Securing the Next-Generation Data Center

Build security into the design phase for maximum flexibility and advanced threat reduction

Key Points

- Data center upgrades are pervasive, driven by needs to:
  - Reduce risk
  - Increase service availability/uptime
  - Enable flexibility to support rapidly changing market dynamics and new on-demand services
- Forecasts for server virtualization remain robust in 2011 and beyond
- Virtual desktop infrastructure assessments and deployments on the rise

"The need for security must not be overlooked or 'bolted on' later during the transition to private cloud computing."

"By 2015, 40 percent of the security controls used within enterprise data centers will be virtualized, up from less than 5 percent in 2010."

"By 2015, 70 percent of enterprises will allow server workloads of different trust levels to share the same physical hardware within their own data center, except where explicitly prohibited by a regulatory or auditor compliance concern."

—Gartner Group

Data center security has traditionally been "bolted on" after the fact rather than built in during the architectural design stage. Because today's data centers must be optimally available, flexible, resilient, and secure, the traditional approach compromises their primary intent: robust and uninterrupted service delivery. While a reactive approach has worked with centralized, monolithic data centers of the past, it's no longer viable. Today's modular, hybrid and distributed next-generation data centers (NGDCs) remove the traditional perimeter. Hard-coded "trust boundaries" that organizations rely upon to secure their critical assets are evaporating.

The advantages of specifying defense-in-depth security solutions at the outset of a data center build-out, upgrade, or consolidation are numerous. Proactively demarcating physical and virtual resources, securing virtual machines, establishing trust zones, implementing deep visibility for advanced situational awareness, and formulating enforceable policies constitute a new set of best practices. The upside? Business-critical services can be deployed more quickly and reliably across physical, virtual, and cloud (PVC) environments. Equally important, these services can benefit from higher availability, greater levels of security, and compliance. In short, built-in security goes well beyond threat prevention. It is a strategic set of enabling technologies that allow mid-sized to large organizations to realize dramatic improvements in operational efficiencies across business units.

This brief examines:

- The velocity of hybrid NGDC deployments
- The security challenges presented by NGDC architectures
- Adaptive NGDC security requirements that can apply hybrid policies and controls to hybrid data center technologies
- How to leverage McAfee® NGDC security solutions spanning networks, servers, data, and storage systems operating in PVC environments

The Velocity of Hybrid Next-Generation Data Center Deployments

The widespread adoption of virtualization, cloud computing technologies, and flattened network architectures is emerging as a fact of life in NGDCs, even for mid-sized organizations deploying just a row of server racks. There is a confluence of drivers at play. Ramped up and accelerating demand for new services, budgetary constraints, and globalization are among the chief influencers fueling this adoption.

Virtualization Is Mission Critical

Data centers are embracing virtualization to enable consolidation (reducing the number of data centers) and increase resource utilization (leveraging shared compute servers to meet peak capacity requirements without additional capital expenses). However, security and compliance concerns remain because most virtualization projects rely on traditional and outdated security models. This introduces significant risks such as not knowing how many or where virtual machines (VMs) are running, whether or not trust boundaries established in the physical environment have been properly migrated to the virtual environment, and whether or not the VMs are secure. And, organizations are rarely willing to minimize the cost savings associated with virtualization by increasing workload and management in other areas like security.

Cloud Computing's Growing Role

Cloud computing introduces additional risks and complexities, especially with public cloud designs where multiple, independent customers share virtualized physical assets. As a result, many IT teams have compromised on a hybrid cloud, in which an organization provides and manages some resources in-house (private cloud) and has others provided externally (public cloud). The hybrid cloud increases utilization of compute and storage resources and sidesteps some of the security concerns of shared resources with other tenants.

The New Flat Network: Management Blind Spots

To maximize the benefits of virtualization and cloud computing, the concept of a "flat" data center network is gaining traction. Flow-based, non-blocking, shortest path network fabrics are being tested to maximize network performance. As this design moves into production, data center teams must ensure that firewall, intrusion detection and prevention, and anti-malware systems are interoperable with new flat network standards to avoid management blind spots.

