Whitepaper

Bitdefender®

# HYPERVISOR INTROSPECTION – A REVOLUTIONARY APPROACH TO TARGETED ATTACKS

# Contents

# Executive Overview

Recent headlines about data breaches are clear – securing infrastructures against increasingly targeted attacks is imperative, yet traditional endpoint security tools are not closing the gap with attack technologies, let alone getting ahead of them.

A study conducted in February 2016 shows it takes companies an average of 5 months to detect a data breach. What's more, 53% of them needed external investigators to discover them, as internal resources showed no signs of a breach.[1]

A lot that goes on in datacenters is invisible, but it doesn't have to be.

Virtualization added a hypervisor layer below operating systems which to date, has not been leveraged to secure those guest operating systems and their workloads.

Working with Citrix, Bitdefender has created a method of revealing malicious activity in the guest operating systems from the level of the underlying hypervisor. Called Hypervisor Introspection (HVI), the solution leverages Citrix Direct Inspect, an API in the XenServer hypervisor.

- A method deemed impossible to achieve until now. Direct Inspect API released by Citrix as part of XenServer 7 is the first commercial hypervisor capable of virtual machine introspection. Bitdefender HVI is the first solution that can offer real-time scanning of raw, 4k memory pages - providing unparalleled visibility into advanced targeted threats.

- Real-Time Attack Detection. With this hypervisor-level view, HVI can uncover a threat during the earliest stages of an attack. HVI inspects the memory for malicious activity signs that an attacker is attempting to compromise a system.These attack techniques include buffer overflows, heap spray, code injection, function detouring, and so on.

- Truly agentless. Having no footprint in the virtual machines means that HVI is isolated; an attacker cannot attempt to disable or compromise the security tool. However, unlike network security tools, HVI has complete contextual information just as in-guest security would.

- Minimum Performance Impact. Bitdefender Hypervisor Introspection runs memory introspection with minimal performance impact. Thanks to lengthy development, the solution monitors your VMs raw memory activity without impacting the user's activity on the machine.

- Run On Top of Your Existing Security Solution. Unlike other solutions that require you to remove and replace existing endpoint protection, HVI complements your existing security tools. It will stop the attack from hiding its tracks, allowing your security solution to detect and remove the remaining payload traces.

- Already proven against APTs. HVI has already been tested against some of the best known APTs of recent years, including Carbanak, Turla, APT28, NetTraveler and Wild Neutron.

1 https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

# Introduction

Endpoint security is struggling. Until now, the very concept of endpoint security was constrained to security running within endpoints – the Windows and Linux server and desktop operating systems upon which every modern organization depends – or as network devices.

Attackers have been taking advantage. Sophisticated attackers use tools and techniques to make detection of their malicious activities difficult with traditional security tools. Kernel-level rootkits, zero-day attacks, novel, purpose-built command and control systems, etc. are commonplace.

These attacks are very different from mass-attacks of the past. Those attacks were designed to infect as many systems as possible, and tended to make their presence known by rebooting systems, generating extreme levels of network traffic, and so-on. Newer, profit-driven attacks are built to be stealthy and defeat traditional security tools. The goal is straightforward; infiltrate your most sensitive systems and exfiltrate your most sensitive, and therefore valuable, data, all without you knowing it.

Revealing what you don't know means going deeper, while delivering actionable insight. While attacks have rapidly evolved, in the meanwhile, the framework of enterprise IT infrastructure has transformed completely. The hypervisor now sits as an intermediary between virtualized endpoints and physical hardware. Endpoint security has not, until now, experienced the same paradigm shift. Traditional network-level security may run as a virtual appliance, but still essentially performs inspection of network traffic just as it did before. Traditional security agents running in protected systems may offload scanning to a virtual appliance for performance, but are still constrained by technical limitations of running within the endpoint operating system.

This solution brief describes the root of the problems experienced by traditional endpoint security, how attackers exploit them, and a new approach called Hypervisor-based Introspection that takes advantage of the hypervisor to reveal malicious activity hiding below the surface of your datacenter.

# The security problem

## The root of the problem

*Know what you don't know*

As organizations architect and build datacenters with ever-further abstracted infrastructure, on-demand computing becomes closer to realization. Yet security has managed to, at best, tread water during the virtualization revolution.

