A Guide to Closing All Potential VDI Security Gaps

IT and security leaders are embracing virtual desktop infrastructure (VDI) as a way to improve security for an increasingly diverse user population. Even with VDI, however, there are still security concerns that can be overlooked. Examples include thin clients running Microsoft Windows Embedded Standard (WES) as well as Windows virtual desktops, which can be insecure because they lack anti-malware software. This white paper discusses how to address these specific challenges within the framework of an overall VDI security strategy that extends all the way from the data center to the edge. With an end-to-end approach, security teams can reduce risk, improve flexibility and support an uncompromised user experience. Here’s how.

Improving security is one of the main reasons why many IT organizations are turning to VDI to support their user populations. By keeping applications and data centrally located under lock and key within the data center, IT teams have more control in closing potential endpoint security gaps and responding to issues if they do arise.

In addition, VDI gives IT a lot more flexibility and control in supporting an increasingly diverse base of users, who may be using combinations of desktops, laptops, tablets, bring your own devices (BYOD) such as smartphones, and company-supplied thin or zero clients. Security and BYOD are typically cited as two of the critical reasons why VDI deployments are
continuing to expand quickly—with a projected compound annual growth rate of more than 27% from 2016 to 2020, according to research from Technavio.¹

While many clients may be running a traditional Windows operating system, a comprehensive end-to-end VDI security solution must also support users of other operating systems, such as Mac OS or Google Chrome, as well as users of nontraditional operating systems such as Microsoft WES.

Despite the overall security improvements and protections engendered by VDI deployments, there are still potential gaps that security teams often overlook. It is important to be aware of these risk areas and address them before they lead to serious and unexpected breaches. One of those gaps can affect users of thin clients running Microsoft WES.

Simply put, without the proper antimalware solution in place, these devices can increase the risk of malware proliferation if a user on the network forwards a malicious attachment to a colleague using a traditional PC. Even sophisticated IT and security personnel may not be aware of this potential threat, which can proliferate through an organization’s most widely used applications, such as Microsoft Skype for Business and Microsoft Exchange.

In attempting to close this gap, it is important that IT and security teams deploy a solution that not only is effective in solving the problem, but does so in a way that supports the key goals of the VDI deployment, which typically encompass the following:

- Improving endpoint security and compliance by keeping all applications and data in the corporate data center.
- Increasing flexibility in terms of supporting a broad range of users and devices and easily scaling the solution as requirements grow.
- Delivering a great user experience that addresses the specific needs of a broad range of users with different job functions and workload requirements.

This white paper focuses on VDI security in general and specifically on how organizations can leverage new technology innovations to deal with the security challenges inherent to VDI thin clients running Microsoft WES and virtual desktops running a Windows client OS, such as Windows 7, 8 and 10. It also discusses specific solutions from Dell and Citrix that address those challenges directly, resulting in not only improved endpoint security and compliance, but also increased flexibility and a great user experience.

Understanding the WES Thin Client Challenge

Thin clients have become an increasingly popular endpoint solution for VDI because of their inherent security protections and very low power consumption. They significantly reduce risk because applications and data are not stored locally but rather are housed within the “vault” of the corporate data center.

About 40% of commercially available thin clients run Microsoft WES. With WES, users have flexibility to use a local browser, install drivers for external peripherals and run small applications


2
locally. Because of these capabilities, however, WES-based thin clients must install security patches on a regular basis, just like any other endpoint running a Windows OS. In fact, Microsoft releases security patches for WES each month. Without the right protection strategy, these endpoints can be infected by a malicious website, an infected web link or an infected file residing on a USB stick or other attached peripheral device. While no data would be affected on the endpoint itself, there is a risk of proliferation on the network if a user forwards a malicious attachment to a colleague using a traditional PC.

Microsoft Skype for Business provides a real-world example of how this particular threat can proliferate. Skype for Business is one of the most widely used applications in the world. Well more than 50% of enterprise customers use Skype for Business, and it is emerging as an increasingly popular replacement for traditional PBX systems.

In a Citrix XenApp and XenDesktop VDI environment, you can and should store sensitive Skype for Business data in the data center to ensure files, contacts, chat logs and more stay safe within the corporate vault, using a solution such as Skype for Business on XenApp from Citrix. But if users are using local cameras or other peripherals such as a USB stick, or if they are using Skype for Business to share files—after all, it is a collaboration platform—they could put your organization at risk.

Another potential concern centers on performance, particularly with Skype for Business. When voice and video traffic has to travel significant distances between the data center and the user, performance can be impacted by something commonly known as the trombone effect. This issue can be easily resolved with the Citrix HDX RealTime Optimization Pack, which provides an optimized architecture for clear, crisp audio and video calls.

