Make your VDI environment more secure

Dell is taking the already-secure desktop virtualization solution one step ahead.

While virtual desktops are inherently more secure than traditional desktops, there are still a number of security considerations to discuss when selecting the ideal solution.

Desktop virtualization security is often overlooked or implemented only as an afterthought. However, the current threat landscape and regular cadence of headlines announcing data incursions require IT professionals to consider baking additional security into VDI solutions from the outset.

Even with architectures that combine the limited attack surface of thin and zero client endpoints and data kept in the data center, it is important to consider the near-constant threat of intrusion and review the necessary steps to safeguarding the enterprise data.

Recent Security Headlines

Inherently insecure might be the most effective way to describe the modern Internet. While IT managers install firewalls, packet-sniffers, and legacy anti-virus (AV) solutions, concern remains that unforeseen vulnerabilities still linger. Can anyone ever be certain?

- In August, a new attack vector was discovered that jumps from spam into Microsoft Word, changing users' browser proxy server settings and capturing authentication credentials or other sensitive information.[1]
- More than 718,500 users were hit with encryption ransomware between April 2015 and March 2016, an increase of 550 percent compared to the same period in 2014-2015.[2]
- Researchers from the security vendor McAfee Labs Threat Report tracked a ransomware network that had received an estimated $94 million in bitcoin payments during the first half of 2016.[3]
- IBM and Ponemon Institute's 2016 Cost of Data Breach Study found that the average cost of a data breach for the 383 companies participating increased from $3.79 million to $4 million during 2015.
- So-called "CEO email scams" where criminals pose as senior executives and persuade finance managers to transfer huge sums to temporary bank accounts, have hit tens of thousands of companies and cost more than $3 billion since January 2015.[4]
- Several public figures had their email accounts breached in 2016, perhaps because they had not yet implemented dual-factor authentication or because their home email accounts were otherwise insecure.

1. *Computing,* "Microsoft Warning Over Malware That Exploits Security Holes In Word," by Dave Neal, August 31, 2016
2. *ZD Net,* "Why Ransomware Is Exploding," by Alison DeNisco, September 1, 2016
3. *ZD Net,* "Ransomware Network Chalked Up $121 Million In 1H2016," by Eileen Yu, September 16, 2016
4. *ZD Net,* "Cybercrime and Cyberwar: A Spotter's Guide," by Steve Ranger, September 1, 2016

Facilitating this approach requires re-examining the vulnerabilities of a VDI environment, even if they may only show up in an edge case. An obvious first step is to enhance VDI security by adding AV applications to the gold image running in the data center. However, this can significantly degrade CPU performance during simultaneous, solution-wide disk scans often described as an anti-virus or anti-malware (AV/AM) storm.

The other limitation to this approach is that most AV/AM software relies on virus definition or "signature" files which must be updated regularly to stay effective. With new viruses constantly emerging, traditional scans that leverage signature databases can leave networks vulnerable to so-called "zero day attacks." Finally, AV/AM solutions themselves can have inconsistent strengths and weaknesses that result in variable functionality and effectiveness.

Ideally, an end-to-end desktop virtualization solution should maintain the same level of security across all access points, including its endpoints. This would mean that all enterprise and customer owned laptops, tablets, desktops, thin clients and smartphones that access the network would have the same level of AV/AM protection, mobile device management software, and two-factor authentication.

However, some deployments can essentially be characterized as half-measures. IT managers must consider how the virtual desktop or OS image was created

and what security tools were implemented in the creation of the master image. The inclusion of browsers within the "master" or gold image, while seen as a necessity, can increase the vulnerability to malware.

Dell Data Protection | Endpoint Security Suite Enterprise (ESSE), is Dell's end-to-end security solution for virtual desktops and physical PCs. This suite includes data-centric encryption, user authentication, and Advanced Threat Protection (ATP), a branded Dell offering. ATP is able to prevent 99% of malware, far above the average 50% of threats identified by the top anti-virus solutions.*

Because ATP leverages proprietary algorithms and artificial intelligence, it does not require frequent updates or a constant Internet connection. Additionally, the suite avoids the heavy CPU overhead of traditional

AV/AM software and is effective against zero-day threats. Finally, Endpoint Security Suite Enterprise can provide data security for mixed environments that include traditional PCs as well as on virtual machines that reside in the data center.

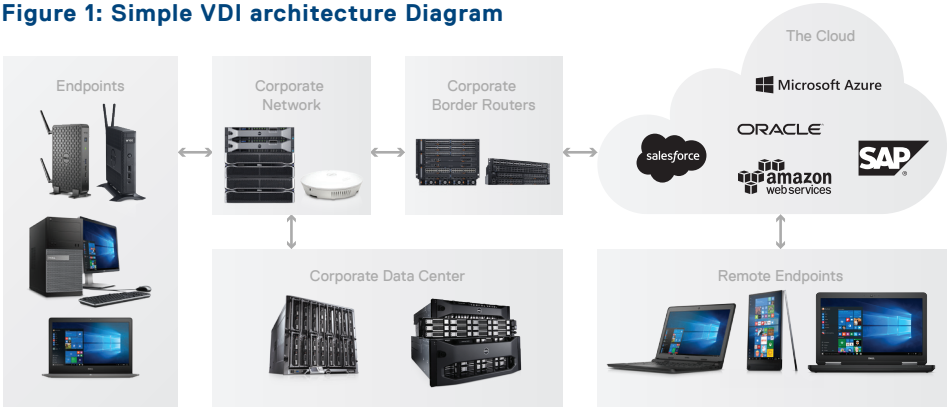
* Results from Cylance Unbelievable Demo Tour, Austin, Dallas and Houston, Texas, May 2015. Also Based on Dell internal testing, November 2016.

