White Paper

Hypervisor Introspection: A Transformative Approach to Advanced Attack Detection

Sponsored by: Bitdefender

Alexei Proskura Mark Child
May 2017

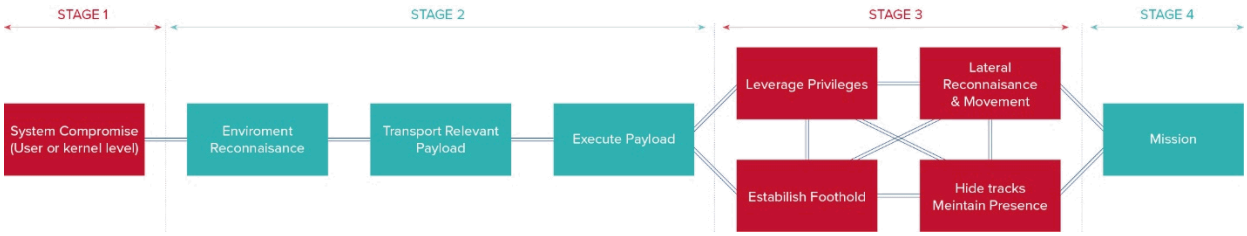
Executive Snapshot

Countering the continually evolving threats that organizations face today requires a qualitative improvement in cyber-defense technologies, particularly the protection of endpoints. The variety of technologies used on the endpoints in an average enterprise makes the task of protecting all devices an uphill struggle for IT and security departments. A significant challenge is conservative thinking: Defenses are typically deployed on the endpoint itself, meaning that the protective software *at best* runs on the system at the same privilege level as malicious software (malware).

An evolutionary shift has occurred with the emergence of new approaches to address the challenge of defending against advanced threats. These approaches are summarized by IDC in the specialized threat analysis and protection (STAP) market, which covers a broad range of non-signature based methods including sandboxing, behavioral analysis, file integrity monitoring, telemetric heuristics, containerization/isolation, network flow analysis, and threat intelligence. Hypervisor introspection, which will be examined in this IDC White Paper, incorporates multiple STAP techniques including advanced system behavior analysis, whitelisting, and monitoring for anomaly detection.

FIGURE 1

Typical Advanced Threat Exploitation Cycle



The four main stages of exploitation: 1. initial compromise 2. environment-specific payload delivery and execution 3. rooting, evasion, and lateral movement 4. main mission (e.g., information collection).

Source: IDC, 2017

SITUATION OVERVIEW

The deployment of new and emerging technologies may occur during technology refresh cycles. Innovative solutions may also be deployed to complement existing solutions in a way that, if they are combined, the overall benefit is greater than the sum of the parts. This multifaceted, integrated approach is widely advocated to improve security posture.

Protection against advanced malware is increasingly viewed as just one component of endpoint protection. The reason is clear: Today's threats include a broad spectrum of potentially sophisticated and damaging attacks, and anti-malware technology alone is not enough to protect endpoints. Again, it comes back to evolution: Many traditional endpoint security solutions were developed to combat what is now regarded as relatively unsophisticated malware that aimed for maximum damage with minimum investment. Modern attacks, however, may focus on very specific targets using intricate and subtle approaches that have been developed over extensive periods of time.

The term "endpoint" has multiple definitions. In this paper, endpoint will refer to any device connected to the network that either provides services or offers users the ability to access those services. Servers, user workstations, laptops, and mobile devices are all endpoints. But it would be imprudent to stop there. To assess the security of an information system of any complexity, it is important to understand the evolution of the system, especially when accelerated by disruptive technologies.

Virtualization Adoption: Increased Risk of Attack

According to IDC data, in 2016 virtualization reached the 50% adoption threshold worldwide, and continues to grow. Positive changes brought by virtualization include reduced capital and operational costs (e.g., by providing higher server density while requiring lower maintenance resources). Software-defined networks (SDNs) provide a similar level of abstraction for network devices that VMs provide for server hardware.

As the technology stack becomes more software oriented and driven, modern IT infrastructure relies more on configuration and orchestration rather than on physical connectivity between devices, whether endpoints or network devices. The increasing dependency on software creates more opportunities for malicious actors to exploit vulnerabilities and misconfigurations. The implication for security solutions that run on endpoints is a limited capability to detect sophisticated attacks.

