Protect Virtual Infrastructure with Next-Gen Security

June 10, 2014
by SentinelOne


Virtual Infrastructure

The concepts of the software-defined data center (SDDC) and the private cloud have begun to explode. While the market is projected to reach staggering heights by the end of the decade, incorrect assumptions about the nature of virtual machines can expose users to a staggering amount of risk. Let's learn why a virtual infrastructure is susceptible to security breaches, along with a few ideas on how to lock down virtual environments ahead of your next attack.

The first thing to understand is that sandboxes are not inherently secure. There was a time when malware ignored or avoided virtual machines, but that time ended in 2012. That year was the advent of 8012 Crisis, the first of a new breed of malware that actively sought out VMs. The authors of Crisis realized that VMs are essentially just files, and thus the program would look for those files on an infected machine, mount them, and then copy itself onto the sandbox devices. Once installed, it would eavesdrop on Skype, steal IM logs, and copy down the user's browser history.

Crisis never really presented a world-shaking threat in terms of its capabilities. Its features have been inevitably iterated upon, however. There's a lot more malware targeting VMs, and some strains resist re-imaging. There are several ways to do this: say that several VMs are connected by a virtual infrastructure switch, for example. Since traffic never passes over a physical network, traditional security tools won't notice when a virus completes a lateral movement from one VM to another. Some malware might specifically target the hypervisor. Worst of all, some malware is able to break out of a VM and attack the host device (although this is rare).

Security professionals have a few paths forward that they can take in order to lock down virtual environments. Auditing is a hugely important step—IT professionals need to monitor the tools that control their cloud environments, as well as the accounts that have access to them. Once you've catalogued your virtual infrastructure, the next step is to lock it down.

As described, malware can attach from VM to VM over a virtual switch—a process known as hyper luminal. There are a few options to ensure that hyper jumping isn't a possibility. The first is simply to segment your networks. The second is to use a Private VLAN that prevents each individual VM from detecting other VMs in its environment.

Lastly, it's important to choose the right kind of server protection. You can protect individual VMs with antivirus, but some programs will massively increase each machine's RAM footprint. When the solution scans for malware, or updates its signatures, this will cause the load on bandwidth, memory, and CPU usage to increase, tying up business-critical processes. It's important to choose a solution that can run without damaging the productivity of your data center.

SentinelOne provides that solution. Our next-gen malware protection platform for servers runs out-of-band, meaning that it ties up a minimal amount of system resources. What's more, our solution doesn't rely on malware signatures. Bad actors will always iterate on their malicious software faster than AV vendors can find signatures for them. SentinelOne dispenses with signatures, instead using machine learning and behavioral analysis to detect infected machines. With SentinelOne, you'll find that you're safe not just from known viruses, but malware that's never been seen before in the wild.

For more information about how SentinelOne can protect your datacenter against threats both rare and exotic, contact us today!

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Axiomatic Security is Fundamental to Data Center Security
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 6 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls
- How to Modernize Vulnerability Management in Today's Evolving Threat Landscape