Adaptive NGDC Security: Applying Hybrid Controls to Hybrid Data Center Technologies

What's clear moving forward is that NGDCs will comprise a hybrid combination of physical, virtual, and cloud computing environments. NGDCs will deploy on-premises security appliances for high-bandwidth applications at physical boundaries. As virtualization is deployed for greater efficiency and scalability, comparable security practices must be implemented in virtual environments. Ideally, these best practices will provide streamlined security management across both physical and virtual environments. And private and public cloud environments will capitalize on software-as-a-service (SaaS) and/or infrastructure-as-a-service (IaaS) implementations to address on-demand peak capacity and overlay controls. That said, "trust but verify" checks and balances must accompany the security practices and controls for those implementations (but without increasing workload).

What this strongly suggests is that for policy enforcement to be effective in the hybrid NGDC—that is, meet uninterrupted service delivery and intensifying risk management requirements—it must be applied on a ubiquitously managed and persistent basis. This suggests that secured trust "zones" will displace legacy concepts of trust "boundaries" typically associated with the centralized, monolithic data center model of yesterday.

These dynamics point directly at vendor consolidation as a logical means of interconnecting security controls, policies, monitoring and reporting. And this goes well beyond "centralized" management paradigms. Instead, the hybrid NGDC requires a "unified" management construct that will free up security resources to focus on nullifying potential attacks that can cripple critical assets and disrupt essential operational and revenue-generating services.

In response to these far-reaching influences on the security posture of NGDCs, McAfee is launching a comprehensive security initiative that provides practical guidelines, reference architectures, and other tools and services to safeguard critical assets and optimize business operations and on-demand services supported by mid-sized to large data centers. Edge-to-edge core McAfee solutions, in concert with its strategic partner technologies, enable network design and security professionals to implement essential security strategies as data centers are in various build-out stages. This initiative is specifically designed to help customers achieve the highest levels of data center service availability, reliability, risk protection, and compliance.

Leveraging Next-Generation McAfee Data Center Security Solutions

McAfee recognizes NGDCs will become:

- *Modular*—The monolithic data center will be re-assembled into its essential elements: compute (server and mainframe), storage, network, data, and policies so each can be fully optimized for operational efficiency
- *Hybrid*—To achieve this optimization, the first four elements—compute, storage, network, and data resources—will be re-deployed in a combination of physical, virtual, and private or public cloud environments
- *Ubiquitously managed*—Policy development and enforcement will work within a unified management environment, including dashboards and reporting, that spans this hybrid physical, virtual, and cloud infrastructure.

In recognition of the scope of security measures required to safeguard mid-sized to large data centers, McAfee is leveraging deep relationships with McAfee Global Alliance, McAfee® Security Innovation Alliance, Service Provider, Technology Alliance, and Reseller partners. Collectively, McAfee products and ecosystem partners offer fundamental principles and technologies that enable network design and security professionals to implement core security strategies without eroding the service delivery, efficiencies, and cost advantages associated with next-generation data centers. These strategies reflect the fact that, as data centers are in various build-out stages, they are designed to achieve the highest levels of service availability, reliability, security, and compliance.