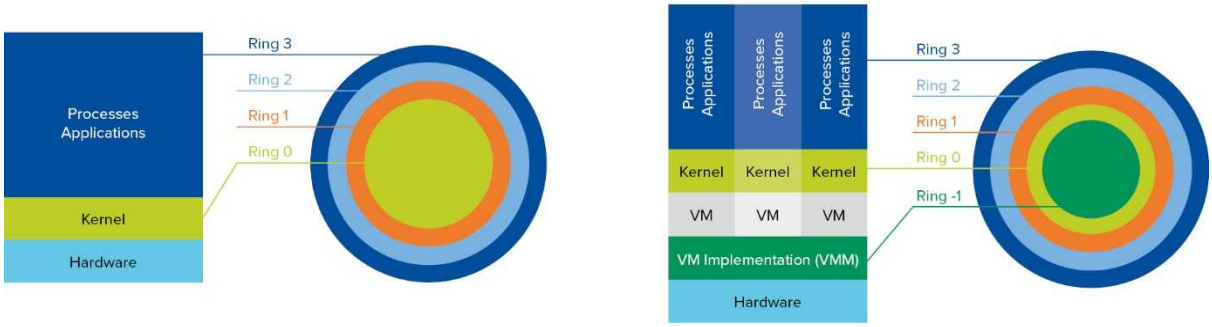
New Technologies: Reevaluating Defensive Strategies

An application itself undergoes very little change, if any, when moved from a physical to a virtual environment. However, the transition will significantly affect the security posture of the application. To explain the change, it is necessary to introduce a hierarchy of protection domains, or "rings," as they are often referred to.

Traditionally, OS and application processes are executed in their respective protection domains. Various OSs use protection domains differently, but when deployed on physical hardware, system, or kernel-level, processes are executed in the domain known as Ring 0. Applications are executed in Ring 3. Rings 1 and 2, while used in some OSs and by some software vendors, are used less commonly.

FIGURE 2

Privilege levels: Physical vs. Virtualized



Source: IDC, 2017

If an application is deployed in a virtual environment, the guest OS is executed above the hypervisor layer. Thus, from the guest OS point of view, the protection domain exists at a privilege level higher than Ring 0. This is a fundamental change of the application security posture that occurs when an application is deployed in a virtual environment.

This architecture presents risks in the case of advanced attacks. From an attacker's point of view, after the initial compromise and takeover of one of the VMs, there are several options for further attack. These may include a "lateral move," aimed at compromising more VMs; an "outward move," aimed at gaining access to SDN components and improving network visibility; or an "upward move," aimed at escalating privileges by crossing from the VM's kernel level to the hypervisor level, an action often referred to as VM escape[1].

New technologies such as virtualization and SDN call for a reevaluation of defensive strategies. Specialized threat protection can be broken into three main strategies – none of which are incompatible, but each of which has different capabilities that should be carefully considered before deployment.

Strategy 1: Deployment of Classic Anti-Malware on Every Endpoint

- **Benefits:** No ancillary costs (subject to licensing in virtual environment) except for initial move/deployment; same (high) maintenance level as current deployments; no personnel retraining necessary (staff already familiar with solution).
- **Drawbacks:** The protection domain level is Ring 0, the same privilege level held by advanced malware, while higher privilege domains exist such as hypervisor/Ring -1 (see Figure 2); competition for resources on the host; poor scalability; unaware of virtual environment and thus prone to conflicts with other software; requires updates on each VM; involves significant efforts to uninstall and replace.

Strategy 2: Agent + Virtual Appliance

- **Benefits:** Can use the advantages of the virtualized environment; uses resources more efficiently because the majority of work is offloaded to the appliance.
- **Drawbacks:** Agent still runs at protection Ring 0 on the guest VM, while higher privilege domains exist; competes for resources on host (though with better scalability than in Strategy

[1] http://www.computerworld.com/article/3182877/security/pwn2own-ends-with-two-virtual-machine-escapes.html.

1); requires updates on each VM and appliance; easier to uninstall than classic anti-malware, but still a significant effort to replace.

Strategy 3: Hypervisor-Based Threat Protection

- **Benefits:** qualitatively new solution that fully leverages virtualized environment, executed below Ring 0, at the hypervisor level; no performance impact on guest VM resources; low maintenance (updates required only on the security server that carries the protection functionality); can be easily replaced or used with other STAP or advanced anti-malware solutions.
- **Drawbacks:** a new technology, which to mature will require ongoing cooperation between security and virtualization vendors.

