EBOOK

A Guide to Private Cloud Security

TechTarget® Custom Media

A TECHTARGET WHITE PAPER

intel® Security

Executive Summary

Enterprise IT leaders are embracing private clouds to improve agility, reduce costs and accelerate development cycles as they transition to a service-based delivery model. With private cloud, IT can achieve virtually all the key benefits of the public cloud—such as resource pooling, self-service provisioning and elastic scalability—while asserting greater control over security, protection and compliance.

According to one survey, 77% of organizations adopted private cloud as of early 2016, a sharp increase from 63% for the prior year.[1] Another survey states that technology advances such as software-defined data centers (SDDCs) and converged infrastructures are narrowing the price differential between private and public cloud models, which will spur an even greater reliance on private cloud for enterprise customers over the next few years.[2]

While the benefits of private cloud are significant, this new infrastructure model also introduces security and compliance challenges. For example, traditional point security solutions were not built to protect the preponderance of traffic that flows within a private cloud. Businesses need to update and modernize their approach to protection. They also need to address gaps in visibility and automation to properly secure highly virtualized infrastructures.

By adopting a modern approach to security and compliance, IT teams can leverage an infrastructure that is much easier to deploy and manage, with security protections that dynamically scale as the private cloud grows, thereby enabling business agility and innovation. This is particularly critical as enterprises strive to accelerate development cycles and embrace digital transformation.

This e-book provides an overview of private cloud models, the underlying technologies that enable successful deployments and the security challenges—and benefits—of deploying a private cloud. Finally, it discusses security technologies and approaches that maximize protection, minimize risk and leverage the private cloud to drive innovation.

Let's get started.

CHAPTER 1:
Private Cloud Overview

Private cloud is not a one-size-fits-all solution. Different deployment methods require different approaches to security. The first step is to understand what private cloud means to your organization and how you are deploying it.

Many IT leaders believe that they are deploying private cloud if their data centers have high levels of server virtualization. By most standards, however, this is not considered a private cloud because server virtualization is only one aspect of deployment.

A private cloud should be able to deliver the key characteristics you expect from a public cloud deployment, in particular:

Empowering development and operations (DevOps) is one way private cloud can deliver significant value to your organization.

- **Self-service provisioning:** End users can spin up computing resources for almost any type of workload on demand.
- **Elasticity:** Companies can scale up as computing needs increase and scale down again as demands decrease.
- **Automation:** IT teams can simplify deployments and reduce risk while alleviating the stress of the cybersecurity skills shortage.
- **Pay per use:** Computer resources are measured at a granular level, allowing for automated chargebacks to the departments consuming resources.

There are also important distinctions between private and public clouds. In the public cloud model, you purchase all of these features and functions as a service and the cloud service provider owns and controls the infrastructure. In a typical private cloud environment, you have to leverage virtualization, automation and orchestration capabilities across your own infrastructure. Ideally, you also want to enable self-service provisioning and automatic chargebacks, and you need processes and guidelines for how users can leverage the infrastructure.

Empowering development and operations (DevOps) is one way private cloud can deliver significant value to your organization. For instance, a DevOps team may be developing an application and needs its own infrastructure resources for development, testing and quality assurance. Rather than filing a formal IT request and waiting for approval and deployment, the DevOps team can simply go to a catalog of services and choose the specific server performance, network bandwidth, storage capacity, storage performance and other capabilities needed.

DevOps teams get access to those services immediately and are automatically charged for the resources they use. When a team no longer needs the resources, it can return them to the pool, making them available to other teams within the organization.

Enabling Technologies for Private Cloud

The path to building and securing the private cloud often begins with a plan to modernize your infrastructure, which can evolve over time toward the desired end state.

The primary benefit of deploying a private cloud versus a public cloud is the ability to build your own on-premises infrastructure. This enables the highest levels of control over security, such as data protection and compliance, while also allowing you to define your own service-level agreements.