Stage	Strategy	Core McAfee Products and Technologies
Modular: **For the highest availability and integrity, build security and compliance into your NGDC, don't bolt it on**—Security controls will be more effective if they are designed in as part of the architecture, optimized for each **modular** component: servers, storage, data, and network, united by a common policy environment.	**1: Risk assessment to assure data center integrity:** • An enterprise-wide risk assessment with real-time visibility is an essential starting point to prioritize security investment • McAfee delivers real-time predictive protection (McAfee Global Threat Intelligence™) across all key threat vectors—file, web, message, and network via its security products to pinpoint at-risk critical assets.	• McAfee® Risk Advisor • McAfee® Vulnerability Manager • McAfee Vulnerability Manager for Databases • McAfee® ePolicy Orchestrator®
	2: **Securing data at rest, in use, in motion. McAfee solutions deliver:** • Complete protection for data at rest, in motion, and in use (databases, applications, servers) • Discover and protect databases with a set of preconfigured security defenses, including virtual patching updates • Delivers confidence migrate data safely between workloads	• McAfee Data Loss Prevention • McAfee Database Activity Monitoring • McAfee VirusScan® for Storage
	3. **Secure workloads: McAfee offers a holistic approach:** Host-level ◦Secure against fast-changing threats with dynamic whitelisting and blacklisting anti-virus ◦Continuously detect system-level changes across distributed and remote locations • Hypervisor enabled ◦ Improves server resource utilization • Intra-VM network security ◦ Apply intrusion prevention and access control policies to monitor Intra-VM traffic ◦ Isolate virtual machine traffic with virtual firewall instances	• McAfee Total Protection™ for Server (McAfee Application Control, McAfee AntiVirus, McAfee Change Control, and McAfee Policy Auditor) • McAfee® Management for Optimized Virtual Environments (MOVE) AntiVirus for Servers • McAfee Network Security platform with Reflex integration • Next-generation McAfee® Firewall Enterprise with policy enforcement across both physical and virtual environments
	4. **Secure virtual desktop infrastructure:** • Optimizing and offloading McAfee VirusScan software's processing enables customers to achieve higher operational returns	• McAfee MOVE AntiVirus for Virtual Desktop Infrastructure (VDI)

Stage	Strategy	Core McAfee Products and Technologies
Hybrid: For the least complexity and the most flexibility and scalability in service delivery (elastic, on-demand services) link security policies to context, identity, and applications across your hybrid infrastructure (PVC). Services can better meet evolving business needs, expanding the strategic role IT plays in enabling business.	5. **Replace physical trust boundaries with secure trust zones, both logical and physical, that cross PVC:** • McAfee network security offerings with Brocade ◦Feature an identity-based strategy that enables IT to apply policies across PVC ◦Eliminate occurrence of inconsistent policies and reduce vulnerabilities ◦Provide a single "pane of glass" to manage policies across both physical and virtual instances	• Next-generation McAfee Firewall Enterprise • Brocade • McAfee Network Security platform with Reflex integration
	6. **Apply context, identity, and application-aware policies:** • McAfee technologies: ◦Make it easy to manage policy by users, groups, and applications, improving efficiencies and accelerating policy-based enforcement timeframes ◦Secure all web, email and data traffic moving between an organization and the public cloud	• Next-generation McAfee Firewall Enterprise • McAfee content security platform
Ubiquitously managed: For efficient risk and compliance management, federate, don't silo. Efficient operations will come from using ubiquitously managed policies to secure workloads and connect network, server, and storage activities in physical, virtual, and cloud infrastructures.	7. **Unified policies, visibility, and reporting:** • McAfee technologies: ◦Measure compliance to SLAs, internal IT policies, and regulatory standards such as PCI DSS, HIPAA, Sarbanes-Oxley, GLBA, and SAS-70 ◦Deliver real-time insight into policies and an organization's security posture across data, applications, endpoints, servers, and networks	• McAfee Policy Auditor • McAfee Vulnerability Manager • Next-generation McAfee Firewall Enterprise • McAfee Database Activity Monitoring • McAfee Change Control
	8. **Ubiquitous or pervasive access:** • McAfee technologies: ◦Enable an enterprise or cloud provider to deliver comprehensive access control for cloud applications ◦Deliver end-to-end assurance for today's and tomorrow's enterprise networking and security needs—from the edge to the core of the data center	• Intel Expressway Cloud Access 360 • McAfee ePolicy Orchestrator • Next-generation McAfee Firewall Enterprise • Brocade

Certified Solutions For NGDC Infrastructure Reference Architectures

In conjunction with its partner ecosystem, McAfee provides certified solutions for data center reference architectures across multiple dimensions:

Network

- McAfee and Brocade are partnering on a portfolio of offerings that blend network innovations and security management to address the challenges of both physical and virtual environments. This unified approach eliminates bottlenecks, inconsistent network policies, management blind spots, and security loopholes. The joint solutions help maximize network availability and enhance threat protection to defend against high-volume attacks.
- McAfee and Crossbeam are partnering to deliver the McAfee Firewall Enterprise on the Crossbeam X-Series platform. The joint solution helps large enterprise and service provider customers optimize their data centers through network and security services consolidation, greatly reducing operational complexity and cost. Combining our industry-leading next-generation firewall with Crossbeam's carrier-class hardware platform is intended to allow customers to realize increased performance, scalability, reliability, and change readiness of security services within their data center.

