Protecting Virtualized Environments—Addressing Security in the Virtual Future

Whitepaper

SentinelOne

Cloud Infrastructure is on the Rise, and Security is Lagging Behind

Cloud technology has solidified itself in the business world to the point that adoption is no longer as much of an option as it is a requirement. With 82% of enterprises adopting a hybrid cloud strategy and 95% of businesses running or experimenting with infrastructure-as-a-service, it's clear that shifting to virtual environments isn't a passing fad—it's a reality that businesses of all sizes must deal with, especially from a security standpoint.

There are plenty of benefits driving the move from physical data center environments to cloud-based virtual infrastructures; but as the virtual infrastructure grows, so does a company's attackable surface area. In fact, 94% of security professionals agree that increasing the number of virtual workloads can increase attackable surface areas by two to 100 times.

In many cases, the prevailing thought is that as the attackable surface area grows, companies are failing to accelerate their security hiring in lockstep. However, accelerating security hiring is only a temporary solution to a problem that will only amplify as virtualization becomes more entrenched in business.

The goal of an increasingly virtual business can't be to hire more security professionals in direct correlation to increased risk—this simply isn't a scalable approach.

Rather than trying to force existing processes and hiring practices into emerging virtualization security challenges, companies should be looking for a more efficient and scalable way to protect their virtualized environments. This white paper will dive into the risks associated with a shift to virtualization and discuss how to effectively defend virtualized environments—the transition from physical data centers to virtualization is inevitable and businesses can't afford any security missteps.

Why Shifting to Virtualized Environments is Good for Business

In the early days of cloud technology, there was overwhelming concern for virtual security as companies were reluctant to lose some of the control they enjoyed in physical data centers.

Now, the benefits of cloud infrastructure are too attractive to ignore and companies of all sizes are looking to capitalize. Shifting to virtualized environments introduces a number of business benefits, including:

1. Cost-Effective Operation: Virtualization makes physical servers far more concentrated than in traditional data centers. Because one physical server can run multiple virtual machines, companies can maximize processor and storage uptime rather than using a server to run one instance of an operating system.

2. Cost-Effective Security: Rather than setting up in-line security appliances and applications for multiple physical servers, many virtual machines can be protected by the same security solutions running on a single, concentrated server.

3. Isolation: Virtual machines run independently with a hypervisor overseeing workloads. This inherent isolation means that if one virtual machine goes down, other VMs will not be affected.

4. Fast Recovery: Going virtual introduces a sense of data mobility that isn't possible in physical data centers. Virtual machines can be copied to multiple locations and backup images are easy to create, meaning that in the case of an outage, a failover VM can be initiated quickly.

5. Variable State: Administrators can take VMs offline or turn them back on with a few simple clicks, making it much easier to troubleshoot and avoid potential attacks when there is a known vulnerability.

Unfortunately, many companies get so caught up in these advantages of virtualization that they grow complacent with security (or security becomes somewhat of an afterthought).

According to recent research from Kaspersky Lab, 34% of businesses don't even realize there's a difference between security of physical and virtual assets. This leads many to implement the same solutions and strategies to protect their virtualized environments as they've used for years in a physical data center environment.

Understanding the security implications of virtualization—the risks, not just the benefits listed above—is critical when trying to effectively shift to a virtual infrastructure.

Virtualization Security Risks—The Vulnerabilities Businesses Must Consider

Despite original reluctance to virtualize, the narrative surrounding virtualization security has started to flip in the last few years. Kaspersky research found that

42% of businesses consider the security risks of virtualization to be less significant than those facing physical environments.

Benefits such as variable state and isolation are inherently positive for virtual machine security, but that doesn't mean virtual environments are necessarily more secure than physical environments—the vulnerabilities are just different.