The Evolution of Modern Threats

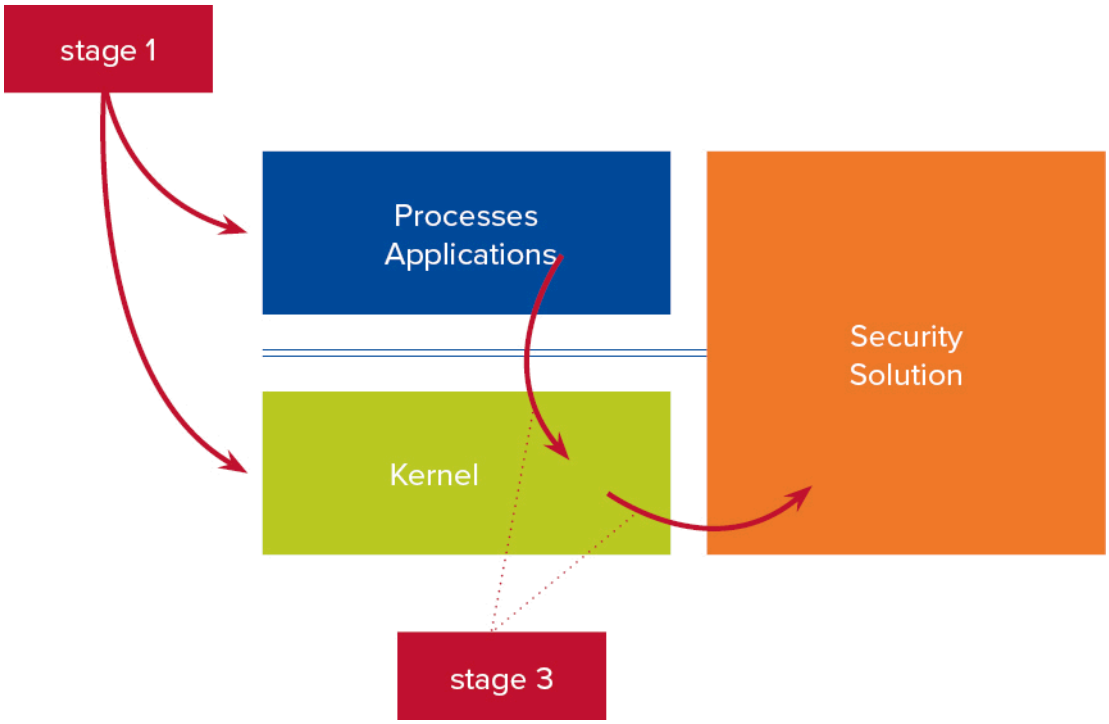
There is a clear benefit to signature-based detection — speed. However, the nature of that technology assumes that the threat is known and has features that can reliably permit its detection. Most modern attacks use evasive techniques to escape detection by signature-based approaches. The other characteristic of advanced threats is persistence: Modern malware uses a variety of techniques to remain on the system. From a business defense standpoint, the most important aspect of advanced threat protection is the ability to detect previously unknown threats and effectively remediate persistent malware or prevent it from infiltrating the system.

In an earlier era, cyberattacks were carried out to cause damage and bring notoriety to the attacker. Today's threats are extremely different. Targets and goals have evolved from loud announcements of an attacker's existence, to the covert pursuit and exfiltration of data that is later sold or used in another way. Advanced threats may even be designed to *wait* for valuable data to appear. These types of threats seek to protect themselves from exposure for as long as possible.

Attackers use a range of techniques to evade detection and remain on the system. Figure 3 shows how advanced malware is used by attackers to gain control of systems and develop an attack. All such attacks can be detected and prevented by hypervisor introspection.

FIGURE 3

Hypervisor Introspection Technology Can Detect and *Prevent* Attack at Multiple Stages (ref. Figure 1)



Advanced tools used by attackers exploit OS limitations that allow them to upgrade privileges and run in Ring 0, alongside security solutions.

