HVI

WHAT SECRETS DOES YOUR INFRASTRUCTURE HOLD?

In late 2013, a standard investigation on a bank in Kiev revealed that for several months the internal systems were being monitored by stealth malware. The malicious software was highly successful at covering its tracks, recording every employee's move, and even sending back video feeds and images, all without raising suspicion.[1]

When finally discovered, the sophisticated attack - known today as Carbanak - was eventually linked to more than one-hundred banks across thirty nations, revealing one of the largest bank thefts ever. This attack inflicted an estimated $1 billion worth of damage globally.[2]

Carbanak is just one of a series of targeted attacks that breached data in key industries around the world, by using stealth malware to gain entrance while avoiding detection. While there are many other similar examples of attacks, no proactive technology has yet been proven effective enough to single out these deep threats.

How Malware Out-Privileges You, Without You Knowing It

Operating systems were not designed with security in-mind. Malicious code is able to run with kernel privilege, just like your security solution, and stands a good chance of bypassing your security.

After it surreptitiously infiltrates the system, both the workloads and the system remain operable. While everything may seem fine, it is only a front for data exfiltration and cyber-espionage.

Some Malware Can Even Bring an Infrastructure to Its Knees

The damage inflicted by successful attacks on a system increases with the time to mitigate. Even a relatively innocuous malware, such a spam-sending Trojan, will impact the resources of an organization. Ultimately, it can impact profit by consuming resources, which may even be partly directed at employees of the company itself, inflicting further wasted time on the company.

5 Months Pass Before an Infiltration Is Uncovered

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.[3]

1 http://www.nytimes.comt/2015/02/15/world/bank-hackers-steal-millions-via-malware.html
2 https://threatpost.com/carbanak-ring-steals-1-billion-from-banks/111054/
3 https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

Bitdefender and Citrix Join Forces to Root out Deep Threats from Your Infrastructure

How Do You Catch That Which You Cannot See?

If a rootkit or kernel exploit tricked the operating system into hiding its tracks, even advanced security solutions will have difficulties discovering them, if those security solutions are in-guest. The trick is viewing a VM from the outside, while also monitoring its inside processes.

The approach lies within the bare-metal hypervisor – a tool that hasn't been used for security before. They hypervisor provides the context of VMs, while staying isolated from them.

In an unprecedented collaboration against targeted attacks, Bitdefender and Citrix put their collective expertize in virtualization and security on the table. Together, they created a new security layer that will see everything happening in your infrastructure, but which malware cannot reach.

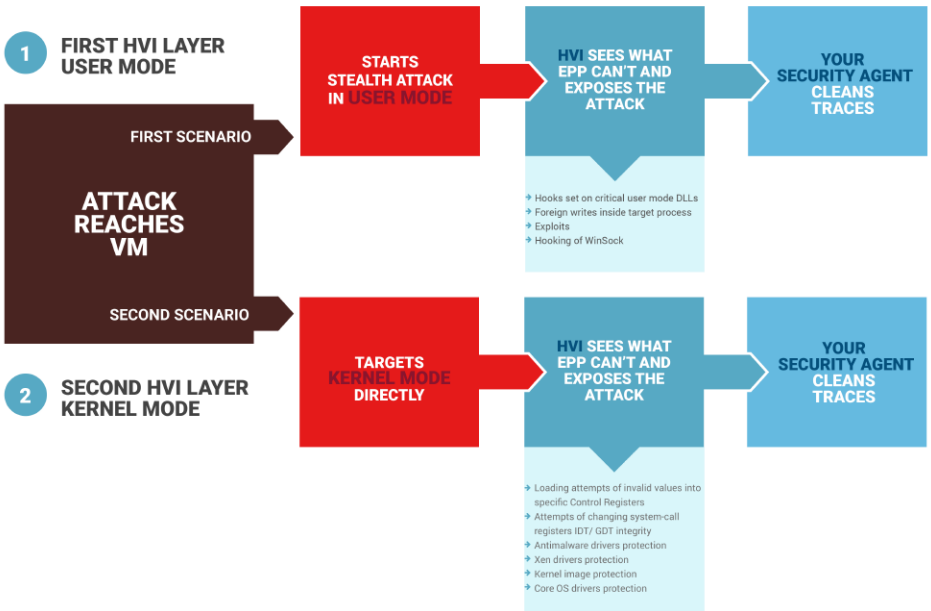
A Solution Deemed Impossible To Achieve

The way to catch the most advanced threats is to not rely on information given to you by the OS. Hypervisors provide clean, low-level information about the memory being used by each virtual machine.