Bitdefender and Citrix have created a technology that gives datacenter owners a view below the surface; the ability to know what has been impossible to see, until now. This is much more than a new iteration of existing security – it is a revolution.

## Contributing factors

*Disruption from virtualization*

Virtualization has facilitated tremendous change in datacenter planning, architecture, and management. Both internal and external IT service providers are embracing an on-demand, everything-as-a-service, software-defined, paradigm. Endpoint security continues to evolve in iterations, including addressing performance issues by offloading protection tasks to virtual appliances. The problem is the underlying model of endpoint security has not experienced, let alone embraced, the same level of disruption as endpoint computing has. This has led to traditional endpoint security models slowly evolving while datacenter architecture and operations have been revolutionized by virtualization.

Fundamental constraints of traditional endpoint security, many of which are described in the technical challenges below, can be addressed by embracing the computing stack that virtualization provides. Rather than relying solely on in-guest agent software, running at the same level of privilege as attackers, the XenServer hypervisor now provides a mechanism for securing virtual machines, and the workloads they host, from the hypervisor level.

## Attack techniques

When attacks are analyzed in-depth, the conclusion is that many use similar techniques at some point in their life-cycle. Often, these techniques involve manipulating memory; buffer overflows, heap spray, code injection, and so-on.

Many security solutions look for specific exploits or activity associated with specific vulnerabilities. Sophisticated attackers know this well, and avoid using well-known, easily detected implementations. It is widely known that highly organized, profit-driven attackers seek unknown vulnerabilities (zero-day vulnerabilities), or use one-off, purpose-built exploits (zero-day exploits) and other tools. Attackers also use advanced techniques to delay and sequence attack payloads to mask malicious activity. They even incorporate security solutions as part of their "Quality Assurance" process.

A solution to this aspect of the problem must not rely on searching for known attacks and previously encountered malicious activity, or employ vulnerability-facing techniques. These approaches, while valid, are either too narrow in scope, or too aggressive. Even when a middle-ground is found, either false negatives (not catching attacks that fall outside a narrow scope) or false positives (flagging the benign as malicious) are, by definition, sacrificed in favor of the other.

### Targeted attacks, stealth, zero-day

Also known as Advanced Persistent Threats (APTs) and Advanced Targeted Attacks (ATAs), these attacks are of tremendous concern to organizations. Recent examples have focused on retail since they lead to wide media coverage and direct financial losses. They are also interesting because many of the highest profile attacks were not detected by the retailer, but by the credit card companies tracking fraud activity.

Other attacks that are well-known in security circles but don't get as much media attention include nation-state sponsored attacks. Some are generally accepted (Stuxnet), while others are widely suspected (Chinese attacks against defense contractors, Nortel, and other industrial targets). On that note, industrial espionage is another area of great concern.

While retail organizations must often disclose successful attacks, industrial and state-sponsored espionage rarely garners wide attention because it is all-but never acknowledged. Yet, the lessons of many of these attacks are clear – a sophisticated attacker can enjoy days, weeks, months, or even years of persistence in a targeted environment.

More mundane attacks can also succeed for a variety of reasons, including unpatched systems, improperly configured or applied security, and so-on.

In all of these case, the greatest fear of organizations is what they don't know.

## Technical Challenges

### Context versus isolation

Traditional security tools suffer from a context versus isolation dilemma. Tools residing on the network (NIDS/NIPS/WAF) are isolated from the protected workloads running on endpoints. If an endpoint is compromised, the isolated security tool is not affected. However these tools lack context; that is, they lack awareness of the state of endpoints, especially memory.

Conversely, traditional endpoint security tools running within an endpoint enjoy rich knowledge of context, but lack isolation. If an endpoint has been compromised by malicious code running with kernel privilege, the security tools also running at the same level cannot be trusted to guarantee detection.

This dilemma created a scenario of trade-offs previously deemed impossible to resolve. It was thought that either context or isolation had to be sacrificed to achieve the other. Virtualization provides a way to resolve this dilemma. Hypervisors can provide rich context while they are isolated from the virtual machines they host and the workloads within.

### Level of privilege

Traditional, agent-based security relies on software running within the protected endpoint. As the tools used by attackers have advanced from user-mode (ring-three) to kernel mode (ring-zero), security followed. The problem is that within a protected endpoint, there is no level of permission higher than ring-zero.

