Securing Virtual Desktop Infrastructure (VDI)

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.

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.

Supported Platforms

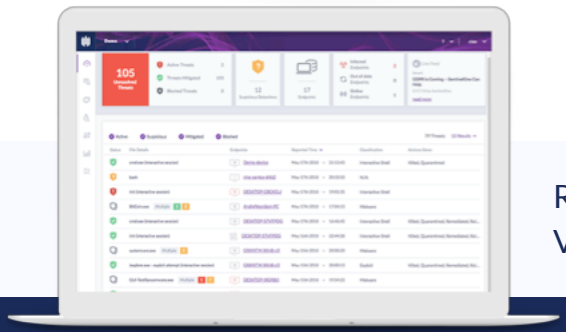
amazon WorkSpaces

CITRIX

vmware Horizon View

Microsoft Hyper-v

VirtualBox



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 automaticly 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. This 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 licesing 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.

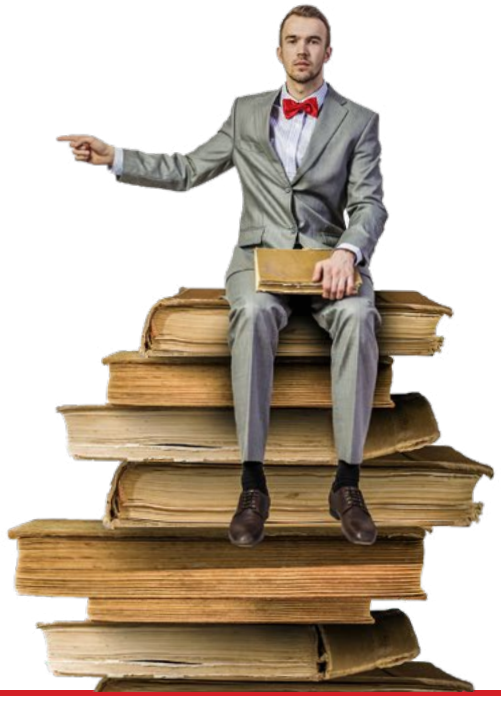
BETTER SCALABILITY
Using predictive technologies which obviate the need for daily/ weekly signature updates. By reducing the disk IO overhead and avoiding IO storms, we help organizations to improve VM density on their virtual infrastructure through efficient scaling.

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.

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

Bedankt voor uw interesse in SentinelOne!



Hopelijk heeft dit document u de benodigde informatie en inzicht gegeven waar u op zoek naar was.

Wilt u meer informatie over SentinelOne? Hier hebben we nog meer voor u:

» **SentinelOne whitepapers en e-books**
» **SentinelOne videos**
» **Vraag een demo van SentinelOne aan**

Andere tools die uw organisatie weerbaarder maken

ProteQtor IT Security is niet alleen reseller partner van SentinelOne, maar biedt nog meer cybersecurity tools aan om uw organisatie zo weerbaar mogelijk te maken.

Hieronder tools die wellicht interessant zijn ter bescherming van uw organisatie:
» Bescherm smartphones en tablets met **Lookout mobile security**
» Beveilig uw e-mail met **Proofpoint email security**
» Train uw medewerkers met laagdrempelige **Wizer security awareness trainingen**
» Bescherm het inloggen met **Watchguard Authpoint multi-factor authenticatie**
» Voorkom bezoeken aan ongewenste websites met **NSOC360 Safeweb webfiltering**
» Krijg inzicht in de veiligheid van uw netwerk met **Guardian360 scans**
» Herstel verloren data met **NSOC360 Safedata online backup**

ProteQtor
Next-Gen IT Security

Laat hackers uw bedrijfscontinuïteit niet in gevaar brengen!

Cyberaanvallen bedreigen privacy, bedrijfskritische data, de reputatie en andere 'kroonjuwelen' die cruciaal zijn voor de continuïteit van uw organisatie. De vraag is allang niet meer 'of' uw organisatie aangevallen wordt, maar 'wanneer' uw organisatie (weer) aangevallen wordt. Het is essentieel om cyberaanvallen te voorkomen en de gevolgen van cyberaanvallen tot een minimum te beperken. Het feit dat u deze pdf leest, toont dat u dat belang inziet.

Vanwege de grootte, de complexiteit en de diversiteit van moderne cyberaanvallen is een multidisciplinaire aanpak nodig. We helpen u graag met praktische adviezen en effectieve oplossingen om deze aanpak te realiseren.

Met de juiste trainingen, tools en support helpen wij u hackers het hoofd te bieden en er voor te zorgen dat alles wat voor uw organisatie van waarde is, beschermd blijft.

Hulp nodig? Bel 088-0660770 of plan een afspraak in

ProteQtor
Next-Gen IT Security

Telefoon : +31 (0)88 066 0770
E-mail : contact@proteqtor.nl
Website : proteqtor.nl