White Paper

Discover. Protect. Expand.

The next big thing in data center security.

intel Security

Table of Contents

Enterprise data centers are undergoing a rapid transformation driven by changing business requirements that range from economic factors and regulatory compliance to demands for greater collaboration and anywhere, anytime access to corporate resources. Modern data centers now encompass physical, virtual, and cloud servers. Companies are investing in technologies like virtualization and cloud computing to drive down costs, satisfy requirements of business users, and achieve a higher level of automation and efficiency—all of which benefit productivity, innovation, and the bottom line. But in the midst of this exciting transformation, IT is concerned about the security challenges presented by the new hybrid data center. As Gary Lovelan of PricewaterhouseCooper points out, "Typically in this industry, the adoption of any technology happens well before security considerations surrounding it are fully addressed."[1] In this white paper, we'll examine these issues and demonstrate how McAfee and Intel technologies provide a holistic, integrated solution that addresses security from the chip level through the multiple layers of the software stack across physical, virtual, and cloud infrastructures.

> *"The data center has become a key component for any organization. As the business platform of the twenty-first century, more of the critical services and offerings being delivered to the end user originate in the data center. And almost all new technologies are being deployed within the modern data center. This includes big data, IT consumerization, and, of course—cloud computing."*[2]
>
> —Latisys, *Hybrid is Here—Your Guide to Understanding the Convergence of Data Center, Hosting and Cloud*

The Modern Data Center

Let's take a brief look at the new types of environments found in the modern data center.

- *Virtualized environments or private clouds*—These refer to single physical machines, which are located and managed on premises, running multiple virtual machines with their own operating system and applications. These virtual machines provide a variety of services and can be scaled up, reallocated, or moved around as needed. The advantages are added flexibility with complete transparency to the user plus significant cost savings.
- *Public cloud services*—In this case, enterprises leverage computing resources offered by various types of providers. For example, Platform-as-a-Service (PaaS) providers offer hardware and software infrastructures for enterprises to develop their own Internet applications. An example is Amazon Web Services (AWS). Software-as-a-Service (SaaS) providers, like Box.com, offer specific applications over the Internet, so companies have no need to host, update, and manage these applications on premises.

Security Challenges of the Hybrid Data Center

There's no doubt that the vast majority of enterprises are convinced of the benefits of cloud computing and virtualization. As the Aberdeen research brief *Evolve Your Datacenter*? *Evolve Your Security* points out, 55% of applications were virtualized in 2012, and that number is expected to grow rapidly.[3] The key advantage is that IT can react much more swiftly to changing business needs and can bring up new workloads in a few hours rather than weeks. The hybridization of the data center is also motivated by the desire to reduce Total Cost of Ownership (TCO) by shifting at least some workloads into the cloud.

But some IT managers are hesitant about deploying these technologies in their data centers because of the security risks. Workloads that rely on public clouds run on infrastructures that are not controlled by the enterprise, so the onus is on IT to make sure that security policies, controls, and processes are aligned with business needs. This potentially puts IT in an uncomfortable position. According to the Intel survey *What's Holding Back the Cloud?*, 91% of IT professionals are interested in a real-time service that could measure the security of providers, and 51% want to feel confident that workloads are running on trustworthy infrastructures.[4]

When it comes to securing the new data center, all IT teams aspire to accomplish the same overarching goal: ensure that applications run in the most optimized environment for the best performance, the highest level of trust, easy user accessibility, and continual compliance. If we drill down a bit deeper, we find the four fundamental challenges:

- *Discovery*—Enterprise security teams need a better way to detect and identify workloads so they can apply proper security control and policies across the various types of deployments: physical, virtual, and private cloud deployments. As workloads are migrated into public cloud environments, such as Amazon Web Services (AWS), this becomes even more challenging.
- *Comprehensive security with minimal performance impact*—Many security solutions can bog down performance, which impacts user productivity and business agility. Enterprises need a better way to protect workloads on physical and virtualized servers, whether they are on or off premises, while ensuring a high level of performance and an optimal level of virtual machine (VM) density to keep up with business demands efficiently.
- *Provisioning security policies to the public cloud*—More and more corporate users are accessing public cloud solutions—sometimes without IT authorization—so it's a challenge to apply the proper security policies to their workloads.
- *Streamlined security management*—Siloed security products bring with them a level of complexity that makes management challenging and offer low visibility into the data center's security posture. Also, with disparate management consoles and lack of integration among security solutions, remediation and reporting are slower and more tedious—and this also impacts security posture.