As a consequence, agent-based security tools cannot guarantee detection of malicious activity. For example, advanced, targeted attacks may use sophisticated rootkits to defeat detection.

Virtualization introduced a layer of privilege that is higher than what is available within protected endpoints. The hypervisor runs below one or more guest operating system instances, essentially as ring-minus-one.

# The solution

Working together, Bitdefender and Citrix have solved the technical challenges of creating a solution to the root problem, thereby giving datacenter owners the ability to know what they don't know, and act on information from this new level of insight.

Citrix XenServer now includes Direct Inspect, which is an API that facilitates virtual machine introspection from a security virtual appliance. Bitdefender has built Hypervisor Introspection (HVI) to take advantage of the virtual machine introspection feature included in Citrix XenServer.

Citrix XenServer is the first commercial hypervisor with virtual machine introspection capability. Bitdefender HVI is the first commercial solution to deliver on this radical new approach to endpoint security.

Leveraging insight provided from the hypervisor embraces, indeed takes advantage of, datacenter architectures that virtualization has brought. This deeper level of insight goes below the virtualized endpoints and the workloads they host.

## Solving the technical challenges

Hypervisor Introspection (HVI), by its very nature, operates at a level of privilege that is higher than that available in-guest. While a rootkit running in a virtual machine may run with kernel-level (ring-0) privilege, as it does in-guest security software, HVI performs at the hypervisor level of privilege.

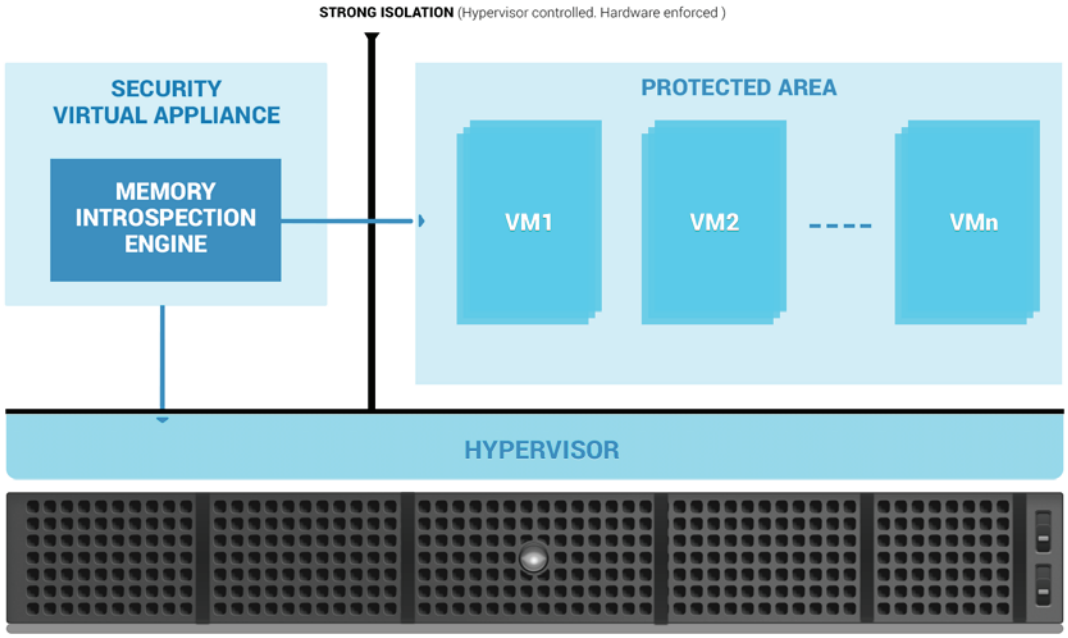


**Figure 2 Overview of HVI architecture**

As shown in Figure 2, HVI leverages an API in the underlying hypervisor. The Introspection Engine applies security rules to virtual machine memory while remaining isolated from the protected virtual machines.

Whether the protected endpoint is Windows or Linux, server or desktop, HVI provides insight at a level that is impossible to achieve within guests. Effectively, it is inspection from below the guest operating systems; ring-minus-one insight and control.