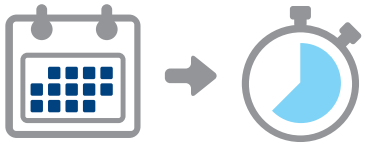
In building—and securing—your on-premises private cloud, you may discover that your existing data center infrastructure needs upgrading. Legacy infrastructures, even those with the highest levels of server virtualization, are often not delivering the performance and agility required for cloud services such as resource pooling, self-service provisioning and automatic chargebacks.

The path to building and securing the private cloud, therefore, often begins with a plan to modernize your infrastructure, which can evolve over time toward the desired end state. Your plan may ultimately culminate in a software-defined data center (SDDC), where you extend virtualization to storage, networking and security, allowing your entire infrastructure to be abstracted and centrally managed under a unified platform.

Software-Defined Data Center (SDDC) is the best option for architecting a private cloud.

Increase Agility

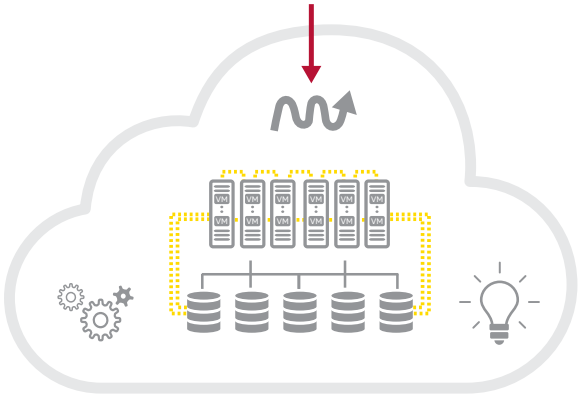
Deploy new revenue-generating apps in minutes, not weeks.



Reduce Capex and Opex

Reduce costs up to 75% vs. traditional infrastructure.[3]

End-to-End Visibility & Policy-Based Orchestration Across Private Clouds



Four key SDDC deployment technologies

In deploying the SDDC, here are four key technologies to be aware of:

1. **Virtualization:** In an SDDC, server virtualization is extended to storage and networking virtualization; the entire infrastructure becomes software-defined. You need to integrate security into this virtualized, software-defined architecture. With the combination of virtualized servers, storage, networking and security, IT teams can converge their infrastructure and manage it dynamically and centrally. This allows for new levels of agility, automation, orchestration and management simplicity.

2. **Micro-segmentation:** Micro-segmentation is a security approach specific to highly virtualized and software-defined infrastructures, leveraging the inherent automation and orchestration capabilities that are used to manage these environments. Micro-segmentation aims to reduce the risk of attackers moving freely within the data center perimeter. Therefore, security controls are wrapped around much smaller groups of resources to strengthen protection in the SDDC.

3. **Containers:** Many organizations are embracing container technology, particularly in support of DevOps. These self-contained execution environments have their own isolated CPU, memory, block I/O and network services but share the kernel of a host operating system. Because containers are much more streamlined than virtual machines (VMs), they make extremely efficient use of hardware resources compared with VMs.

4. **APIs and extensibility:** In a private cloud or SDDC deployment, APIs enable IT teams to integrate applications and other workloads with the underlying compute, storage and network infrastructure. APIs are the tools that enable software-based security service insertion. APIs also increase flexibility and agility, and they enable IT to adopt a more open private cloud deployment, supporting standards such as OpenStack.

Deployment Models for the Private Cloud

IT teams have several options for deploying a private cloud. Over the long term, the SDDC promises to become the definitive model, but there are ways to get there that do not require a “rip and replace” of your existing infrastructure. Here are your deployment options for building the private cloud infrastructure:

1. **Converged infrastructure:** With converged infrastructure, the compute, storage and network resources are virtualized and abstracted so they can be pooled and centrally managed through a unified management platform. Converged infrastructures are typically deployed through vendor-certified reference architectures or as pre-integrated, pre-validated appliances.