- Reflex integrates virtual and physical security and management in McAfee Network Security Platform for system-wide monitoring and compliance reporting across current and next-generation data center infrastructure
- McAfee and Riverbed have partnered to address IT initiatives for data center consolidation and server centralizations by delivering advanced wide-area network optimization and branch office security together on a single device. By leveraging the Riverbed Services Platform (RSP) on Riverbed Steelhead, McAfee and Riverbed can address both application performance and security challenges, while helping to reduce total cost of ownership.

Servers

- McAfee Total Protection software for Server and McAfee MOVE AntiVirus have been certified with HP Cloud Maps for HP's BladeSystem Matrix reference architecture. HP Cloud Maps provide a technical guide to automate infrastructure and application provisioning and deployment on HP BladeSystem architectures, enabling organizations to accelerate the deployments of private clouds securely. In addition, HP Information Security offers consulting and managed security services for McAfee Total Protection for Server and McAfee MOVE AntiVirus deployments.

Storage

- McAfee and NetApp are collaborating on joint solutions to help ensure business continuity by protecting network-attached NetApp storage devices against viruses and other malware. This includes the market's first fully integrated on-board anti-virus solution (McAfee® VirusScan® Enterprise software) for Data ONTAP 8.1 customers.
- EMC is an active member in the McAfee Connected for Storage Partner Program and has certified McAfee VirusScan Enterprise for Storage software with Celerra and VNX series network-attached storage devices

Virtual Desktop Infrastructure (VDI)

- The *Cisco Validated Design Guide* provides design considerations and guidelines for deploying an end-to-end Cisco Virtualization Experience Infrastructure (Cisco VXI). McAfee MOVE is the only endpoint security solution included in the guides offered for both Citrix- and VMware-based deployments.
- McAfee MOVE is an approved and recommended endpoint security solution for Dell's Virtual Desktop Infrastructure
- McAfee MOVE AntiVirus for VDI is also included in the HP Cloud Maps for HP's Blade System Matrix reference architecture
- EMC includes McAfee VirusScan for Storage software in its published VDI reference architectures for Citrix and VMware

As a certified solutions provider for these vendors' published reference architectures, McAfee and its strategic partners are helping customers address their security needs in the design and implementation stage, rather than retrofitting security for existing systems.

Summary

By building in comprehensive security measures at the design and architectural phase of NGDC build-outs, organizations can preemptively optimize business-critical service availability by minimizing potential downtime through greater resiliency. Forward-thinking enterprises that take this route are in a much better position to deploy new on-demand business services more quickly and safely while maintaining efficiencies.

As NGDCs evolve with rapidly changing PVC infrastructures, the need to improve risk and compliance management becomes greater than ever. And with the rapid onset of PVC environments, IT and security managers will face mandates calling for significant reductions in operational complexity and cost. While the "bolt on, after-the-fact" approach to security was the modus operandi in monolithic data centers of yesterday. However, today's flattening, modular, and hybrid architectures of future NGDCs require a proactive, strategic approach to dramatically improve service delivery while reducing risk and improving compliance. In order to achieve optimal security for NGDCs, it comes down to two words: advance planning.

To learn more about securing your next-generation data center, visit mcafee.com/datacenter or contact your local McAfee authorized reseller. They'll work directly with you on current and future NGDC plans to ensure that you implement the right security measures to meet the needs of your growing organization.

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

31100brf_securing-next-gen_0711_fnl_ETMG