Just as the hypervisor controls hardware access on behalf of each guest virtual machine, HVI has intimate knowledge of both user-mode and kernel-mode in-guest memory. The result is HVI has complete insight into guest memory, and therefore full context. At the same time, HVI is isolated from the protected guests, just as the hypervisor itself is isolated.

Overcoming the root problem

With hypervisor-level access to in-guest memory, and isolation from in-guest exposure to compromise, Bitdefender Hypervisor-based Introspection delivers a new level of insight into what was previously deemed impossible to know.

While a targeted, highly sophisticated attack may use customized, one-off tools and exploit zero-day vulnerabilities to get a foothold and defeat in-guest endpoint security, HVI will expose these attacks by leveraging changes in the software stack that virtualization has introduced.

HVI identifies attack techniques rather than attack patterns. In this way, the technology can identify, report and prevent common exploitation techniques. The kernel is protected against rootkit hooking techniques that are used during the attack kill chain to provide stealth. User-mode processes are also protected against code injection, function detouring, and code execution from stack or heap.

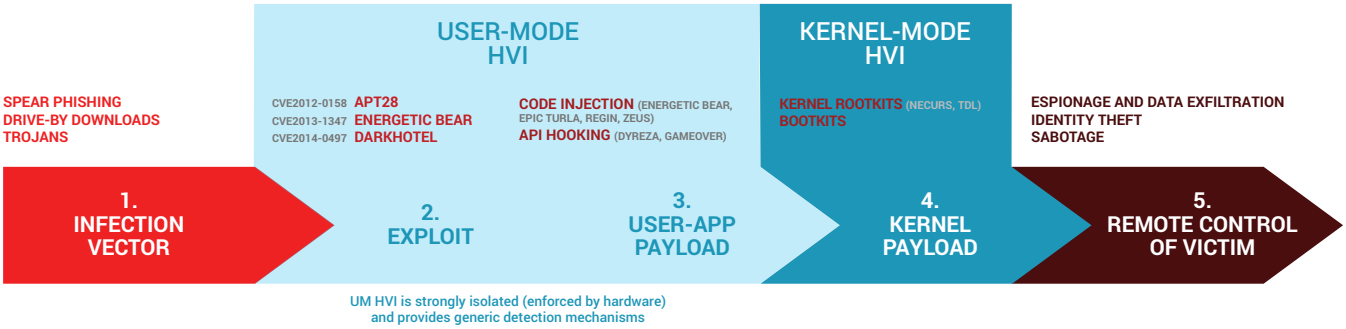


**Figure 3 HVI protection applied to an example of attack action flow**

Figure 3 shows where in an example attack action flow HVI protection applies. A remote attacker may attempt to exploit a vulnerability remotely or send a specially crafted malicious email to create an infection vector. When the exploit attempts to execute, if it relies on a common technique such as a buffer overflow, HVI will detect it. After a successful exploit, an attacker may then push a user application payload to escalate system privilege. Again, if a common technique such as code injection or API hooking is used, HVI will detect it. Moving ahead, if an attacker attempts to deploy a kernel-mode rootkit or bootkit to hide from kernel-mode inspection, HVI will detect it since it runs below the operating system. All of these detection points come before an attacker can achieve the ultimate goal, which is remote command and control of a compromised system.

While an in-guest security mechanism may detect an exploit attempt or malicious payload, the approach is limited since the security and malicious activity take place at the same level of privilege. For example, if a sophisticated rootkit is already in-places, it will hide the presence of malicious payloads. Since HVII runs at a higher level of privilege, it is impossible to use in-guest malicious techniques to avoid detection.

# Conclusion

The Citrix Direct Inspect API introduces a new method of security virtualized endpoints and the workloads they host. Bitdefender Hypervisor Introspection (HVI) is the first, and presently only, security solution to leverage this revolutionary approach.

Virtualization has revolutionized datacenters, while attackers have rapidly evolved their techniques to take advantage of the shortcomings of traditional endpoint security. By taking advantage of the privilege level and hardware-enforced isolation of hypervisor, HVI provides levels of insight that were not possible before.

By operating at a different level, HVI overcomes technical challenges of traditional security to reveal malicious activity in your datacenter. Keeping this very activity hidden is what attackers rely on to keep sophisticated attacks stealthy.

The approach used by HVI is not simply an evolution in endpoint security, it truly is a revolution.

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.


FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-May.31.2016-TK#: 91248