2. **Hyper-converged infrastructure:** A hyper-converged infrastructure is similar to a converged infrastructure in that the compute, storage and networking functions are virtualized, abstracted and centrally managed with a unified management platform. However, it is more tightly integrated and typically includes the virtualization software. It is offered as an integrated, pre-validated appliance and usually aimed at a specific application or workload, such as virtual desktop infrastructure (VDI). Converged and hyper-converged infrastructures are sometimes referred to as building blocks to the SDDC because they enable organizations to incorporate SDDC capabilities without impacting existing infrastructures.

3. **Software-defined data center:** The SDDC is widely regarded as the archetypal model for the data center of the cloud era. It offers organizations the benefits of private clouds, including cloud economics, agility, resource pooling, self-service and elastic scalability. The SDDC also accelerates DevOps and makes it simpler and less expensive for organizations to roll out new applications and business services, giving more power and control to business decision makers and line-of-business managers.

CHAPTER 2:
Security Challenges

In deploying any cloud deployment model or service, the primary concerns facing business leaders, CIOs, CSOs and other IT decision makers are typically around the areas of security, data protection, control and compliance.

IT leaders have much more faith in private cloud than public cloud in addressing these challenges. In a 2016 survey of 1,200 IT decision makers sponsored by Intel Security and conducted by Vanson Bourne, 47% of respondents say they completely trust on-premises and internally hosted infrastructure and 37% say they completely trust private cloud. In contrast, only 13% say they completely trust the public cloud.[4]

...while an on-premises private cloud offers the best opportunity to control security and compliance, it comes with security challenges of its own.

However, while an on-premises private cloud offers the best opportunity to control security and compliance, it comes with security challenges of its own. Private cloud is a new type of infrastructure—highly virtualized and software-defined—versus legacy data centers.

Whenever there is such a paradigm shift, it can create new opportunities for exploitation by those who would do harm to your business. That is certainly the case in today's environment. Targeted attacks traverse the private cloud environment differently than in a traditional data center.

IT and security teams must understand these new challenges and build in security solutions that achieve visibility and combat targeted attacks in this environment. Here are some of the specific challenges in securing the on-premises private cloud:

1. **Changing traffic patterns:** In a highly virtualized or software-defined private cloud, network traffic flows primarily in an east-west direction between virtual machines. Traditional point security solutions are not built for this type of traffic; they protect north-south traffic, or traffic that flows through the data center's perimeter. These traditional solutions lack visibility into the east-west traffic that stays within the data center, thereby creating a gap in protection. If solutions do not inspect east-west traffic, internal threats can propagate laterally inside the data center.

2. **One compromised server attacking another:** This can be an outcome of changes in internal traffic, or it could be a challenge when your on-premises private cloud is part of a hybrid cloud environment through a platform as a service or other use case.

3. **Gaps in protection:** In a highly virtualized private cloud environment, automation is critical. As new VMs are dynamically provisioned, you will experience security gaps if policies and protections are not applied to them immediately. In the private cloud, you can apply security through a virtualized or software-defined model that leverages automation and orchestration of security policies.

4. **Increased risk caused by manual processes:** If your legacy security solutions are not highly automated, you increase the risk of errors caused by manual processes. In an era when always-on availability is a business requirement, manual processes create unnecessary risks when provisioning and securing infrastructure.

5. **Performance impact:** If you are running traditional antivirus in a highly virtualized cloud environment, it will cause a tremendous negative impact on performance and operations.

6. **Compliance concerns:** Different geographic regions have different regulatory requirements for data protection and privacy. As data and applications flow through the cloud—private, public or hybrid—you must adhere to policies for each location in which you do business.

CHAPTER 3:
Security Benefits

Along with the challenges of securing your private cloud environment there are also huge benefits. If you build in the right security model from the beginning, you can make it much simpler and more cost effective and efficient to dynamically manage security, data protection and compliance.