Source: IDC, 2017

The following section highlights selected attack techniques that require an effective response from modern threat defense solutions:

- **Kernel-level malware:** This malware runs in Ring 0, making it impossible to detect from lower protection domains (Rings 1-3). Kernel-level malware can hide not only from signature-based detection techniques, but is also difficult to detect with behavior-based techniques when executed in the same protection domain. A prominent example of such malware was Turla, which had full kernel access and therefore was able to evade Kernel Patch Protection on Windows. This made the Turla malware practically invisible.
- **File-less malware:** This kind of malware does not create any files on the system, thus entirely evading file-based anti-malware defenses. By injecting itself directly into the memory of active processes or executing a malicious payload (e.g., with PowerShell on Windows), such malware attacks do not leave any traces on disk. Log entries will contain records of legitimate process execution. The PowerSniff family of malware uses macros in the documents attached to email and PowerShell to execute a payload, often entirely in memory.
- **Environment-aware/multi-stage malware:** Most modern advanced malware distributes itself using a minimal piece of code. The main goal is infiltration of the system. The next goal of this "first stage" code is to understand what environment is running on the system. This will permit the code to pull in a "second stage" code, which is selected based on the specifics of the environment. The Carbanak campaign, which reportedly stole as much as $1 billion from

banking institutions, was a persistent attack that lasted between two and four months at each bank that was attacked. The initial infection was usually via a spear phishing email with a malicious control panel files attachment that deployed a backdoor. This was followed by a lateral movement, mapping, and intelligence gathering on networks and bank processes. In the last stage, money was stolen via a range of methods.

With all the advances in server technology and threats, it is only natural to ask: Are attacks becoming advanced enough to escape the guest VM and infect the host? Unfortunately, and although it is not easy to carry out such attacks, the answer is *yes*.

The security community, including *hardware* manufacturers, is doing its best to change this situation. It must be remembered that while host memory is difficult to access directly from guests, it may be possible due to bugs in the technology stack that result from the increasing role of software. There are also other ways to reach the host machine. Networking is frequently used by threat actors and malware families.

Architecture: Beyond Endpoint Anti-Malware Solutions

As shown in the section on privilege levels (see Figure 2), the issue of a guest security solution being executed at the same privilege level as an advanced attack is part of a broader security dilemma created by architectural constraints.

- Endpoint-level security tools, including anti-malware solutions, application sandboxing, application whitelisting, or device control are effective in understanding the context of an attack. But they remain vulnerable to sophisticated attacks that deploy techniques capable of evading or bypassing these measures.
- Network-based intrusion prevention/detection and higher-layer firewalls (i.e., applications) have significantly reduced vision (if any) into endpoints. If an endpoint is compromised, the isolated security tool and its capabilities are not affected. These tools lack context – that is, they lack awareness of the state of endpoints, especially memory. Any solution that involves an endpoint-based agent in addition to a network-based component suffers from the same limitations as the endpoint security tools.

Though each of these layers can be effective for specific purposes, they may fail to protect against advanced attacks. A solution placed in the hypervisor layer, protected from attacks on the network and endpoints, but with high visibility into endpoint context, would go a long way toward resolving security architecture constraints. Hypervisor introspection provides a mechanism for security solutions to be upgraded to a qualitatively new level.

Hypervisor: A Solution to Contextual Dilemmas

Architectural constraints create trade-offs that make it difficult to counter advanced attacks. It was once thought that either context or the safety of the security solution had to be sacrificed to achieve the other. However, hypervisors can provide rich context while remaining isolated from the VMs they host and the workloads within them.

Table 1 describes the differences in context and protection offered by a hypervisor in comparison to other security solutions.

TABLE 1

Comparison of Hypervisor vs. Endpoint vs. Network-Based Security Solutions

	Context	Solution Protection
Traditional Endpoint Security	Generally rich context, but perspective might be limited by attacks that use evasion techniques to hide malicious action; does not see any other traffic other than what originates or terminates at the machine	May be vulnerable to sophisticated attacks involving advanced malware (such as kernel exploits, zero days)
Network Security	Limited; sees only network traffic and network traffic attributes, but has no visibility to endpoint systems and memories	May be vulnerable to sophisticated attacks involving advanced malware if attacked directly, just as traditional endpoint security is
Hypervisor-Based Introspection	Richest context available; unaltered information drawn directly from the hypervisor layer	Hardware enforced protection drawn directly from the hypervisor layer

Source: IDC, 2017

There are two other key characteristics of hypervisor-based introspection:

Raw Memory at the Hypervisor Level — An Unaltered, Reliable Source of Information

- Hypervisor introspection looks only at raw memory, which is a very reliable source of information.
- Kernel introspection technology analyzes the raw memory image of guest OSs, services, and user-mode applications.
- Hypervisor introspection-based solutions audit both kernel and user memory to identify advanced threats, such as known rootkit hooking techniques and zero-day, or out-of-reach, malware that runs at an equal or higher privilege level than OS security solutions.