In response to these challenges, many enterprises simply avoid or limit expansion into the cloud, since the security requirements are so different. Others have followed the trend but have simply given up on applying consistent security policies across physical, virtualized, and cloud environments. More often than not, for lack of a better solution, enterprises end up relying on security measures they already know about or are comfortable with—such as traditional antivirus and blacklisting—in spite of the fact that these solutions are inadequate and have high performance impact.

McAfee Server Security Suites

The McAfee® Server Security Suite Essentials and the McAfee Server Security Suite Advanced tackle the challenges of safeguarding the hybrid data center by helping IT *discover* all workloads, *protect* servers from known as well as complex zero-day threats, and *expand* workloads securely into the cloud, both private and public. These suites enable enterprises to automatically apply the same security policies and controls across all servers to ensure that precious corporate data is protected. The cornerstone of this comprehensive approach to data center security is the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console, which facilitates these three key processes and provides ultimate visibility across the entire data center.

Discover

In the new data center model, virtual machine (VM) instances are constantly changing according to shifting business needs and data center configurations. To properly secure the virtual environment in the data center, IT first has to locate all VM instances. Until recently, enterprises could not get full visibility into their virtual infrastructures. As they moved from on-premises data centers to hybrid and fully hosted data centers, it has been difficult to identify the relationship of VMs to specific hosts and their locations. Discovery of virtual and physical servers is paramount because you simply cannot secure what you cannot see.

Thanks to McAfee Server Security suites, things have changed dramatically. With McAfee ePO software serving as a "single-pane-of-glass" management hub, you get a view of all registered data centers and workloads, on premises at the enterprise data center and off premises on servers accessed through the cloud—including actionable information like anti-malware status. Through the McAfee ePO console, IT can accomplish the following:

- Automatically discover all virtual and physical machines.
- See the relationship between hypervisors, virtual machines, and virtual appliances.
- Gain insights into their security status.
- Manage updates, remediations, and policies.

The customizable data center dashboard within McAfee ePO software displays key metrics for all McAfee Server Security suite products, along with historic security data and overall trends. Whitelisting status is displayed as well, and applications are categorized as "Known Good," "Known Bad," or "Grey List."

Data center connectors, which are part of the McAfee Server Security suites, automatically discover cloud instances so that administrators can then ensure that the security posture in their on-premises data centers and cloud-based data centers are aligned. These connectors provide you with critical information:

- The host on which a particular VM is running.
- The data center where the VM resides.
- Whether the VM is in the private cloud or public cloud.

Data center connectors are available for VMware vSphere, Amazon AWS, OpenStack, and Microsoft Azure. They allow IT to import workloads directly into McAfee ePO software, offering visibility beyond just the workloads protected by McAfee.

