Citrix and Bitdefender Cloud Workload Protection

Performance, security, and management for the virtualized enterprise

Ready

Bitdefender

How can you combat a threat or attack if you don't know it's there?

This is the challenge faced by myriad organizations as they seek to protect their corporate assets and those of their clients from increasingly brazen and devastating theft and cybercrime. Sophisticated data breaches are increasingly common, targeting organizations around the globe with stealth malware that can lie undetected for months—offloading data, stealing money, or tracking employee actions. Traditional scanning solutions are insufficient for modern virtual digital workspace environments, and can compromise security, performance, and user experience.

High performance security for virtual workspaces

Detecting and preventing breach attempts in virtual digital workspace and hybrid cloud environments can be difficult with outdated antivirus and anti-malware scanning tools. With a focus on virtual workspace user experience and management, Citrix and Bitdefender are ideally positioned to offer performance-centric security and protection across hybrid cloud infrastructure.

Citrix Workspace: the preferred way to work

Digital transformation requires that organizations provide a productive user experience along with stronger security policies for data loss prevention. Citrix Workspace offers a user-centric focus where everything needed for work is found in one unified app, with conditional access and performance made simple based on user context and IT-designed policies. Citrix Workspace fully aggregates all apps and data across all applications—both on-premises and in the cloud—to deliver the right experience to the right user at the right time.

Citrix Workspace encompasses apps, content, devices, and analytics within a secure digital perimeter, enabling organizations to:

- Modernize IT security
- Enforce security controls for Software as a Service (SaaS) and Internet access
- Maintain productivity in an increasingly mobile workstyle
- Increase efficiency and lower costs with a cloud strategy

GravityZone Security for Virtualized Environments (SVE)

Performance is key for virtual app and desktop infrastructure, both in terms of the resources consumed by virtual machines (VMs), as well as the quality of the experience delivered to the end user. Traditional virus and malware scanning approaches require an agent installed on each VM. These agents require constant updates and monitoring, and can consume significant local resources. VM sizing exercises must take this additional resource consumption into account, reducing the number of VMs that can be supported by a given hardware platform.

Citrix Workspace

Only Citrix offers the most complete and integrated workspace to enable people to securely access their apps, desktops, and data from anywhere. Rely on Windows app and desktop delivery from Citrix Virtual Apps and Desktops, device security from Citrix Endpoint Management, secure file sync and sharing with Citrix Content Collaboration, and network security with Citrix Gateway. Only Citrix Workspace offers you complete choice of device, cloud and network, streamlined for IT control and simple, secure access for users.

In contrast, Bitdefender GravityZone Security for Virtualized Environments (SVE) provides the option of delivering anti-malware protection using security virtual appliances (SVAs). These virtual appliances function as centralized points of intelligence, without a traditional security agent installed on each VM. The SVA offloads most scanning functionality, covering file system, memory, process, and registry scanning on both Windows and Linux.

GravityZone SVE uses a multi-layered caching mechanism that contributes to leading performance. A local cache is maintained within each VM, so objects are scanned only once. A shared cache is maintained on each SVA so that objects scanned on one VM are not scanned on another. Finally, a series of file block-level caches deduplicate scanning down to the level of file chunks, so that files with few differing blocks of interest to the anti-malware engines are not completely rescanned.

These Bitdefender-exclusive technologies result in industry-leading performance. Bitdefender's efficient architecture and patented security algorithms also help minimize impact on infrastructure resources. Testing using industry-standard Login VSI tools showed the highest infrastructure optimization when compared to competitors, freeing resources to increase VM density and lower infrastructure costs. Since GravityZone takes fewer system resources away from production processes, it introduces only minimal latency to boot times and application response—improving the user experience. In Bitdefender testing, applications that ran on infrastructure protected by GravityZone ran 17% faster than competitors.

The Citrix Ready Program

The Citrix Ready technology partner program offers robust testing, verification, and joint marketing for Digital Workspace, Networking, and Analytics solutions—with over 30,000 partner verifications listed in the Citrix Ready Marketplace.

Integrating security with virtual and cloud infrastructure

GravityZone offers ubiquitous single-console management covering all workloads with a single point of visibility and management across hybrid and multi-cloud inventories (Figure 1). The SVA is delivered as a Linux (Ubuntu) self-configuring hardened virtual appliance. Failover capabilities and load distribution with multiple SVAs helps ensure optimum performance and protection at all times. Bitdefender supports any hypervisor, is integrated with Amazon Web Services (AWS) and Microsoft Azure, and supports all cloud environments.

