McAfee
Together is power.

Data Center and Cloud Defense

Protecting your hybrid cloud

Today's compute environment continues to evolve rapidly. Instantaneous cloud-based access means that vital intellectual property and enterprise and customer data are scattered across myriad infrastructures. Most data centers today have a hybrid infrastructure that spans physical, virtualized, and cloud deployments, both on premises and off premises. The key driver for this massive data center transformation is a need to keep up with the changing compute landscape and, more importantly, a need to provide an agile IT infrastructure services to help meet business expansion goals.

A highly distributed compute environment brings with it an exponential growth of the attack surface, which presents big security challenges. Simultaneously, the threat landscape continues to evolve—both the frequency and sophistication of targeted attacks are growing at an alarming rate. Organizations need to improve their ability to detect breaches quickly and to adopt continuous incident response. This is especially important as the costs associated with attacks are increasing. Unfortunately, most current security tools are challenged to deliver the efficiencies and scalability required—which are particularly crucial when there is an acute shortage of qualified security talent able to respond.

Security technologies need to support a strong security posture with common policies across the hybrid infrastructure without adding operational costs or reducing business agility. In this new world order, securing hybrid infrastructures requires an understanding of these key elements:

- **Visibility is paramount:** It is essential to have visibility into the entire environment, both private and public clouds. Shadow IT is posing an enormous risk for enterprises because of the lack of visibility, which makes it untenable to ensure strong security policy.
- **The perimeter is shifting:** Gone are the days of relying entirely on the traditional perimeter. With workloads shifting to Infrastructure-as-a-Service (IaaS), host-based security technologies are a critical perimeter defense.
- **Security controls must align with the dynamic hybrid infrastructure:** It is essential for security technologies to be agile and offer simplified operations and reduced operating expense.
- **Advanced threats:** Fast, accurate, and automated containment and remediation of sophisticated threats is essential. Security capabilities must extend across multiple architectures. Having access to strong local and global threat intelligence is also increasingly important for enhanced and timely threat detection and remediation.
- **Optimized security for new deployment architectures, such as the software-defined data center (SDDC):** As virtualized private cloud environments are transitioned into SDDCs, learnings from the traditional virtualized private cloud environment can be applied, such as implementing an optimized antivirus solution for virtual machines that delivers robust protection and simplified management with a low-performance footprint. Additionally, in SDDCs, the network is virtualized as well, so east-west traffic inspection is required. The implementation of software-based network protection, such as a virtual intrusion prevention system (IPS) is essential. It is also important to assess overall orchestration technologies and ensure that rules can be easily deployed and updated.

Enterprise IT Challenges

Many considerations need to be taken into account when securing hybrid infrastructures. Most enterprises face three main challenges:

- **Visibility across multiple cloud architectures:** The data center is moving to a services-oriented architecture to meet the needs of lines of business, and the hybrid infrastructure has emerged, where data and applications reside on premises and off premises. The big challenge is lack of full visibility into the data and applications. Without visibility, enterprises cannot sufficiently secure this infrastructure, and this can result in serious breaches that may have significant reputational, legal, and financial consequences.
- **Efficient deployment of security controls:** Workloads need to be secure wherever they reside or move. Consistent security controls need to extend easily from traditional on-premises deployments into public cloud environments. Security protection needs to be elastic so as not to hinder business agility and add to operational costs.
- **Uniform management of security posture:** Security policies also need to be managed centrally to facilitate centralized policy definition, monitoring, and response and to enforce compliance and risk posture across the hybrid infrastructure. Detection capabilities must traverse a heterogeneous compute environment without significant delays.

Network Protection

- McAfee® Network Security Platform (available as physical or virtual IPS appliances)

Server Protection

- McAfee Server Security Suite Essentials
- McAfee Server Security Suite Advanced
- McAfee Public Cloud Server Security Suite

Database Protection

- McAfee Data Center Security Suite for Databases

Threat Intelligence

- McAfee Threat Intelligence Exchange

Figure 1. The McAfee product portfolio for the hybrid cloud.

The McAfee Solution

McAfee enables enterprises to extend security across the data center, whether on premises, in the cloud, or in a hybrid environment. We provide protection that can be deployed across physical, virtual, and cloud infrastructures; that has the ability to detect and correct breaches; and that provides professional services that deliver expert knowledge and 24/7 care and monitoring to tackle complex security requirements.