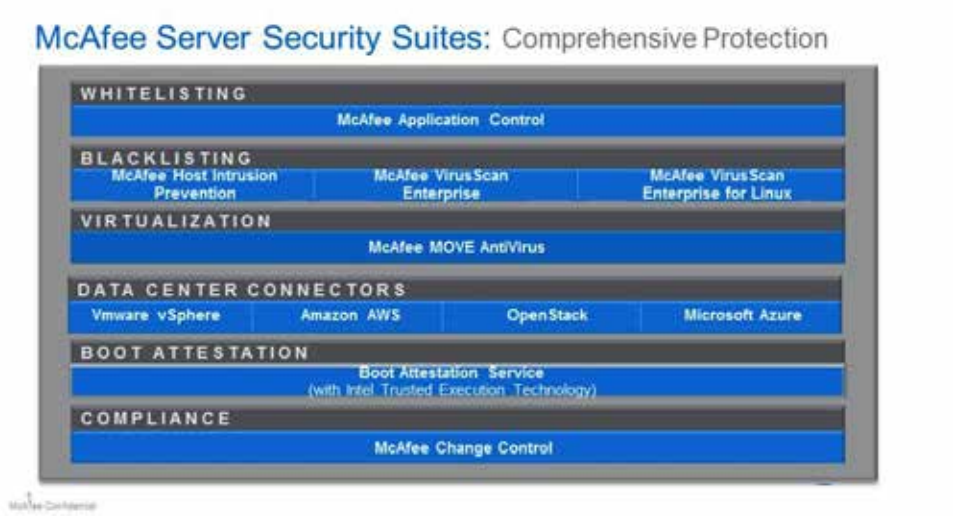

Figure 1. Comprehensive, layered protection provided by McAfee Server Security suites.

Protect

Perhaps one of the biggest challenges of securing today's multifaceted hybrid data centers is keeping downtime to a minimum and ensuring adequate data protection without sacrificing performance. The SANS Institute suggests that the complexities of today's data centers demand solutions that bring together "various technologies to securely provision servers, manage vulnerabilities over time, protect access to information, rapidly identify threats as they appear, and improve network security operations."[5] Traditional point security solutions are limited in scope, haven't kept up with advancements in virtualizations, and have ignored the cloud completely. In fact, as IT scrambles to keep up with increasing business requirements for high performance and accessibility to applications, virtualized environments end up underprotected or unprotected. What's needed now is a unified suite of server security solutions that:

- Provide centralized visibility and management across physical servers, virtual servers, and cloud environments.
- Consume less computing resources, unlike, for example, typical blacklisting technologies that must scan and rescan to detect threats.

Enjoy comprehensive, layered protection.

McAfee Server Security suites meet all of these requirements, offering comprehensive security with multiple layers of integrated core threat protection for both physical and virtual deployments, on premises and in the cloud. The suites combine antivirus for Microsoft Windows and Linux, antivirus optimized for virtualized environments and host intrusion prevention. In addition, McAfee Server Security Suite Advanced provides whitelisting, change control, and an agentless host firewall for VMware environments. McAfee ePO software, with its data center dashboard, ties these technologies together and provides centralized management and reporting, as well as the ability to distribute policies to all environments—physical, virtual, and the cloud. According to John Jon Oltsik, senior principal analyst, information security and networking at Enterprise Security Group, McAfee Server Security suites "provide an enhanced security posture while maintaining the high server performance needs of the data center."[6]

Protect against malware.

Data center servers are favorite targets for cybercriminals because they contain the corporate "crown jewels"—high-value assets like intellectual property, financial information, customer lists and personally identifiable information (PII), and human resources records. According to the *2014 Verizon Data Breach Investigations Report*, servers are more susceptible to breaches than any other corporate asset: "Servers have typically been on top, probably because attackers know that's where the data is stored."[7] In the past, traditional blacklisting technologies would have been considered a viable solution for securing physical servers, but it's not enough to protect valuable assets from today's complex and often evasive threats, not to mention the fact that these solutions are not optimized for virtualized environments. The ideal remedy for known and zero-day threats that put data centers at risk is a solution that extends various layers of strong anti-malware technologies to physical servers and virtual machines.

McAfee Leads the Industry in Threat Protection

- In a recent NSS Labs comparative analysis, McAfee achieved the highest possible score in protection against exploit and evasion attacks.
- A West Coast Labs study showed that McAfee Application Control, McAfee Host Intrusion Prevention, and McAfee VirusScan Enterprise provided 100% malware protection against 7,300 malware samples by allowing only authorized software to run on COE and fixed-function computers.