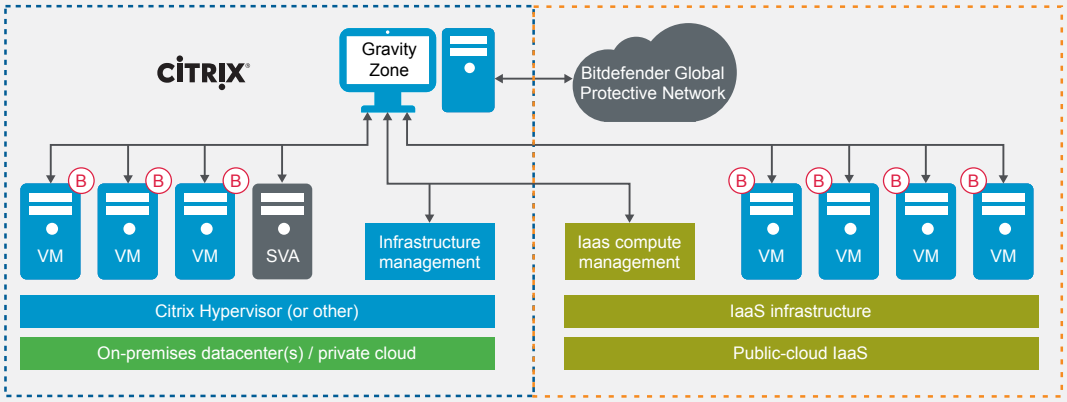

Figure 1. GravityZone SVE integrates with Citrix and the public cloud.

By integrating with virtual infrastructure management solutions like Citrix Virtual Apps and Desktops and Citrix Studio, Bitdefender provides dramatic management simplification. This integration provides extensive security management automation, reducing the management burden across these highly dynamic, high-flux environments. This level of integration allows:

- Up-to-date VM inventory, hierarchy, and tags
- Automatic discovery of VM instantiation, termination, and movement
- Remote platform deployment and configuration
- Automatic SVA deployment
- Automatic policy assignment based on VM tags
- Rapid security deployment and efficient, automated operations
- Centralized security management for multiple Infrastructure as a Service (IaaS) accounts
- Automatic security-license recovery for non-persistent VDI applications
- Infrastructure-specific reporting

With its ability to rapidly provision and decommission virtual workspaces, Citrix Apps and Desktops is ideal for non-persistent virtual deployments—such as call centers with multiple shifts. These same environments often provide challenges for traditional anti-malware scanning solutions. GravityZone and Citrix can dramatically improve security management in non-persistent virtual deployments.

- **Secured and manageable clones**. Duplicate Globally Unique Identifiers (GUIDs) often result from golden-image cloning. As a result, traditional threat detection solutions are often unaware of environmental or organizational details. With GravityZone and Citrix, clones are created already secured and manageable, with unique security IDs, precise locations, and automatic activation.

- **Automatic security license recovery**. Security license management can be a significant issue in non-persistent virtual environments. With manual management, VM decommissioning can cause active but inaccessible licenses, resulting in increased costs, reduced productivity, and exposure for virtual apps and desktops. In contrast, GravityZone is integrated with Citrix Apps and Desktops to coordinate available licenses with VMs. License are tracked accurately and VMs boot fully protected, lowering risk and cost for the organization.
- **Infrastructure-aware policy assignment**. Without coordination, traditional anti-malware solutions are unaware of underlying infrastructure, and the policies that govern it. GravityZone integration enables true inventory-based policy. Citrix infrastructure management hierarchies are visible to GravityZone, allowing security policies to be managed in a coordinated fashion with the rest of the virtual infrastructure.

Seeing the invisible: Bitdefender Hypervisor Introspection and Citrix Hypervisor

With a goal of exfiltrating information, capturing credentials, or performing cyber espionage, malware now commonly targets virtual machines in addition to bare-metal systems. These attacks can wreak considerable havoc, even while they remain undetected. Because malicious code is able to run with kernel privilege within the operating system—just like security solutions—it has a good chance of bypassing security once it is introduced. After a surreptitious infiltration, both the workloads and the system generally remain operable, making malware difficult to detect. Worse, some malware is designed to cover its tracks to avoid detection, or obliterate any sign that it was even there. File-less attacks can confine malicious activity to memory, with no malware written to storage at all.

So how do you catch what you cannot see? The answer lies in within the bare-metal hypervisor—a tool that has rarely been used for in-guest (or in-VM) security. Bitdefender Hypervisor Introspection (HVI) is a security layer that fortifies Citrix Virtual App and Desktop infrastructure against targeted attacks through live memory introspection at the hypervisor level. This unprecedented collaboration between Bitdefender and Citrix creates a new security layer with broad visibility, unaffected by malware.

Citrix Hypervisor includes Direct Inspect APIs, and is the only commercial hypervisor capable of delivering virtual machine memory introspection. These APIs offer insight into the raw memory stack of every virtual machine running in Citrix Hypervisor. They can be used to reveal and eliminate blind spots while also protecting existing security layers against sophisticated kernel-based malicious activity, including zero-day attack techniques. The approach uses no software in the VMs themselves, and benefits from the rich context that only hypervisor-level access provides.

