CYLANCE™

SECURING VIRTUAL DESKTOP INFRASTRUCTURE

Virtual desktop infrastructure (VDI) was heralded as the cure-all for cybersecurity and malware, but the celebration would be short-lived. VDIs can still leave enterprises vulnerable, unless artificial intelligence and machine learning protect their endpoints.

VDI: Not As Secure As Promised

VDI puts important enterprise data and the operating system on a virtual machine on a server while users access the data and OS through lightweight endpoint devices. The theory is that by keeping the important data locked up on a server and only exposing the lightweight endpoints to the outside world, malware attacks can be avoided.

Enterprises believe that by turning to VDI, they can skip having to secure their endpoints because if an endpoint becomes infected, it is far enough away from the important data and infrastructure that the endpoint device can just be sacrificed and re-imaged without having any effect on the important data on the server.

But in reality, malware can work its way through a VDI-based network with just a little extra effort on the part of the attacker. By including a specialized call into their malware, the malware will let the hacker know that the endpoint it has found is part of a VDI, then can search for the next endpoint, over and over again, until it finds an endpoint that is not VDI-based. All it takes is for the attackers to find one connected endpoint that is not running in the VDI, and they can infect all of the other connected endpoints.

And while the sacrificial VDI endpoint may be viewed as completely free of anything the hackers can use to gain a foothold within an organization, this is just not the case. These VDI-based endpoints still house user profiles and browser caches, which contain files that can be infected with malware.

This challenge has led some organizations to simply put their traditional antivirus solution on the lightweight VDI endpoints in an attempt to secure them, but with traditional antivirus systems relying on downloading and storing signatures or continually pinging servers to check new files in the browser cache against a list of existing threats, lightweight endpoints can become bogged down fairly easily, drastically impacting users.

Other solutions have attempted to avoid endpoint strain by developing an ‘agentless’ product which runs on the server instead of the endpoints, but this still leaves user profiles, browser caches and memory vulnerable to script-based and other attacks. The only true solution to secure VDI-based environments is to have a lightweight artificial intelligence and machine learning based endpoint agent on the exposed endpoints.

CylancePROTECT®: Protecting VDIs from Malware

Cylance clients can protect both physical and virtual machines with our award-winning product, CylancePROTECT, which can be deployed onto Windows VDI workstations as well as every other network endpoint.

Based on artificial intelligence and machine learning, CylancePROTECT is proven to work on the following enterprise virtualization technologies:

- Microsoft RDS/Terminal Services
- Microsoft Hyper-V
- Citrix XenDesktop
- VMware Horizon/View
- VMware Workstation
- VMware Fusion

CylancePROTECT works well as a guest OS component and has several advantages, including:

- A lightweight agent that does not compromise endpoint performance
- Endpoint security that is invisible to end-users
- Protection from malware that does not require regular updates or an Internet connection
- Preparation and deployment in virtual environments that is as easy as deployment on physical machines
- Execution control at the endpoint that eliminates the need for offload scanning of any sort
- Elimination of the need for a dedicated virtual appliance to conduct offload scanning, resulting in one less piece of network infrastructure to maintain

Traditional and 'agentless' solutions CANNOT protect organizations from malicious scripts and malicious processes in memory, but CylancePROTECT offers memory protection and script control for VDI-based environments. Both of these functions use a process injection method whereby the agent code injects itself into running processes in order to identify and block unwanted or unauthorized code from running. Cylance memory injection technology ensures compatibility with third-party applications and conflict prone environments while maintaining protection against violations in the memory space.

What Should Security-Minded Enterprises Do?

Take the extra security precautions they feel are necessary in setting up their VDI environment, but then secure those environments with CylancePROTECT.

1.844.CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Ave., Suite 700, Irvine, CA 92612

CYLANCE™