In conjunction with our professional services, our key products for hybrid infrastructures are:

- **Server security and management for physical, virtual and cloud deployments:** McAfee® Server Security Essentials and McAfee Server Security Advanced Suites, McAfee Public Cloud Server Security Suite.

- **Database protection:** McAfee Database Security Suite for Databases.
- **Network protection:** McAfee Network Security Platform and local threat intelligence via McAfee Threat Intelligence Exchange.

In addition, we offer centralized management that provides full visibility into your IT security posture for faster remediation and reporting to reduce risk and cost.

Our products help enterprises secure their hybrid infrastructure in the data center as we provide efficiency and effectiveness with our integrated architecture. Unlike multivendor, best-of-breed environments, which often have serious protection gaps, our products are connected, which greatly reduces the complexity of managing security across hybrid infrastructures.

McAfee Solves Customer Challenges

Securing the Hybrid Infrastructure

Mitigate the risk of compromised or malicious east/west for virtualized networks.	Remotely discover, assess, and fix issues in the cloud from your McAfee® ePolicy Orchestrator® (McAfee ePO™) console	No need to trade security for performance
Secures data "crown jewels" in databases and on servers	Reduced data center interruptions by combating threats more efficiently	Provides agent-based or agentless deployment

Figure 2. How McAfee products provide protection required by the hybrid infrastructure.

McAfee provides **visibility** across hybrid infrastructures:

- Across physical and virtual servers, on premises and off premises, and supports all major cloud platforms: Amazon Web Services (AWS), Microsoft Azure, OpenStack, and VMware.
- Into your database landscape and security posture to fully align database security policy administration while efficiently maintaining regulatory compliance.
- From global threat intelligence (McAfee Global Threat Intelligence) and local threat intelligence (McAfee Threat Intelligence Exchange).

McAfee Customer Support

At McAfee, we have a passion for security, and that extends to our McAfee Support and Customer Service. Regardless of the size of your business, McAfee Technical Support offers highly trained and certified security professionals who can provide the right information, tools, and programs. Our goal is to address potential issues quickly and efficiently to help you combat today's threats so you can focus on the demands of your business.

McAfee provides **consistent deployment of security controls** across the hybrid cloud:

- We provide the most comprehensive server protection across physical, virtual, and cloud deployments, unlike our major competitors, who have weaker IPS, whitelisting, and change control and who provide less flexibility for virtual deployments. In addition, we have higher detection rates than other vendors.
- We prevent the spread of threats in the data center. Inspection of both north-south and east-west traffic protects network traffic, which is important since 80% of network traffic remains in the virtual network and doesn't leave the data center. Competitive solutions are not inspecting east-west traffic.

McAfee **simplifies security management** for the hybrid cloud, enabling IT to centrally define security policies, monitor security status, and respond to threats, as well as manage security in an elastic fashion as compute resources are spun up and down. We provide:

- A single management console for all endpoint security solutions with McAfee® ePolicy Orchestrator® (McAfee ePO™) software. We also offer a network security console that can interface with McAfee ePO software.
- Elastic security, where policy is automatically applied as compute resources scale up and down, enabling IT to keep up with business demands.
- Network protection that provides cost-efficient management of network security with streamlined administrative workflows and signature-less protection from zero-day attacks and advanced malware. We also deliver the industry's highest real-world throughput of up to 320 Gbps.
- Rapid deployment and orchestration of security for SDN and SDDC environments with our IPS solution, which integrates with Open Security Controller from Intel and VMware NSX.
- A unique threat intelligence ecosystem where detected threat data can be shared throughout the organization to all connected components for real-time protection.