Focusing on a Handful of Attack Techniques Rather Than Thousands of Threats

- Despite the variety and large number of malware types, they use only a limited number of memory violation techniques, all of which are visible and detectable at the hypervisor level.
- Memory introspection can detect and help remedy a zero-day attack just as easily as it can counter a known piece of malware.

Several technical challenges had to be overcome to achieve hypervisor introspection:

- The necessary processor developments were realized when Intel launched its Haswell generation of CPUs. This enabled hypervisor-controlled and hardware-enforced isolation between VMs, with lower overheads.
- Hypervisor implementation needs to securely expose introspection capabilities to security solutions, providing access to the memory stream of each VM. This was achieved with the Direct Inspect API released by Citrix.
- A security appliance needs the ability to extract semantic meaning from raw memory lines. Bridging the semantic gap between the hypervisor's hardware-level view of a guest OS is the most demanding challenge. Bitdefender bridged this gap by producing a commercially available kernel introspection solution.

In IDC's opinion, hypervisor-based threat protection holds significant potential as a qualitatively new approach that addresses both advanced threats and traditional malware in virtualized environments. Already highly usable, this technology has the potential as it matures to provide significant security and operational advantages, whether used separately or in combination with other endpoint protection. Hypervisor introspection technology, however, should be used in conjunction with existing security layers, as its ability to protect against file-level threats is limited. Hypervisor-based threat protection is part of IDC's STAP market.

Security: Narrowing Down Business and IT Essentials

Ideally, a security solution should satisfy the needs of both business and IT stakeholders. The difficulty is in the potential conflict of IT and business priorities in the choice of a solution.

What are the most important **business** factors in any IT solution, including security? One will likely get as many answers as the number of times the question is asked. But ultimately, the chosen solution must (a) cause minimal disruption, and (b) reduce operational costs. Operational costs reductions often combine cost avoidance (e.g., early detection or better prevention of security incidents, before damages are incurred) and reduced maintenance costs (i.e., the combined costs of management, updates, and configuration conflicts resolution).

Technology factors are more complex and vary from company to company, but fall mainly into three areas:

- **Technical capabilities:** How good is the solution in detecting threats and halting their execution? How efficient is the solution – that is, does it exert a minimal impact on system resources (mainly CPU and memory)? Can the deployed solution coexist with other processes running on the same hardware without causing conflicts?
- **Operational capabilities:** Does the solution offer ease of deployment and maintenance (e.g., frequency of updates and testing before updates are rolled out in the production environment)? Does it easily integrate with other security solutions, most importantly solutions providing increased situational awareness, such as security information and event management (SIEM)? Does the solution provide actionable information?
- **Architectural benefits:** These advantages are often ignored by smaller companies and overlooked or misinterpreted by larger enterprises. Successful security architecture should fulfill two goals: a) provide a qualitative improvement of defense capabilities, enhancing the total value of existing security solutions; and b) provide flexibility, meaning the solution should have the capability to adjust to changes in security and architectural requirements. Ideally, the chosen security solution should also have a *useful* lifespan that allows sufficient time for a superior replacement to enter the market.

BITDEFENDER OFFERING

The Hypervisor Introspection (HVI) solution developed by Bitdefender is a commercially available technology that provides a qualitative improvement in the security of virtual environments. Memory inspection, often sacrificed by security vendors to preserve the performance of endpoint-deployed agents, is conducted at the hypervisor level with hypervisor privileges (i.e., at Ring -1 – see Figure 2). This provides all the benefits of the highest possible privilege level, while maintaining separation from guest VM environments that are unattainable to agent- or endpoint-based products. This technological advancement came from close cooperation between Bitdefender and Citrix.

