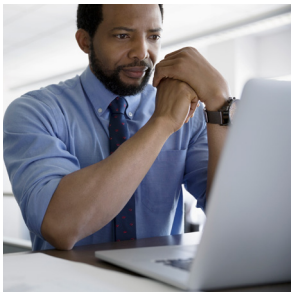
CYLANCE

BUSINESS BRIEF

SECURING VDI WITH CYLANCE®



MISPLACED TRUST

Implementing Virtual Desktop Infrastructure (VDI) solutions does not necessarily result in significant cybersecurity benefits. While there is the belief that keeping sensitive data off of endpoints greatly reduces the risk of information loss, there are still risks related to the common practice of employees removing data from centralized control. Email forwarding, cloud storage, and client drive mapping are a few ways users circumvent VDI-imposed data restrictions.

VDI customers may also be unaware that both persistent and non-persistent clients can be hacked to grant admin access to the larger environment. This is accomplished by using the Help tab to access a web browser or exploiting *File -> Open* to jailbreak out of applications.

TRADITIONAL AV HEADACHES

Signature-based AV solutions are difficult to maintain on VDI platforms. New signature updates require a full image scan, which consumes considerable system resources and degrades productivity. Deploying more servers to mitigate AV driven productivity losses can be extremely expensive. Excluding portions of an image from being scanned can improve the process but also creates additional security risks. These issues result in many VDI enterprises foregoing AV solutions altogether.

CYLANCE AI PROVIDES SOLUTIONS

Cylance uses advanced artificial intelligence (AI), mathematical models, and high performance lightweight agents to overcome the major issues facing cybersecurity in VDI environments.

CylancePROTECT®

- Profiles and prevents threats by using advanced AI instead of signatures, eliminating the need for frequent and costly updates
- Runs services on the endpoint which hook directly into the OS and provide added security against memory exploitation

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

- Is proven to detect and prevent unknown malware that did not exist when the AI models were trained and deployed, with an average lead time of over two years
- Identifies non-persistent VDI installations and assigns them unique IDs

CylanceOPTICS™

CylanceOPTICS deploys machine learning models directly on the endpoint and monitors systems for suspicious or malicious behavior. It facilitates easy threat hunting, detailed root cause analysis, remote forensic investigations, and automated threat detection and response. CylanceOPTICS includes powerful research tools for threat responders:

- InstaQuery - Identifies suspicious behavior by comparing current actions to historic system behavior
- Focus View - Creates context by providing a timeline of events leading up to each detection
- Auto Response - Endpoints can be configured to respond to threats automatically, freeing up critical business resources for other uses

SECURING VDI CHECKLIST

VDI can provide organizations with a cost-effective and scalable way to support growth. As with any new environment, however, ensuring consistent security is paramount. To ensure a solid VDI security strategy is in place, consider these five questions before deploying VDI:

- What systems should move to a VDI?
- Does my existing security solution officially support VDI deployments?
- How will my security tools respond to the dynamic nature of VDI instances?
- Is there a security tool that I could use in my VDI that does not require significant, on-going maintenance?
- Can my existing security solution adequately protect remote endpoints that may suffer from unreliable connectivity?

VDI deployments are commonplace today, saving organizations significant time, money, and resources. By taking a moment to prepare for a move to VDI, organizations can ensure a smooth transition with minimal business disruption.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

©2018 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20181024-1120