An Innovative Approach to Thin Client Security

How do you mitigate risk from WES thin-client endpoints? A traditional best practice is to install an antivirus/antimalware (AV/AM) solution on a WES-based thin client. In fact, some organizations require that an AV/AM solution be installed on all endpoints, including thin clients. However, a traditional signature-based AV solution is impractical for VDI environments.

On a thin client, a traditional AV/AM solution has a negative impact on the user experience, slowing the system to a crawl when a virus scan takes place. This limits its effectiveness: Traditional AV solutions in this environment stop an average of only 50% of threats, based on data from internal testing by Dell.* They also leave users dissatisfied. As a result, most companies don’t use a traditional AV/AM solution on their thin clients.

The key to protecting these thin clients is to use an advanced threat prevention methodology that can detect malware—even unknown malware—before it can run. Dell is the only vendor that has developed this technology, released as the Dell Data Protection | Threat Defense solution.

Threat Defense is based on dynamic mathematical modeling and artificial intelligence. The algorithm was trained by analyzing tens of thousands of file attributes for millions of known real-world good and bad files. Any new file is assessed and immediately classified as

---

* "Skype for Business Adoption Trends 2016." No Jitter, May 19, 2016
good, suspicious or bad. If it is identified as malware, the file is not allowed to run. Dell’s internal testing has shown that Threat Defense prevents 99% of executable malware, far above the 50% on average of threats identified by top antivirus solutions.* It will also identify and stop zero-day attacks.

Another important benefit of Threat Defense is that it does not depend on signatures or known patterns to recognize a threat, and does not depend on human intervention or frequent signature updates. It uses an agent, installed on the endpoint or virtual machine, that consumes only 1% to 3% of the CPU and less than 40 MB of RAM. Therefore, it has virtually no impact on system performance or the user experience.

A Broader VDI Security Strategy

Dell’s Threat Defense is part of a complete, end-to-end set of security solutions designed to protect VDI environments in conjunction with solutions from the company’s key strategic partners, Citrix and Microsoft. The combination of products from Dell, Citrix and Microsoft enables organizations to deploy a comprehensive security VDI security strategy all the way from the edge to the data center. Products include:

- **Dell Data Protection | Threat Defense**: Threat defense should be part of an overall strategy and solution set designed to provide maximum advanced threat protection for WES thin clients in particular and other endpoints in general, including Mac OS and Windows Server systems. It should be noted that in planning a strategy, IT teams also have the option of using thin clients running Dell Wyse ThinOS, which don’t need any form of antivirus software because they have no published APIs and offer zero attack surface. Therefore, thin clients running Wyse ThinOS are the intrinsically most secure endpoints that can be used in VDI environments.

- **Dell Data Protection | Endpoint Security Suite Enterprise (ESSE)**: This can be used to protect persistent virtual desktops running Windows as well as all VDI endpoints. In addition to offering antivirus protection, ESSE is available with features such as data encryption, authentication and centralized management.

- **Citrix XenApp and XenDesktop**: Citrix has been at the forefront of desktop virtualization from its inception and has developed many of the technologies and innovations that have defined best practices in desktop virtualization security. These include application virtualization; centralization of functions such as patches, hotfixes, and application and configuration updates; two-factor authentication; containerization for mobile applications; network and host segmentation; and many others.

- **Application virtualization**: With Citrix, organizations can leverage both desktop virtualization and application virtualization through a complete solution that provides centralized control and management, flexible delivery schedules, granular policy-based access control, endpoint protection and compliance support. The core of the solution is Citrix XenApp for app virtualization and Citrix XenDesktop, which integrates the full power of XenApp for on-demand delivery of virtual Windows apps and desktops complemented
by application delivery control, secure access control and client-side virtualization and encryption.

Conclusion

Security is one of the main reasons organizations are turning to desktop virtualization. The ability to keep all applications, data and desktops under lock and key in the corporate vault is an inherent advantage of VDI environments. But that doesn’t mean there aren’t risks, and those risks must be addressed through an overall VDI security strategy that extends all the way from the edge to the data center.

As part of that end-to-end security strategy, IT and security professionals must be aware of areas where there may be hidden gaps, such as thin clients running Microsoft WES or Windows virtual desktops. New solutions may be necessary to close these gaps. One such solution is Dell Data Protection | Threat Defense. When used as part of an end-to-end security strategy incorporating solutions from Dell, Citrix and Microsoft, Threat Defense can significantly reduce the threats of attacks from all clients, including thin clients using the Microsoft WES operating system.

The combination of Dell, Citrix and Microsoft not only closes such gaps, but is best positioned to enable IT teams to address all potential VDI security challenges, without compromising flexibility or diminishing the user experience.

For more information on how your organization can close your VDI security gaps, please visit Dell at Dell.com/wyse/shield.

* Based on Dell internal testing, November 2016