In addition, by addressing security as a critical and integrated component of the software-defined architecture, you can leverage a security-as-a-service model that represents a fundamental shift in how you manage and deploy security.

...by addressing security as a critical and integrated component of the software-defined architecture, you can leverage a security-as-a-service model that represents a fundamental shift in how you manage and deploy security.

Here are some of the tangible benefits you can deliver if you take a holistic, integrated approach to private cloud security:

1. **Reduce complexity and close security gaps:** Using automation and orchestration tools across the entire infrastructure, your IT teams can easily provision new users and upgrade existing ones. What's more, you can close security gaps because all security functions and policies follow workloads as they are created, scaled, migrated and decommissioned.

2. **Lower costs with security as a service:** When security is built into the private cloud infrastructure, you can adopt a service-centric model for deploying security and save money by delivering security as a service. Business departments can choose the type of security they need and pay an appropriate fee for that service.

3. **Improve agility and accelerate time to market:** With security services provisioned and upgraded dynamically, it is much easier and safer for DevOps and business teams to leverage the cloud to accelerate the development of services and applications. They can have confidence that the security is built in without needing to go to IT. This is particularly valuable for applications development teams, which can use the private cloud to spin up new, secure infrastructures for test and development.

4. **Reduce risk through compliance automation:** With security built into the virtualized infrastructure, you can prove that security policy is in place and maintained at all times. Build your security model into a VM and network template and validate it as compliance. Thereafter, every VM spun up from that template automatically inherits its validation.

CHAPTER 4: Securing the Private Cloud

IT and security teams need to understand how to minimize the challenges of securing the private cloud. At the same time, they must deploy a security platform that drives agility, accelerates DevOps and delivers other business benefits.

First, include security when planning the transition to private cloud. Your CSO and security architect experts need a seat at the table in setting strategy and building the execution plan for the private cloud.

These are the key technologies to incorporate:

1. **A virtualized network security platform for intrusion prevention:** This solution should be designed for the unique demands of virtualized environments, tightly integrated with the hypervisor to discover and block threats in virtual networks.

2. **Antivirus optimized for virtual environments:** You need a view into virtual data centers to gain complete visibility into all VMs. Once you've achieved that visibility, you need antivirus protection that is deployed automatically to cover all machines, with minimal performance impact and built-in cache sharing.

3. **Threat intelligence:** Leverage threat intelligence to get immediate visibility into the presence of advanced targeted attacks, sharing relevant security intelligence among endpoint, gateway, network and data center security solutions.

4. **Threat defense:** This should let you close the gap from encounter to containment by detecting advanced targeted attacks and converting threat information into immediate action and protection.

5. **Virtual security controller:** This is a new type of controller that enables network function virtualization by providing abstraction for the security infrastructure within the SDDC. It should enable security function virtualization by virtualizing and abstracting common security functions such as antivirus, intrusion prevention, sandboxing, firewall, Web filtering and data loss prevention.

Key steps to secure the private cloud

To ensure the highest levels of security for your private cloud deployment, follow these four critical steps:

1. **Formulate an overall security strategy** as part of the architecture, and monitor how it is executed every step of the way.

2. **Build in security** so protections and policies are automatically provisioned with all upgrades, additions and adaptations of the infrastructure.

3. **Leverage an integrated set of solutions** that work together to give you the highest levels of visibility, insight and protection.

4. **Ensure that your solution uses automation, integration and orchestration** to simplify deployments, reduce risk, and achieve and maintain compliance.

Your CSO and security architect experts need a seat at the table in setting strategy and building the execution plan for the private cloud.

6. **Centralized management platform:** You need to unify security management across endpoints, networks, data, clouds and compliance solutions, with the ability to create automated workflows between security systems and IT operations systems to quickly remediate outstanding issues.

How do you secure the SDDC?

Ensure security is built into the SDDC architecture.

A core security strategy is an integral aspect of the entire SDDC architecture solution.