Cyber attackers are creative and seem infinitely capable of exploiting new vulnerabilities every day, but the Cloud Security Alliance has identified 10 specific vulnerabilities that come along with a move to virtual environments that offer an idea of what businesses are dealing with from a security standpoint:

1 Virtual Machine Sprawl: On the one hand, companies have the benefit of spinning up new virtual machines very quickly. But on the other hand, this can lead to a rapidly expanding footprint of virtual machines that becomes increasingly unmanageable. When VM sprawl leads to unpatched and unaccounted-for machines, cyber attacks become much more likely.

2 Sensitive Data Within a Virtual Machine: Again, the convenience of virtual machines is both a blessing and, at times, a curse. Because it is so easy to move and change data within a VM, confidentiality can be difficult to maintain amidst human error.

3 Security of Offline and Dormant Virtual Machines: With virtualization, it's easy to take an instance offline when it's not in use. This is a great cost saver, but can become a security risk depending on how long the VM has been offline. If a company has reconfigured its baseline traffic expectations multiple times since taking a specific VM offline, turning that VM back on can have a negative effect on security.

4 Security of Pre-Configured Virtual Machines: In the case of virtualization platform compromise, attackers can reconfigure VMs or inject viral payloads into virtual disks.

5 Lack of Visibility into Virtual Environments: If visibility isn't addressed when moving to virtualized environments, it can be easy to lose track of whether or not security appliances and applications see 100% of network traffic, leaving holes for attackers to exploit.

6 Resource Exhaustion: Virtual workloads can place heavy demand on physical resources. Resource exhaustion causes application downtime that can result in security holes.

7 Hypervisor Security: The hypervisor acts as the controlling software/firmware above virtualized environments. If it goes unpatched, it can become a single access point for attackers to compromise the entire virtual infrastructure. Virtual machines benefit from inherent isolation, but compromising the hypervisor eliminates this advantage.

8 Account/Service Hijacking Through Self-Service Portals: Privilege escalation is a major component of any advanced attack—having access to a self-service portal gives attackers an opportunity to move laterally until they compromise admin credentials.

9 Workloads of Different Trust Levels on the Same Server: Virtual machines are isolated, but companies still must take the proper steps to segregate workloads within a server to avoid creating vulnerabilities.

10 Insecure Cloud Service Provider APIs: Today's virtualized environments typically manifest in a hybrid cloud strategy. The APIs associated with public cloud providers can pose security risks if they aren't used correctly.

The benefits of virtualization make the shift from physical data centers to virtual environments inevitable. However, addressing these potential risks—and more specific types of attacks—must become a higher priority for businesses hoping to leverage virtualization for business value.

How Can Attackers Compromise General Virtualization Vulnerabilities?

Understanding the potential holes that attackers can compromise in virtualized environments is a good first step when considering how to protect virtualized environments. The logical next step is to determine the different ways that attackers can actually exploit those vulnerabilities.

There are potentially countless ways that attackers can leverage these vulnerabilities, but attacks on virtualized environments generally fall into two categories—attacks between two (or more) virtual machines and attacks between virtual machines and their hypervisors.

Three common VM-to-VM attacks are sniffing attacks, spoofing attacks, and denial-of-service attacks. Because virtual machines share a common host, attackers can potentially sniff packets that are traveling between VMs, stealing valuable data in the process. If hosts are misconfigured, attackers can identify IP addresses of communicating VMs and divert packets to their own machines.

Spoofing attacks are when attackers compromise the virtual switches that connect VMs to their hosts. Because the address resolution protocol (ARP) used to help VMs communicate to their hosts doesn't require proof of origin, attackers can use it to capture MAC addresses and redirect VM traffic to a command and control server.

Denial-of-service (DoS) VM-to-VM attacks take a different approach than sniffing or spoofing attacks—rather than diverting traffic to a command and control server, denial of service occurs when attackers flood VMs with requests, overloading them until resources are exhausted and systems go down.

While VM-to-VM attacks are problematic, companies face more serious consequences in cases of VM-to-hypervisor attacks. Similar to VM-to-VM attacks, there are three types of threats to be aware of—VM hopping, VM escape, and mobility.

