SentinelOne™

Securing Virtual Desktop Infrastructure (VDI)

SENTINELONE VDI SOLUTION

The SentinelOne agent is an efficient solution to secure virtual infrastructure including virtual machines, thin clients, layered apps, and VDI implementations. It does not need updates and is not dependent on signatures or other legacy antivirus requirements.
The SentinelOne offering for VDI includes all protection engines and functionality - the same as we support for physical devices - without exceptions.

In recent years, VDI (Virtual Desktop Infrastructure) implementations have become more common than ever before. VDI hasn't replaced the entire desktop market as some predicted, but more and more enterprises have adopted VDI environments due to a variety of operational benefits. According to Gartner, large enterprises are adopting VDI at high rates, with only 15% not planning to invest in VDI technology.

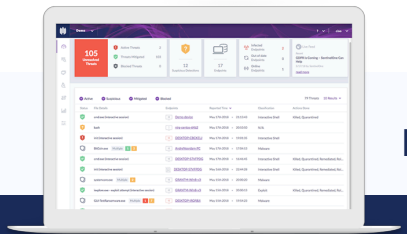
THE NEED TO SECURE VDI

Common risks impacting data still prevail in VDI environments: ransomware, social engineering, drive-by downloads, network sniffing, vulnerability exploits, insider threats, privilege escalations, and malware. Some would claim VDI is a more secure option, mainly because one can terminate the VDI instances once done, but the overall security state is only as strong as its weakest link – and VDI deployments tend to be exactly that for several reasons:

1. Patching cycles require updating the golden image and are therefore not rapid.
2. VDI implementations commonly try to consume as little resources as possible, so administrators try to reduce the amount of software deployed - sometimes at the expense of protection.
3. The human factor: users tend to be less aware of security implications when running on VDI because they often don't own the system and use it for a temporary session.

SUPPORTED PLATFORMS

Oracle VirtualBox · Citrix · vmware® · Microsoft Hyper-v · amazon WorkSpaces



READY FOR A DEMO? *Visit the SentinelOne website for more details.*

SentinelOne™

www.sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043

6 Key Factors to Secure VDI

1. DON'T SETTLE FOR RELIANCE ON UPDATES

Products that rely on updates will create an "AV storm" every time users login because they mandate an update. Products which rely on updates for security need to overcome the challenge of new sessions starting over and over again and then trying to update them. Once a session terminates, this vicious cycle repeats, consuming bandwidth, resources and impacting productivity. For these reasons, deploying security products has traditionally been quite painful in VDI environments.

2. REQUIRE EASE OF MANAGEMENT AND AVOID DUPLICATE ENTRIES

Products that rely on device names to identify users will experience collisions. Another important aspect is the ability to automatically decommision agents. A security product which does not retire closed sessions leads to numerous "phantom devices" rendering a distorted operational view and inability to manage assets effectively at scale.

3. BASE IMAGE SCANS ARE NEEDED

Ensure the golden image is flawless, and clean from malware. Products which solely rely on "seeing" the malware dropped to the disk or simply checking only on file execution are not sufficient for this attack surface, leaving your VDI environment vulnerable.

4. REQUIRE EQUIVALENT PROTECTION AND FUNCTIONALITY

Some vendors offer dedicated agents for VDI albeit with limited functionality. It leaves VDI environments as an exposed attack surface. There is no reason to have crippled VDI coverage. Look for vendors who do not compromise and can deliver full protection, visibility, and response capabilities.

5. CALCULATE THE TRUE COSTS

There are several licensing models when it comes to VDI:
Concurrent (pay as you go) or Per-seat (pay for each user) - look for the right license model for you as it will reduce your costs.

6. PERFORMANCE IMPACT MATTERS

One advantage of VDI is a reduction in hardware and operational costs. If you end up with an AV solution that requires resource allocation as if it was a physical device, you are missing out. Another aspect that will influence VDI performance is the number of applications you need to install on the base image. Opt for endpoint protection solutions that are lightweight and robust so that computer power and end user experience/productivity aren't compromised to run AV.

SENTINELONE BENEFITS FOR VDI

BETTER SECURITY

SentinelOne combines prevention, detection, and response in a purpose-built single agent/single console architecture.

BETTER SCALABILITY

Using predictive technologies which obviate the need for daily/weekly signature updates. By reducing the disk IO overhead and avoiding IO storms, we help organizations to improve VM density on their virtual infrastructure through efficient scaling.

EASIER TO MANAGE

The console automatically decommissions VDI instances that are no longer in use reducing the administrative overhead and preventing decommissioned "ghost endpoints" from appearing in the management console.

SUPPORTS ALL VDI USE CASES

SentinelOne supports persistent/non-persistent setups, linked clones, and even cloud deployments. We offer a concurrent licensing model tied to your enterprise license. Natively managed by SentinelOne policy, including auto-decommissioning of agents.

FOR MORE INFORMATION ON SENTINELONE, VISIT WWW.SENTINELONE.COM.

SentinelOne
www.sentinelone.com • sales@sentinelone.com
+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043