Solution Brief

Securing the Private Cloud

Protect Your Private Cloud with an Integrated Approach to Security.

Built to run and scale dynamic workloads on highly virtualized infrastructure, private cloud deployments create security challenges that traditional 'static' security solutions were never designed to address. In response, Intel Security has developed cutting-edge technologies and an integrated deployment model that maximizes protection of private cloud instances including software-defined data centers (SDDCs) and multitenant customer environments. Now, enterprises and managed service providers (MSPs) can enjoy the business flexibility and cost savings associated with private clouds, while keeping intellectual property and customer data safe. Intel Security solutions protect private clouds against both internal and external threats such as targeted attacks and malware, while ensuring compliance with industry and government regulations.

The Challenges of Private Cloud Security

Organizations of all sizes are increasingly embracing private clouds. The objective is to achieve the cost efficiencies and agility of public clouds without compromising IT control and security. According to one survey, more than 70% of enterprises are using, implementing, or evaluating private cloud models.[1] Private clouds offer IT greater control versus public clouds as well as benefits over traditional data center models. But private clouds create unique security challenges that must be addressed in order to maximize protection and compliance.

One key challenge is the lack of visibility into all traffic to ensure that the organization is not victim to a targeted attack. In a highly virtualized private cloud environment, network traffic increasingly flows in an east-west direction between virtual machines (VMs). Traditional point security solutions are not built for these types of virtualized data center environments—they protect north-south traffic, or traffic that flows through the data center's perimeter. These traditional solutions lack visibility into traffic that stays within the data center—or east-west traffic—thereby creating a gap in protection. If solutions don't inspect east-west traffic, internal threats can propagate laterally inside the data center.

intel Security

Another key private cloud challenge is providing security at the speed of the cloud while still maintaining compliance. As the IT team moves to a more dynamic and agile computing model, network security needs to adapt just as fast as the cloud. In addition, IT needs to comply with regulations such as PCI and HIPAA. Unfortunately, point security solutions don't scale and therefore can't migrate automatically with virtualized workloads.

The final key challenge is the limited ability to confidently manage security policies and ensure strong SLAs to support line of business demands. IT typically has insufficient security staff to effectively and efficiently manage security across private clouds. The staff they do have mostly use traditional tools, but do not share threat information in a timely manner, if at all.

The Goals of Private Cloud Security

You need to protect your organization against both external attacks and insider threats. This means you can't have any gaps in your private cloud security. For external attacks, you want to discover and block inbound attacks at the perimeter and also detect and block outbound command-and-control server communications. For internal threats, you must be able to discover and remove malware from virtualized servers within the data center and detect and block attacks stemming from privileged user accounts.

To achieve these goals, you need complete security visibility, dynamic protection, and efficient policy management across your private clouds. Complete security visibility of all private cloud workloads is mandatory to protect your organization, because you cannot protect what you cannot see. Dynamic protection provides the ability to secure a private cloud environment with security that adapts to the ever changing environment where virtual machines are constantly moved to different hosts. Finally, you need simplified security management that leverages staffing resources and enables them to efficiently deliver on SLAs while keeping the business protected.

How the Intel Security Coordinated Model Works

Intel Security delivers the most complete and integrated security solution to help enterprises efficiently and effectively secure and maintain compliance for highly virtualized private cloud or SDDC environments without sacrificing agility, operational efficiency, and cost savings.

We deliver maximum protection against advanced targeted attacks through a combination of solutions designed to work seamlessly together to address the specific challenges of highly virtualized private cloud deployments and SDDCs. Here is an example of how the integrated Intel Security model works for threats at the perimeter of the data center:

Combating emerging threats. Detecting a targeted attack and stopping its spread is different in a private cloud. A file is inspected at the perimeter by McAfee® Virtual Network Security Platform, an inline virtual intrusion prevention system (IPS). It is then scanned using various signature-less engines enabled in the solution's advanced malware policy. If the file is suspect but status cannot be determined with certainty, the McAfee Virtual Network Security Platform sends the file to McAfee Advanced Threat Defense which scans it and publishes the reputation to McAfee Threat Intelligence Exchange. This information is shared with McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) on the server which takes action and deletes the file.