In the case of VM hopping, attackers with access to the hypervisor can move from one VM to another with nothing more than an IP address. From here, attackers can choose to disrupt or modify the flow of traffic or even launch a widespread DoS attack.

A VM escape attack takes hackers out of the virtual machine context. They can run code on a VM that helps them break out of the specific machine and into the hypervisor itself, enabling attacks on operating systems rather than machines themselves.

Mobility isn't so much an attack vector as a way for attackers to compromise virtual environments. Because VM files are stored on the hypervisor, moving a virtual machine to another host requires a new virtual disk as well. If attackers gain access to this copied virtual disk, they can quietly steal sensitive data because it's difficult to trace the many copies of a VM.

With so many different ways to attack virtualized environments, it may seem surprising that any company could lose focus on security. However, companies have been able to relax on virtualization security because virtual environments have not yet experienced a watershed—a massive breach that sees mainstream media attention, similar to the now-famous attacks on Target, Anthem, Sony Pictures, and so many more.

The problem is that the consequences of even a small-scale attack on virtual environments can be more painful than companies might expect.

Attack Aftermath—Physical Environments vs. Virtualization

Contrary to popular belief, an attack on a virtual environment can prove to be far costlier than those on physical data centers. According to Kaspersky Lab, the average cost of a virtual breach is $800,000—more than double the cost of a physical breach. While a virtualization attack hasn't hit mainstream media just yet, the costs can be potentially crippling to many businesses.

The consequences of a virtual data breach are, for the most part, the same as a physical data breach—loss of personally identifiable information (PII), reputation loss, etc. However, attacks on virtual environments are more costly because of business-critical application downtime.

While 66% of incidents affecting virtual platforms result in critical-information downtime, only 36% of attacks on physical environments have this consequence. This isn't the sole reason why attacks on virtualized environments are more expensive, but it is a leading factor.

The bottom line, though, is that attacks on virtualized environments cannot be ignored any longer. Businesses need a legitimate means of protecting their virtualized environments outside of simply hiring more security professionals.

What Can Businesses Do to Defend Against Emerging Virtualization Threats?

Virtual environments are becoming too vast for companies to implement universal protection across every server—it's simply impossible (financially and operationally) to cover everything to such a degree. This will necessitate a risk-based approach to security in which companies will have to evaluate various levels of protection for specific server workloads.

Neil McDonald recently laid out a server workload protection hierarchy with 10 separate levels of optional and core server protection strategies to discover.

According to McDonald, the following 5 strategies are core pieces of security for every server workload:

1. Exploit prevention/ memory protection
2. Application control/ whitelisting
3. Configuration and vulnerability management
4. Integrity monitoring/ management
5. Network segmentation and traffic visibility

Traditional signature-based anti-malware solutions won't suffice in a world where these strategies are core components of protection. Because attackers are launching advanced threats with zero-day components, signature-based solutions won't effectively identify or stop such attack vectors.

However, virtualization security solutions typically only address one of these core components (and that's not to mention the additional 5 optional, but often important, strategies). Managing a multi-vendor stack with potentially 5 or 10 different virtualization security solutions is a sure-fire way to create new vulnerabilities as a result of mismanagement or poor integration amongst solutions.

This is why SentinelOne created a new approach to protecting servers in virtual environments. In one solution, companies gain access to exploit prevention, memory protection, whitelisting, and (soon) application control. In addition to these core components, SentinelOne's solution includes advanced behavioral detection and response, an optional strategy for more advanced virtualization protection—for more valuable assets in virtual environments.

If you want to learn more about how the SentinelOne solution helps companies consolidate their security stacks while also addressing key vulnerabilities specific to virtualized environments, contact us today for a free demo.

For more information on SentinelOne, visit www.sentinelone.com. To schedule a demo tailored for your organization, visit www.sentinelone.com/contact.