parent also has to ensure that the older children do not remove their seat belts.

Ultimately, the driver is responsible for driving the car appropriately for conditions—more slowly in rain and snow and not speeding around corners.

There is, therefore, a responsibility shared among four groups of people: the car manufacturer, the rental company, the passengers, and the driver. Everyone has their part to play. If one area is ignored, there could be an accident with tragic consequences, and it is no good to say, "but I checked the other areas." Every aspect needs to be considered in totality.

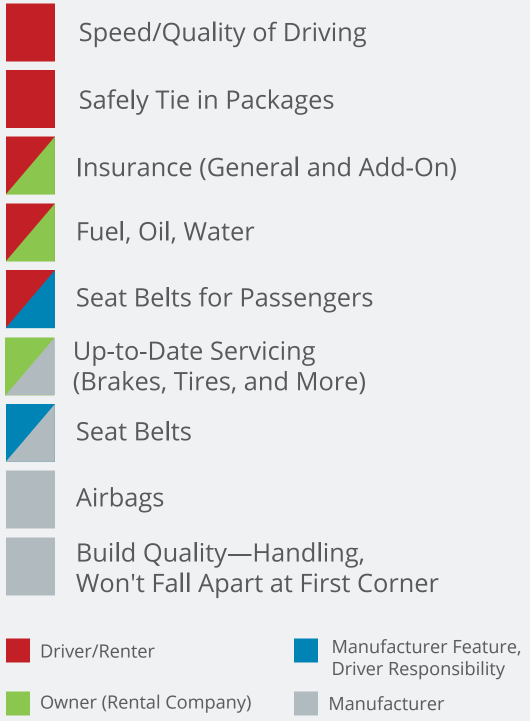

Speed/Quality of Driving
Safely Tie in Packages
Insurance (General and Add-On)
Fuel, Oil, Water
Seat Belts for Passengers
Up-to-Date Servicing (Brakes, Tires, and More)
Seat Belts
Airbags
Build Quality—Handling, Won't Fall Apart at First Corner
Driver/Renter
Manufacturer Feature, Driver Responsibility
Owner (Rental Company)
Manufacturer

Figure 3. Family car rental and shared responsibility.

1. Gartner Magic Quadrant for Cloud Access Security Brokers, October 2018: https://www.gartner.com/doc/reprints?id=1-5NLQ0H4&ct=181026&st=sb

## About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

**www.mcafee.com**

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