McAfee Server Security suites do exactly that. They include anti-malware protection for physical servers that is ranked number one by NSS Labs against zero-day exploits and evasion attacks. With signature-based blacklisting technologies, like McAfee VirusScan® Enterprise, built into its antivirus capability, and host-based intrusion prevention, the suites can:

- Cut down on the frequency of signature scanning, which reduces processing overhead to a minimum—a significant boon to efficiency.
- Reduce the frequency of urgent security patching.

In addition, McAfee Server Security Suite Advanced can:

- Shield servers from both known and zero-day malware.
- Safeguard newly scanned systems from malware by allowing only authorized application codes to execute.

Choose flexible antivirus scanning options for virtual machines.

An important component of McAfee Server Security suites is McAfee Management Optimized for Virtual Environments (MOVE) AntiVirus, which is specifically designed for virtual environments. McAfee MOVE AntiVirus supports major hypervisors (VMware, Citrix, Hyper-V, Kernel-Based Virtual Machine, and others) and offers ultimate deployment flexibility with agent or agentless deployment. It protects while ensuring unimpeded hypervisor performance by offloading scanning and .DAT updates. Security is uninterrupted as VMs move between hypervisors.

Agent deployment increases efficiency.

In multiplatform installations, the McAfee MOVE AntiVirus agent runs on each guest image while the McAfee ePO software agent oversees scanning and policy configurations for individual VMs or a group of VMs. When a user accesses a file or initiates a task that involves accessing a VM, the McAfee MOVE AntiVirus Offload Scan Server is notified. If the file has been scanned before and is deemed safe, no scanning is required; this is called "scan avoidance." In the case of a file that has not yet been scanned, an on-access scan is performed and results are reported to the VM. All antivirus scanning occurs over the network with agent deployment. If security issues arise, a pop-up alert notifies the user, and files are quarantined, awaiting further action. This type of deployment is highly efficient—a single security virtual appliance (SVA) can handle many as 450 VMs.

McAfee MOVE AntiVirus Advantages

- Offload antivirus scanning to an SVA for instant protection with minimal impact on memory and processing.
- Prevent antivirus storms by using options that include on-access, scheduled, and selective scans.
- Minimize setup and updates with a dedicated, hardened virtual appliance.
- Block even the most recent threats by leveraging file analysis through McAfee Global Threat Intelligence service.
- Leverage McAfee ePO software for visibility, control, and reporting across your endpoints.
- Support all major hypervisors through multivendor or agentless deployment options.

Agentless deployment increases scanning speeds.
McAfee MOVE AntiVirus also offers an adaptive, agentless alternative integrated with VMware vShield, which offloads antivirus processing to the McAfee MOVE Antivirus SVA. vShield uses the hypervisor to make a high-speed connection with the SVA. During the scanning process, the McAfee MOVE AntiVirus SVA instructs vShield to cache good files or delete or deny access to files that contain malware. Once you install McAfee MOVE AntiVirus SVA on VMware ESX servers, you can rest assured that every virtual image is protected the moment it is created. There is no need to install a McAfee software agent on VMs because communication between McAfee MOVE AntiVirus SVA and virtual images happens via the VMware tools. This significantly boosts scanning speeds, and you can be confident about security because VMs are automatically protected.

Fine-tune scanning performance.
Diagnostics and flexible tuning policies in McAfee Move AntiVirus help you further enhance performance of your antivirus protection in virtualized environments. These advanced diagnostics give you visibility into scanning bottlenecks ("antivirus storms") in the SVA so that you can make more precise adjustments for large, dynamic environments. In addition, you can review statistics on the most frequently scanned files and processes per SVA and then set up exclusion policies that may, for example, schedule scanning of non-critical files or archived files after hours, instead of on-access. This will free up computing resources for more important tasks.

You can also improve overall performance by setting specific policies. For example, scanning certain files that are not prone to infection, such as log files or text files, offers minimal value and can consume a great deal of overhead in the McAfee MOVE AntiVirus infrastructure. You can lighten the load by specifying only the critical file types that need to be scanned on access. In addition, you can save even more overhead by deciding not to scan files that don't change much, such as 75% of Windows operating system files. Another way in which McAfee MOVE AntiVirus speeds up performance is by using system RAM for files that are waiting to be scanned.