Maximizing Protection and Compliance through Intel Security Solutions

The combination of Intel Security solutions that form the foundation for this level of visibility, dynamic protection, and efficient policy management are as follows:

- **McAfee Virtual Network Security Platform.** This full-featured advanced IPS is designed specifically to meet the demands of virtual environments. It's a virtual instance of the McAfee Network Security Platform, enabling you to quickly deploy virtual sensors to protect various network architectures. Leveraging tight integration with other Intel Security technologies such as the Intel® Security Controller and McAfee Advanced Threat Defense, McAfee Virtual Network Security Platform enables immediate action when a file is determined to be malicious. With a coordinated security approach you can immediately block other copies of this file from coming onto the network, without the need to reanalyze the file. In addition, the solution can quarantine an infected host, preventing the spread of malicious activity on the network.
- **McAfee MOVE AntiVirus.** McAfee MOVE AntiVirus brings optimized malware protection to virtualized desktops and servers. It eliminates scanning bottlenecks and delays by offloading scanning, configuration, and .DAT update operations from individual guest images to a hardened virtual appliance/offload scan server. By leveraging a global cache of scanned files, McAfee MOVE AntiVirus ensures that once a file is scanned and confirmed to be clean, subsequent VMs accessing that file won't have to wait for a scan.
- **McAfee Threat Intelligence Exchange.** McAfee Threat Intelligence Exchange enables adaptive and collaborative threat detection and response, providing organizations with superior visibility and control in the battle against emerging and targeted attacks. It combines important global threat information with locally collected intelligence, operationalizing intelligence across servers, gateway, network, and data center security solutions in real time. By sharing this intelligence instantly, McAfee Threat Intelligence Exchange allows your security solutions to operate as one, exchanging and acting on shared intelligence. With this type of adaptive threat protection, you can close the gap from encounter to containment down to milliseconds—compared to days, weeks, or even months using traditional security models.
- **McAfee Advanced Threat Defense.** With McAfee Advanced Threat Defense you can detect advanced targeted attacks and covert threat information into immediate action and protection. Unlike traditional sandboxes, McAfee Advanced Threat Defense includes additional inspection capabilities that broaden detection and expose evasive threats. It uses an innovative, layered approach to detect zero-day malware. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior. To address the challenge of threats evading sandbox detection, McAfee Advanced Threat Defense includes extensive unpacking capabilities that remove obfuscation, exposing the original executable code. The solution enables static code analysis to look beyond high-level file attributes for anomalies, analyzing all the attributes and instruction sets to determine the intended behavior.
- **McAfee ePolicy Orchestrator® (McAfee ePO™) software.** McAfee ePO software provides integrated security and central policy management across all your cloud deployments. Discover and gain visibility into all VMs, simplifying the task of securing clouds. Administrators can monitor hypervisor-to-VM relationships, security status, and power status in near real time.

Achieving Your Protection and Compliance Goals for the Private Cloud

By leveraging the integrated Intel Security portfolio for private cloud protection, you can achieve all of your critical security goals, including:

- Complete visibility into what needs to be secured and advanced threats to help fortify security for private clouds. This helps safeguard customer data and corporate intellectual property housed in the private cloud.
- Integrated dynamic protection technologies that match the agility of private cloud environments to protect against advanced threats and maintain compliance, and that also east-west traffic flows inside the private cloud environment. This helps achieve—and demonstrate—compliance with industry and governmental laws and regulations.
- Advanced policy management across the infrastructure with automation to efficiently deploy security policies for private clouds. This helps lower the costs associated with security, threat remediation, and maintenance within the software-defined data center. It also reduces the time it takes to discover and remediate external and internal threats and attacks.

Key Intel Security Advantages

A Complete Portfolio
Leverage a full portfolio of solutions designed to work seamlessly together to address the specific security challenges of private cloud environments.

Dynamic Protection and Remediation
Dynamically protect, manage, remediate, and support compliance in your private cloud with next-generation IPS services.

Prevent External Attacks
Discover and block attacks, malware, and threats at the SDDC perimeter and detect and block inbound command-and-control server communications at the perimeter.

Prevent Insider Threats
Discover and remove malware from virtualized servers within the SDDC and detect and block attacks from privileged users.

Strengthen Compliance
Achieve and demonstrate compliance with industry and governmental laws and regulations.

Accelerate Response
Leverage adaptive threat protection to reduce the time it takes to discover and remediate external and internal threats and attacks.

Lower Costs
Reduce the costs associated with security, threat remediation, and maintenance within the SDDC.

Enhance Visibility
Get immediate visibility into the presence of advanced targeted attacks within your organization.

For more information please visit **www.intelsecurity.com/cloudsecurity**.

1. "State of the Market: Enterprise Cloud 2016," Verizon, November 2015

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com