Bitdefender

HYPERVISOR INTROSPECTION

Technical Preview Program for KVM Environments

STOP ADVANCED TARGETED ATTACKS AND PREVENT BREACHES

Of the 2,216 confirmed data breaches covered in the latest Verizon® Breach Investigations Report, 68% took "months or longer" to discover, 48% featured hacking, and 38% were perpetrated by organized crime or state-affiliated actors. Sophisticated and stealthy, advanced targeted attacks behind the breaches bypass conventional tools, such as traditional endpoint security, and cost companies sensitive data, intellectual property, and millions of dollars in damages, fines, and lost revenue.

Described by industry-analysis firm IDC® as "a transformative approach to advanced attack detection," Bitdefender Hypervisor Introspection (HVI) uniquely protects virtual environments against advanced threats—kernel-level exploits, rootkits, bootkits and environment-aware, multi-stage infections. As illustrated in Figure 1, HVI performs raw memory introspection at the hypervisor level, correlating memory changes with exploitation techniques. Consequently, HVI can uncover memory violations in real time and stop zero-day, sophisticated attacks that endpoint-security solutions may not even see. Whether on Windows or Linux, a virtual desktop or server, HVI protects the entire VM memory footprint (including both the kernel- and user space) without requiring in-guest presence or signatures. And, since HVI operates outside of the virtual machine (VM), it is physically isolated from in-guest threats and impossible to compromise.

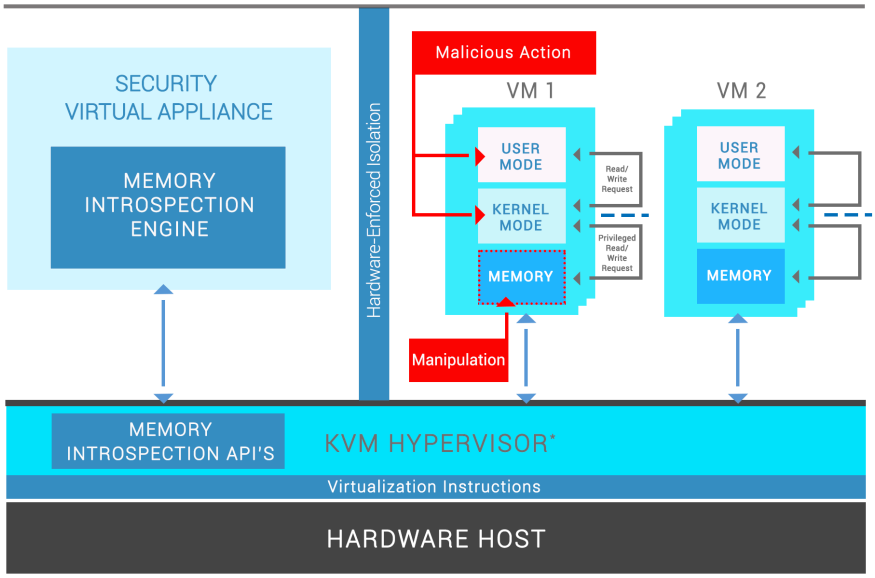

Figure 1: Hypervisor Introspection: Immune to attacks. Sees what others can't

* - KVM version with Bitdefender patches

"Bitdefender HVI offers an innovative approach that protects the memory and hypervisor outside of the VM and still monitors the VM itself. We never saw anything on the market that came even close. It's an additional layer of security that protects us from the most advanced attacks."

– *Simon Gassmann, Chief Information Officer and Managing Director, Quilvest*

PRESERVE CONSOLIDATION RATIOS AND OPERATIONAL EFFICIENCY

HVI is truly agentless, with zero footprint within the VM, hence no negative impact on performance and virtualization density. Plus, HVI complements any endpoint-protection platform, so you can use it to reinforce your existing security infrastructure. HVI deploys in minutes and delivers simple single-pane-of-glass manageability from a central GravityZone console. And with no endpoint-side software to maintain or update, your team can focus on strategic projects rather than managing security.

Hypervisor Introspection has proven effective against such cyberweapons as:

- EternalBlue (CVE-2017-143)
- 2018 RIG kit (CVE-2018-8174)
- Flash (CVE-2018-4878 & 2014-0497)
- Dirty Cow (CVE-2016-5195)
- Firefox JIT (CVE-2016-9079)
- IE8 Code Injection (CVE-2013-1347)
- ActiveX BO (CVE-2012-0158)

JOIN THE HVI FOR KVM TECHNICAL PREVIEW

Bitdefender has partnered with the KVM community to advance KVM's memory introspection capabilities and bring HVI to KVM environments. Organizations using KVM can now safeguard their intellectual property and sensitive data from advanced threats and more easily comply with NIST SP-800-125A, Rev. 1 "Security Recommendations for Server-Based Hypervisor Platforms" and other regulatory requirements.

Be among the first to try this revolutionary security technology on KVM. Test HVI and share your feedback directly with the Bitdefender product team. Join the HVI for KVM Technical Preview program today!

SC MEDIA INDUSTRY INNOVATOR

"Hypervisor Introspection is a qualitative improvement in the security of virtual environments."

– IDC, 2017

How the Technical Preview Program Works

As part of the Program, Bitdefender will provide you HVI beta software at no charge in exchange for your feedback on its strengths and areas of improvement. The Bitdefender team will be available to help you with deployment and administration. More information is available in the Technical Preview Program Guide.

How to Join

Please email enterprise-beta@bitdefender.com with **"HVI for KVM"** in the subject line to be considered for the program.

System Requirements for the Tech Preview

Minimum Hardware Requirements	• x86 server with one Intel® CPU, 32 GB RAM, 500 GB storage • Intel CPU microarchitecture (Sandy Bridge or newer) • Intel Virtualization Technology VT-x or VT-d extensions must be enabled in the BIOS
Virtualization Platform	• KVM hypervisor, customized and provided by Bitdefender

Supported Guest Operating Systems

Windows®

- Workstation OS: Windows 10 (TH1, TH2, RS1 – RS5, 19H1), 8.1, or 7 (no SP, SP1)
- Server OS: Windows Server 2019, 2016, 2012 R2, 2012, or 2008 R2
- 32-bit or 64-bit architectures are supported (as applicable)

Linux®

- Debian®: 10 (kernel v.4.19), 9 (kernel v.4.9), or 8 (kernel v.3.16)
- Ubuntu®: 18.04 LTS (kernel v.4.15), 16.04 LTS (kernel v.4.4), or 14.04 (kernel v.3.13.139 and newer, 4.4)
- CentOS 7 (kernel v.3.10)
- RedHat® Enterprise Linux®: 8 (kernel v.4.18) or 7 (kernel v.3.10)
- OpenSUSE Enterprise 12: SP4 (kernel v.4.12), SP3 (kernel v.4.4), SP2 (kernel v.4.4), or SP1 (kernel v.3.12)
- Oracle® Linux: before 7.5 (with kernel v.4.1 – UEK branch); newer than 7.5 (with kernel v.4.14 – UEK branch)

To learn more about Bitdefender Hypervisor Introspection, please visit: bitdefender.com/hvi.

Bitdefender®

www.bitdefender.com