Monitor the virtual data center infrastructure with McAfee Boot Attestation Service.
For an added layer of security, McAfee Boot Attestation Service is included in the McAfee Server Security suites. McAfee Boot Attestation Service works with Intel Trusted Execution Technology (Intel TXT), a feature of the Intel Xeon processor, to determine the trust worthiness of the hypervisor boot by displaying the trust status in McAfee ePO software. If the host matches the "gold image," according to certain values assigned by Intel TXT, then it is assigned a trusted status. With this technology, you can:

- Determine whether a hypervisor boot is trusted by validating the firmware/BIOS and the hypervisor or virtual machine manager image that booted. McAfee Boot Attestation Service provides you with these trust designations: unsupported (the hardware does not support TXT), trusted (the hypervisor matches the expected TXT values), or untrusted (the hypervisor does not match the expected values assigned by TXT).
- Monitor the boot trust status in the McAfee ePO console.
- Develop security policies based on this status. For example, administrators can receive alerts if a critical VM is running on an untrusted hypervisor.

Enable whitelisting through application control.
As part of the McAfee Server Security Advanced suite, McAfee Application Control is one of the best means of defeating sophisticated zero-day threats and advanced persistent threats (APTs) that target data center servers. This critical layer of security provides three key components that support and build on one another:

- *Dynamic whitelisting*—This is a relatively simple but essential aspect of server protection. All you have to do is identify the authorized programs and updates that are used routinely at your organization. If an unknown executable tries to run, it's blocked because it's not on the whitelist. McAfee Application Control's unique dynamic whitelisting automatically updates the list of authorized applications when systems are patched and new versions of applications are installed. IT is relieved of the burden of manually updating the whitelist every time there's a change.
- *Memory protection*—Some threats, like buffer overflows, can circumvent whitelisting. Memory protection helps ensure that application vulnerabilities cannot be exploited in this manner.
- *File reputation*—It is entirely possible that malware can accidentally end up on your whitelist. File reputation checks the whitelist on every server, accessing McAfee Global Threat Intelligence service, which discovers emerging threats in real time. This global threat intelligence enables you to quickly determine whether the applications on your whitelist are legitimate or should be blocked.

McAfee Application Control helps increase the overall efficiency of your data center server security and positively impacts your bottom line. It adds another level of powerful protection against today's complex and insidious threats without the need for signature updates. It also reduces the need for costly security patches and manual whitelisting updates and increases time-to-protection.

Add more layers of protection.
To maintain data center server uptime and business continuity, McAfee Host Intrusion Prevention for servers is included as part of the McAfee Server Security suites feature set. Using a combination of signature and behavioral intrusion prevention system (IPS) technologies, it guards your servers against malicious traffic that may otherwise introduce known or advanced zero-day threats. It both boosts your server security and reduces your operational costs by minimizing the need for urgent security patching.

Unauthorized changes on your data center servers can have serious consequences—from data breaches to outages to compliance violations. The McAfee Server Security Suite Advanced includes McAfee Change Control, which provides uninterrupted monitoring and detection of critical system, configuration, and file changes across distributed and remote locations. It prevents tampering by blocking unauthorized changes. IT can track and validate attempted changes on the server in real time to ensure that they follow policy. For example, you can specify that authorized changes can be made only within certain time windows, by trusted sources, or through approved work tickets.

McAfee ePolicy Orchestrator software is at the helm.
The McAfee ePO management console makes it easy to manage security across all your data center servers and workloads—physical and virtual. Its customizable data center dashboard provides IT with accurate and complete information needed to maintain uptime, including metrics from data center security solutions, historical security data, power status, trust categorization of applications, risk scores for assets, and trend views. On the dashboard, administrators can instantaneously see all the registered data centers and risk information for each system, such as important data like anti-malware status, which will enable them to take corrective action, if required.