Utilize integrated security solutions.

Extend visibility, control, and threat protection from the SDDC to the cloud.

Deploy a software-defined security model.

Leverage automation, orchestration, and dynamic scalability to manage security across the entire infrastructure.

Deploying an Integrated Model for Private Cloud Security

Rather than separate solutions from a diverse group of vendors, you need an integrated, coordinated approach to private cloud security. Therefore, you should work with a single vendor that not only offers all of these solutions, but also provides tight integration among them to provide the highest levels of coordinated protection.

Intel Security delivers a fully integrated portfolio of solutions for next-generation private cloud security that allows you to achieve all of your critical security goals. Further, your Intel solutions are future-proofed as you evolve to the SDDC. The Intel Security portfolio consists of:

1. **McAfee® Virtual Network Security Platform,** a full-featured advanced intrusion prevention system designed specifically to meet the needs of virtual environments.

2. **McAfee® MOVE AntiVirus,** which brings optimized malware protection to virtualized desktops and servers.

3. **McAfee® Threat Intelligence Exchange,** which enables adaptive and collaborative threat detection and response, providing organizations with superior visibility and control against emerging and targeted attacks.

4. **McAfee® Advanced Threat Defense,** enabling IT to detect advanced targeted attacks and convert threat information into immediate action and protection.

5. **Open Security Controller,** which is the industry's first security controller that enables automated and dynamic security provisioning, synchronization, protection and remediation for the SDDC.

6. **McAfee® ePolicy Orchestrator® (McAfee ePO™) software,** which provides integrated security and central policy management across all cloud deployments, enabling IT to discover and gain visibility into all VMs.

CHAPTER 5:
Conclusion and Next Steps

Private cloud is one of the critical deployment architectures IT teams are adopting as they transition to a service-centric delivery model. More than 75% of organizations[5] already use private clouds to lower costs, increase agility and exert greater control over security, data protection and compliance.

The transition to private cloud represents a paradigm shift in how IT is provisioned and data centers are deployed. Virtualization is expanding beyond servers into storage and networking, while software-defined models allow new levels of agility through advanced automation and orchestration.

Security technologies and techniques of legacy data centers do not carry over into cloud. Organizations must take a fresh approach to cloud security that recognizes and leverages the shift to highly virtualized software-defined environments.

This shift has a big impact on how IT and business leaders approach security. Security technologies and techniques of legacy data centers do not carry over into cloud. Organizations must take a fresh approach to cloud security that recognizes and leverages the shift to highly virtualized software-defined environments.

The cloud era provides both challenges and opportunities. The challenges are represented by a changing threat landscape that takes advantage of new gaps in protection as well as changes in how data and applications are delivered. The opportunities are in deploying a more strategic approach to cloud security that not only closes these gaps, but also creates an integrated security model that provides greater protection over the long term.

By taking a strategic, built-in, service-centric approach to security, organizations will improve security and compliance, while simplifying IT operations, reducing costs, accelerating time to value and future-proofing their organizations as security challenges continue to evolve.

Building the right strategy and building in the security model are great starting points, but you also need to deploy security technologies that have been designed for virtualized environments and software-defined architectures. That is why it is critical to partner with a security provider that understands the challenges of the cloud era and has designed an integrated portfolio of solutions that provides a safe, secure and compliant path to private cloud.

For more information on how we can help you take the next step, please visit intelsecurity.com/privatecloudsecurity.

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

1 "RightScale 2016 State of the Cloud Report," RightScale, Feb. 9, 2016
2 "State of the Market: Enterprise Cloud 2016," Verizon, Nov. 9, 2015
3 VMWare, Global Financial Institution Selects Software-Defined Data Center http://vmw.re/1QMuguY
4 "Blue Skies Ahead? The State of Cloud Adoption," Intel Security, Apr. 14, 2016
5 "Cloud Computing Trends: 2016 State of the Cloud Survey," RightScale, Feb. 9, 2016