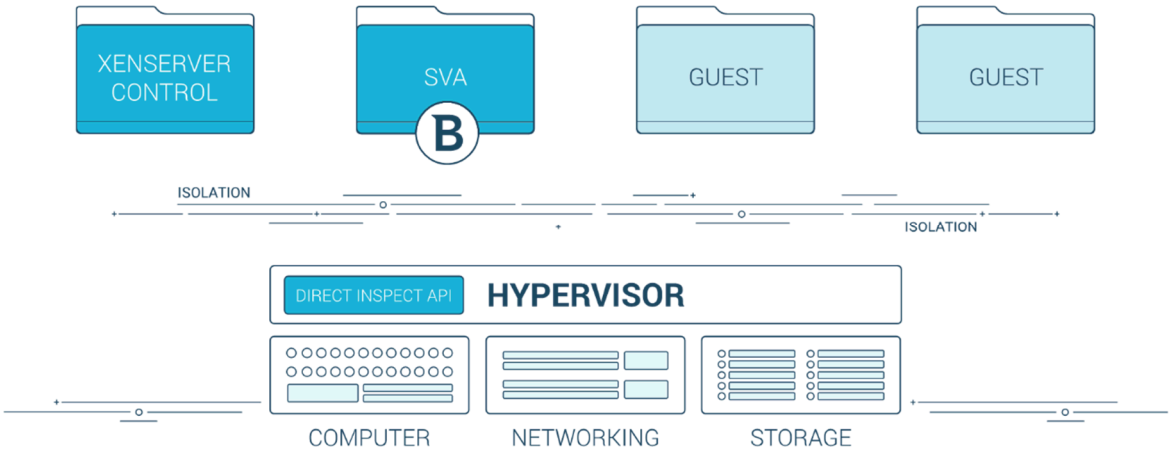
Bitdefender HVI bridges the security capability gap between context-aware endpoint security solutions and context-unaware network security solutions. Attack techniques used by advanced threat actors are increasingly designed to not only evade endpoint defense at the stage of initial compromise, but also to undermine the protection capabilities of any security solution deployed at the same privilege level. This typically renders malicious processes effectively invisible to the deployed security solution.

While running in strong hardware-enforced isolation, HVI is context-aware; context-related information is gathered from the hypervisor. At the same time, the solution lacks the Achilles heel of endpoint-deployed software, as there are no known techniques to circumvent HVI from the guest VM.

One of the most important features that the HVI solution adds to the security toolkit is the ability to detect and stop *unknown* attacks. HVI detects anomalous software behavior in the guest VM and can stop all advanced attacks described in this paper, including zero-day attacks. HVI can detect legitimate process memory access attempts performed by attackers, as well as OS-level techniques used to cloak malicious processes.

FIGURE 4

HVI: API



Source: Bitdefender, 2017

In addition to its innovative technical capabilities, Bitdefender's solution is attractive from an operational standpoint. It requires significantly less maintenance due to the agentless nature of the solution, and because there is no endpoint-side software to maintain or update. Another feature is independence from the guest OS because detection of anomalies is performed at the hypervisor level. Once an anomaly is detected at the hypervisor level, HVI will remediate the threat in real time. HVI provides an integration capability with SIEM or similar solutions to provide the necessary data (such as attack source, targeted areas, and details of the attack technique) for further correlation and analysis, helping improve overall situational awareness. HVI also has the capability to automatically inject a temporary tool into the affected VM to remediate the threat.

Attempts to exploit a system or application send a clear signal to operations that additional attention is required. Depending on the information, the request can be addressed to an appropriate party — IT, if the compromise attempt was on OS or other off-the-shelf software, or development, if the compromise attempt was on an in-house-produced application. However, when attacks are stopped by HVI, there are no associated response costs, as the incident was effectively prevented rather than just detected. This extends the time companies have to improve their defenses, such as by issuing or applying security patches to vulnerable software.

Many security vendors concentrate on the detection of compromises, with the aim of shrinking the time between compromise and detection and reducing post-incident clean-up costs. Bitdefender created a qualitative improvement that can be used in addition to or instead of some existing security solutions.

Whether HVI is deployed as a complementary or replacement solution depends on the risk appetite of the specific business entity.

HVI: Significant Potential, but Challenges Remain

There are several challenges that adopters of this promising solution should be aware of:

a) While thoroughly tested by Bitdefender and Citrix, the technology is new and is likely to go through an initial adoption and maturity phase. There is no doubt, however, about the potential of this technology, and the significant impact it will have on virtual environment defense capabilities.