For virtualized environments, IT can drill down and find out which VMs are unmanaged. For example, some VMs may be unmanaged because they are running an unsupported operating system or because vShield is not installed or is disabled.

Additionally, through data center connectors, McAfee ePO software provides complete visibility to all virtual machines, even if they are off premises and do not yet have McAfee protections. Supported environments include VMware vSphere, AWS, OpenStack, and Microsoft Azure. By gaining visibility into all virtual machines—through monitoring security and power status—IT can more easily secure them.

Figure 2. McAfee ePO software data center dashboard.

> *"McAfee's ePO gets an A on its scorecard for bringing the various security components together in a common management framework. With [McAfee] ePO, it was easy to spot the highest risks in the data center test environment and to determine the patch status for any given system, what security components were installed, and where the risks for the system came from. The system tree view made it simple to navigate the test environment."*[8]
>
> —SANS Institute, *Securing Data Center Servers: A Review of McAfee Data Center Security Suite Products*

Expand

Today's dynamic and highly demanding business environment is driving enterprise departments to low-cost, easy-to-use public cloud services—and it's driving IT to enhance levels of service by building private clouds for provisioning of computing resources. But along with the flexibility and agility this type of multifaceted infrastructure offers, security complexity has increased. Regardless of whether workloads are running inside the firewall or in the public cloud, they all need to be defended so that vital corporate data doesn't fall into the wrong hands.

McAfee Server Security suites provide data centers with "elastic security"—security with policies that can extend into the public cloud as well as the private cloud. Elastic security means that IT has visibility into all workloads, is automatically able to protect them with security policies, and can monitor them on an ongoing basis. As mentioned previously, the data center connectors for McAfee ePO software make it easy to gain visibility into workloads that live in both private and public clouds.

The McAfee Data Center Connector for VMware vSphere connector is available for private clouds and provides visibility into private cloud environments. Administrators can determine the relationship between VMs and the VMware ESXi virtualization server (hypervisor) and find out on which host a given VM is running. This enables monitoring of VMs and the ability to apply granular policies, resulting in a stronger and more consistent security posture across VMs in the private cloud.

The McAfee Data Center Connectors for Amazon AWS, OpenStack, and Microsoft Azure give you a view into your public clouds. The process is as simple as entering your account information for your cloud service provider. You can then start managing and monitoring policies from the McAfee ePO console, which displays security status and incidents and allows you to deploy the necessary protection. The data center connectors enable you to automatically tag workloads based on where they were imported from and dynamically discover new VM instances and discard old ones that are no longer in use.

Summary

There's no doubt that data centers are undergoing a major evolution. With that in mind, a more all-encompassing, integrated approach to security is essential for protecting your prized corporate assets. McAfee Server Security suites help you keep pace with the unique security requirements of hybrid deployments that span physical servers, virtual environments, and cloud technologies—on premises and off premises. These comprehensive suites help you discover all workloads, *protect* them with powerful, layered anti-malware defenses, and *expand* into private and public clouds with automatic provisioning of security policies. With McAfee Server Security suites, you can more confidently embrace advanced data center technologies and better serve the business needs of your organization.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

1. **http://www.networkworld.com/article/2163059/cloud-computing/hybrid-clouds-pose-new-security-challenges.html**
2. **http://comtechpros.org/wp-content/uploads/2013/10/Latisys-Hybrid-WP-Aug2013-2.pdf**
3. **http://www.mcafee.com/us/resources/reports/rp-aberdeen-data-center.pdf**
4. **http://www.intel.com/content/dam/www/public/us/en/documents/reports/whats-holding-back-the-cloud-peer-research-report2.pdf**
5. **http://www.sans.org/reading-room/analysts-program**
6. **http://www.securityweek.com/mcafee-launches-new-data-center-security-offerings**
7. **http://www.verizonenterprise.com/DBIR/2014/?gclid=CJKR6cSIpb8CFUMIvAodpagAog**
8. **http://www.sans.org/reading-room/whitepapers/analyst/securing-data-center-servers-review-mcafee-data-center-security-suite-products-35200**

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