Through Citrix Hypervisor, Bitdefender HVI has direct access to low-level information about the memory being used by each VM (Figure 2). Unlike tools that merely match patterns for existing exploits, HVI works by correlating raw memory changes with common attack techniques such as buffer overflows, heap spray, code injection, function detouring, and API hooking. Bitdefender HVI

stops attackers from gaining a foothold, and can even inject remediation tools on demand, notifying the control center of suspicious activity. In conjunction with Citrix Hypervisor, Bitdefender HVI has been able to detect multiple zero-day attacks with no prior knowledge (including Eternalblue, APT28, Energetic Bear, Epic Turla, Zeus, Darkhotel, and Dyreza).

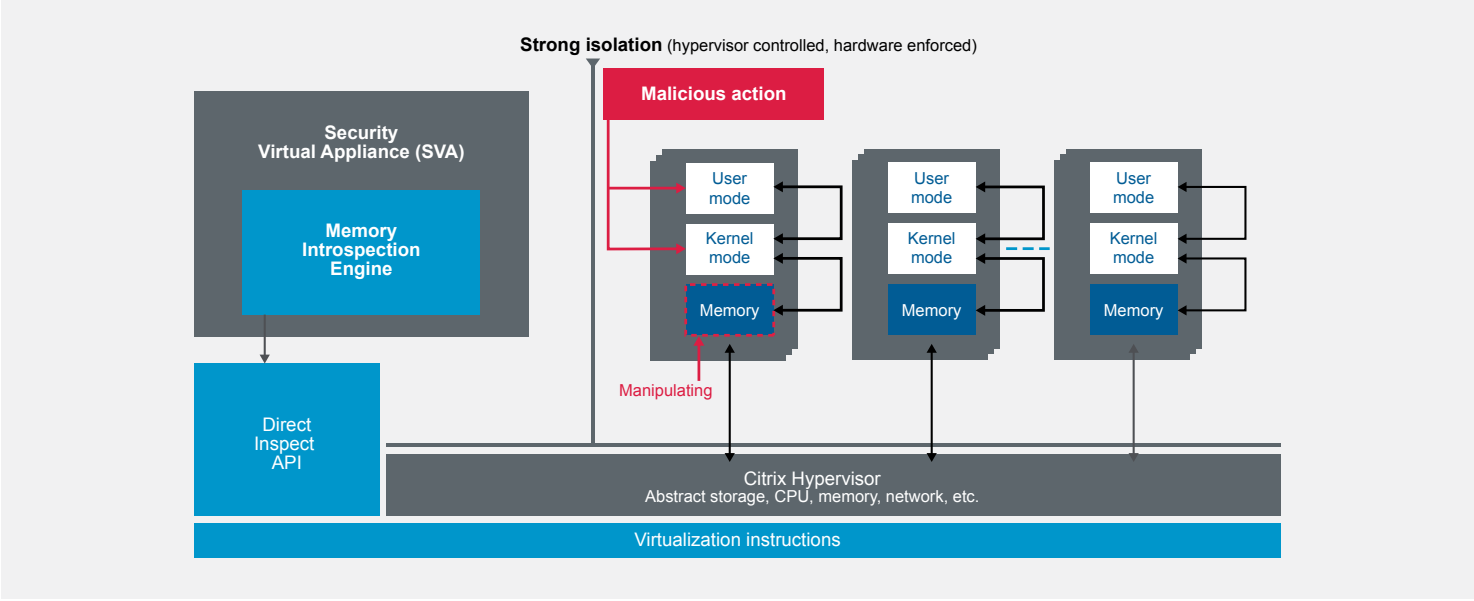

Figure 2. Citrix Hypervisor and Bitdefender Hypervisor Introspection

Conclusion

The move to hybrid cloud environments demands a new approach to security that fundamentally understands virtual environments. Together, Citrix and Bitdefender provide a compelling technology combination that integrates the entire arsenal of award-winning Bitdefender threat protection tools with Citrix Workspace. This unique technology combination provides consistent security for hybrid cloud environments. Bitdefender SVE offers leading performance, improved utilization, and a better user experience in terms of latency and response. Citrix Hypervisor and Bitdefender Hypervisor Introspection provide a new level of security that can literally detect security threats as they occur.

For more information, visit the Bitdefender page on the Citrix Ready Marketplace at citrixready.citrix.com/bitdefender.html.

About Bitdefender

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers, and Cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on. Learn more at bitdefender.com.

About Citrix Ready

The Citrix Ready technology partner program offers testing and verification for joint Digital Workspace, Networking, and Analytics solutions. After a robust testing process, validated partner solutions are listed in the Citrix Ready Marketplace, giving customers and channel partners a simple and effective way to explore and select Citrix Ready verified solutions—increasing confidence while reducing risk. Learn more at citrixready.citrix.com.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States