McAfee Solution View by Deployment Architectures

Architecture	McAfee Advantage
Private Cloud	**McAfee Network Security Platform and McAfee Virtual Network Security Platform** ▪ Actionable workflows out of the box that organize multiple alerts into single events, focusing operators on what matters most in the detection process. By cutting through the noise and working only with relevant data, these solutions correlate multiple IPS alerts into a single, actionable event. ▪ Display security data via an intuitive interface that has preconfigured, guided threat workflows. Traditional IPS dashboards typically arrange alerts by timestamp, placing the newest alerts on top. This overloads the operator, creating noise and confusion. ▪ Advanced technologies, such as signature-less traffic inspection, that go beyond traditional signature-based defenses, empower security administrators to block advanced threats and zero-day attacks for which IPS signatures do not exist. ▪ Get connected visibility with McAfee Network Security Platform, the only IPS to integrate across multiple security products, plugging the infrastructure gaps. We provide improved ROI and lower TCO when McAfee Network Security Platform leverages data and workflows from five other security products. Alert relevance and prioritization is improved with endpoint data to close gaps and increase ROI. Native integration lowers TCO via automatic tuning and plug-and-play deployment. Due to this connected visibility, both ROI and TCO are improved as efficiency increases—outside data seamlessly integrates into known workflows. **McAfee Server Security Suite Essentials, McAfee Server Security Suite Advanced, McAfee MOVE AntiVirus** ▪ McAfee Cloud Workload Discovery for private clouds, including VMware and OpenStack, provides end-to-end visibility into all workloads and their underlying platforms. Insights into weak security controls, unsafe firewall and encryption settings, and indicators of compromise (IoCs) lead to faster detection, while McAfee ePO software or DevOps tools enable quick remediation. ▪ Superior whitelisting and change control solutions plus user-based policies rather than only machine-based policies. ▪ Antivirus for virtualized servers (McAfee MOVE AntiVirus) supports agentless and multiplatform deployments for protecting virtualized environments, while some vendors only support agentless deployment. ▪ McAfee MOVE AntiVirus, with its advanced detection, provides the highest malware detection rates with true offline scanning. **McAfee Threat Intelligence Exchange** ▪ Delivers local threat intelligence that not only detects emerging threats, but also shares this information across the infrastructure in seconds to allow for immediate protection. ▪ Built on the McAfee Data Exchange Layer, which allows for ultra-fast, bi-directional communication between connected systems. Our competitors have endpoint systems only, which do not work in conjunction with network, gateway, and third-party solutions. **McAfee Data Center Security Suite for Databases** ▪ A database security solution that is built with a non-intrusive host-based agent (sensor) for speed and scale across virtualized private cloud deployments.

SDDC	**McAfee Virtual Network Security Platform, McAfee MOVE AntiVirus, and Open Security Controller** ▪ The only vendor to offer both virtual network security and virtual machine-based security. ▪ Better management of VMware NSX compared to other vendors. ▪ Open Security Controller rapidly deploys and orchestrates security within the SDDC. ▪ McAfee Virtual Network Security Platform integrates with Open Security Controller and VMware NSX, enabling IT administrators to rapidly deploy and orchestrate security within the SDDC, protecting VM network traffic by scanning the 80% of data center traffic that typically remains in the virtual network.
Public Cloud	**McAfee Network Security Platform and McAfee Virtual Network Security Platform** ▪ McAfee Virtual Network Security Platform offers cloud scalability through an innovative approach to virtual network inspection, so administrators can easily scale security into the dynamic nature of cloud platforms. ▪ Support for network virtualization enables administrators to quickly deliver east-west network protection to virtual workloads. Support for cloud sharing allows administrators to share their IPS throughput and license across any combination of public and private cloud. ▪ With McAfee Virtual Network Security Platform, McAfee has delivered a simplified solution that easily embraces virtual networks and scales across both public and private clouds. Customers receive the operational efficiency to provide a unified security solution into their private and public clouds at a scale never before possible. **McAfee Server Security Suite Advanced, McAfee Public Cloud Server Security Suite** ▪ Security visibility and control across a wide variety of server instances, residing in the public cloud across AWS, Microsoft Azure, OpenStack, and VMware. ▪ McAfee Cloud Workload Discovery for public clouds, including Amazon AWS, Microsoft Azure, and OpenStack, provides end-to-end visibility into all workloads and their underlying platforms. Insights into weak security controls, unsafe firewall and encryption settings, and IoCs lead to faster detection while McAfee ePO software or DevOps tools enable quick remediation. ▪ A single management console (McAfee ePO software) for all endpoint and server security solutions. ▪ The leading file integrity monitoring and control solution with application control and change control for servers, which is critical when deploying instances in an IaaS environment.

McAfee Professional Services

Managing both cloud (public/private) and non-cloud assets and the data they contain is a growing and complex problem. Whether using multiple vendor solutions or a complete McAfee portfolio, companies often require additional services, expert knowledge, and 24/7 care and monitoring to tackle the complex security requirements for the hybrid data center. The McAfee Professional Services team provides comprehensive services help organizations protect, design, staff, and manage their hybrid infrastructures.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 2052_1216
DECEMBER 2016