To provide these insights, Citrix is now introducing a new, specially designed API in XenServer, which offers insight into the raw memory stack of every virtual machine from the hypervisor.

At this level, access to memory is so raw, and at such a low-level, that analyzing it has been impossible so far -- only a handful of people in the world write security at this level.

Bitdefender is now introducing Hypervisor Introspection(HVI), a ground-breaking solution that detects suspicious activities by working directly with raw memory – a level of insight from which malware cannot hide.



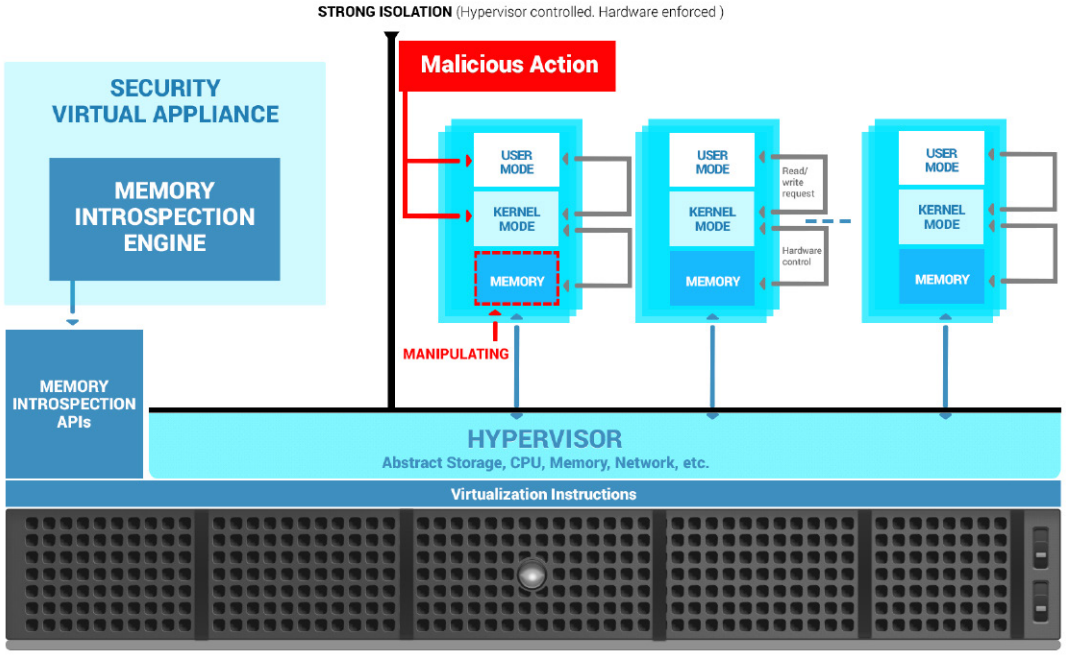
An Innovative Security Layer That Protects Your Privileges

Working together, Bitdefender and Citrix are now giving datacenter owners the ability to know the previously unknowable, and act on information from this new level of insight.

Bitdefender Hypervisor Introspection (HVI)