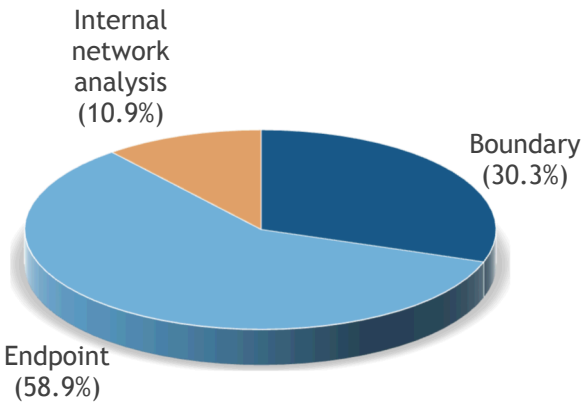
b) At the time of this writing, Bitdefender HVI is available only for the Citrix (Xen) platform. Other virtualization platform implementations are under development. In addition to working closely with virtualization vendors, Bitdefender is cooperating with Linux to ensure high visibility for its efforts and to improve the prospects for long-term success. Positive reactions from the broader technology community emphasize the possibilities offered by the hypervisor introspection method.

STAP — BEYOND THE ENDPOINT

Just as security posture is defined by more than endpoint protection, so the STAP market is much broader than solutions that focus only on endpoint hardening. IDC's market structure divides STAP into three segments: Boundary STAP, Endpoint STAP, and Internal Network Analysis, as detailed in Figure 5.

FIGURE 5

Worldwide Specialized Threat Analysis and Protection Market Share by Segment, 2016



Total = $1,700.5 Million

Source: IDC, 2017

This market grew by around 27% worldwide in 2016, and is projected to continue growing at a double-digit rate in each of the next four years. Note that the STAP market is made up of distinguishable products, as opposed to embedded features within some other product. Preventing advanced threats requires dedicated activities, and this approach reveals the extent to which enterprises are consciously

taking action to deal with these threats. In technology terms, IDC's taxonomy describes areas that deliver non-signature-based malware detection or blocking:

- **Sandboxing:** This involves taking a file and "detonating" it to see how it behaves. The operations of the file are analyzed to determine if any unexpected activities, such as the modification of registry keys, the running of processes, or suspicious communications occur that would signify possible malicious activity.
- **Containerization/isolation:** Solutions in this framework essentially work to prevent malicious files from having access to an internet connection or the system resources of an infected machine. Specific applications or tasks can be virtually segmented from the rest of the machine, ensuring that malware is not able to spread or "phone home," rendering it benign.
- **Static file analysis:** This technique inspects files for content (e.g., embedded URLs or file calls) that the file should not have.
- **Advanced system scanning:** This technology examines system behavior for signs of malicious activity. Generally, it will include taking a snapshot of a system to get a baseline that is later used to identify when subtle changes take place. This can be done by monitoring the operating system for registry modifications, questionable processes, or other signs, or by analyzing the actual physical memory for malicious activity.
- **Whitelisting:** This allows the execution of approved processes only.
- **Telemetry analysis:** This examines many different actions to monitor operations for anomalies. Telemetry analysis uses both behavioral analysis and heuristics. It can be used across all submarkets by looking at data from the file system, registry changes, network connections, binary executables, and execution calls. Most bot command and control detection is based on telemetry analysis.

Hypervisor introspection incorporates multiple STAP techniques, including advanced system behavior analysis, whitelisting, and monitoring for anomaly detection.

LEARN MORE

Related Research

- *Worldwide Specialized Threat Analysis and Protection Forecast, 2016–2020: Enterprises Modernize Security Infrastructure* (IDC #US42068916, December 2016)
- *Western Europe Specialized Threat Analysis and Protection Forecast, 2016-2021: The Enterprise Strikes Back* (IDC #EMEA42348817, March 2017)

Synopsis

The Hypervisor Introspection (HVI) solution developed by Bitdefender delivers a commercially available technology that provides a qualitative improvement in virtual environment security. Memory inspection performed at the hypervisor level with hypervisor privileges, while maintaining strong, hardware-enforced, separation from guest VM environments, is capable of halting advanced attacks. The technological advancement came from close cooperation between Bitdefender and Citrix

.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC CEMA

Male namesti 13 110 00
Praha 1 110 00 Czech Republic
+420 2 2142 3140
Twitter: @IDC
idc-community.com
www.idc.com