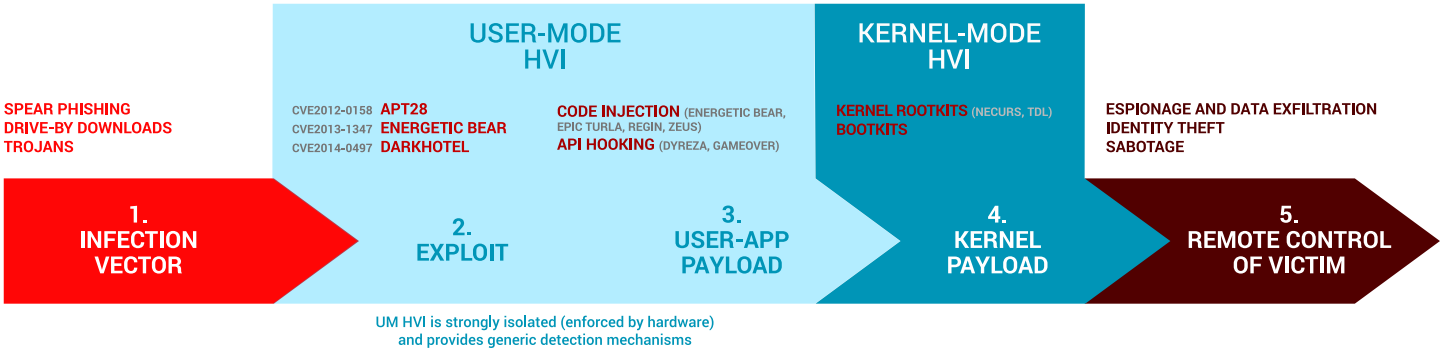
HVI is able to detect attacks that can be hidden in your infrastructure for days, weeks, or even months – spying and exfiltrating information invisibly. HVI does not assume your systems are clean upon arrival; you can instruct HVI to inject cleaning tools into live virtual machines – a temporary footprint into running systems. This also allows your native endpoint protection to take care of the rest, from within the VM.

HVI can also prevent further breaches, ensuring you have full visibility of the activity in your datacenter.



ALREADY PROVEN AGAINST TARGETED ATTACKS

HVI already detects and blocks famous targeted attacks including Carbanak, Turla, APT28, NetTraveler or Wild Neutron without knowing beforehand the actual vulnerabilities used by the hackers.



Among the targeted attacks that HVI can detect is a massive cyber-espionage campaign uncovered in 2015 by Bitdefender called APT28. The attackers infiltrated political, e-crime services, telecommunication services or aerospace industries in US and
Eastern Europe – stealing passwords, and gaining system privileges – all while remaining undetected.

Coincidentally, during this period, in Minsk, the political leaders of Belarus, Russia, Germany, France and Ukraine were participating in a summit, discussing the ceasefire in the Donbass region in the east of Ukraine.[4]

Minimum Investment. Easy To Deploy.

Unlike other vendors that require you to remove your endpoint protection and replace it with theirs, HVI is complementary to your existing security tools. It is a new security layer, and is fully compatible with every existing EPP today.

It also works hand in-hand with you current agent-based solution – it stops attackers from gaining privileges on your infrastructure, preventing them from hiding from your in-guest security.

Try it now

Learn more about Bitdefender Hypervisor Introspection and request a demo at www.bitdefender.com/hvi

SYSTEM REQUIREMENTS
Supported Guest Operating Systems
Windows desktop operating systems:
· Windows 8, 8.1
· Windows 7
Windows 10 (TH1, TH2, RS1, RS2, RS3, RS4, RS5, 19H1) and 19H2, 20H1 64-bit
Windows server operating systems:
· Windows Server 2012 R2
· Windows Server 2012
· Windows Server 2008 R2
Windows Server 2016
Windows Server 2019

Linux operating systems:
· Debian 8.2, 9, and 10, 64-bit
· Ubuntu 14.04 (kernel 3.13.139 onward) 16.04, 18.04, 20.04 (all LTS, 64-bit)
· Ubuntu 14.04, 16.04, 18.04, and 20.04, 64-bit
· CentOS 7, 8, and 8.2, 64-bit
· Red Hat Enterprise Linux 6.9/6.10, 7, 8, and 8.2 64-bit
OpenSUSE 12 (SP 1, SP 2, SP 3, SP 4), 15 (SP 1)
Oracle Linux below 7.5 (kernel 4.1) and at or above 7.5 (kernel 4.14)

Host Requirements
CPU microarchitecture:
· Any Intel® Sandy Bridge processor or later, with support for Intel® Virtualization Technology.
· VT-x or VT-d extensions must be enabled in BIOS.
Software requirement:
· Citrix XenServer 7.1 or later
Citrix Hypervisor 8.0 or later

[4] http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28–The_Political_Cyber-Espionage.pdf