Desktop Virtualization Security Threats

The major elements of a Desktop Virtualization solution are shown in Figure 1. Dell balanced and purpose-built components provide a single-vendor, end-to-end solution including data center components, endpoints, leading virtualization software, services, and security software. Public cloud options are included because many companies are moving their virtual desktop infrastructure to cloud services like Amazon Web Services (AWS) and Microsoft Azure.

To maintain a sensible security posture, the same protection applied to the virtual machines in a company's secure data center should also be applied to those hosted in the cloud. Similarly, a deployment of unprotected, remote endpoints may be vulnerable if they are located outside of your secured network without firewall protection. For that reason, it is important to maintain firewalls at the edge and within the network to isolate sensitive data and make sure that virtual desktop environments are only accessed over secure connections.

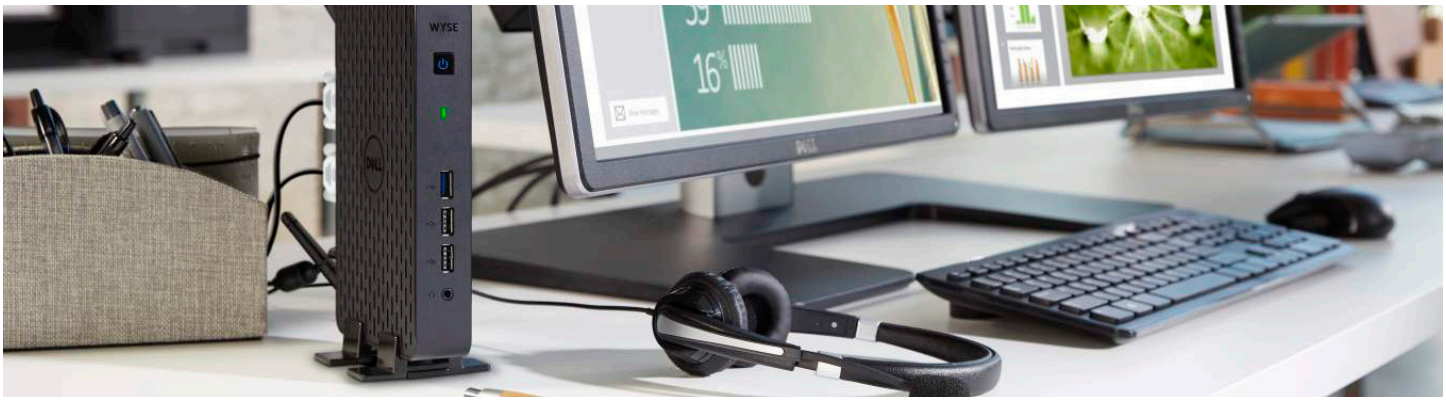
Figure 1: Simple VDI architecture Diagram



Categories of Malware

Attacks and threats whether physical or virtual, generally fall into six categories:

- **Adware:** Applications which surreptitiously track a user's path online and provide data to third parties for the purposes of delivering targeted ad messages. These applications produce unwanted pop-ups but most troublingly, they open a pathway for malware to gain control of the endpoint.
- **Bot:** Short for robot, an application that gets installed in the system to link the endpoint to a broader attack on a third-party network or website. "Bots" which often collect data including keystrokes and user responses to data fields can pass sensitive data along to software pirates, credit card thieves, or other bad actors.
- **Bug:** Software error that alters the normal operation of the OS or applications, thereby creating a vulnerability.
- **Ransomware:** Malicious application which overrides system files, encrypts user data, and requires a user to pay an exorbitant fee to avoid having the files deleted.
- **Spyware:** Malicious applications which monitor and collect user data such as keystrokes, browser history, passwords, or other sensitive information.
- **Rootkit:** Applications which install malware into the operating system – or even into the BIOS – making the endpoint vulnerable. This type of malware is difficult to identify, can be overlooked by traditional anti-virus software – and may act as a platform or gateway to installing additional malware.



Anatomy of a potential attack

Figure 2 outlines the steps of a theoretical Web-based attack. In this particular case, the user is accessing the Web but not accessing any data-sensitive information during the attack. However, since many applications cache data, the building blocks of malware may be present in memory or residing in a temporary file stored on local media.

Traditional security vendor's approach and gaps

In general, the older and less streamlined the client OS, the larger the attack surface. Outdated, legacy operating systems are particularly vulnerable. As a result, the largest potential target of course, is a Web-connected traditional PC running a locally-installed, unsupported version of Windows.

While that configuration represents the least-secure option, thin clients are able to increase security by reducing the attack surface. This is because thin clients are typically built around an embedded OS with limited or reduced functions or because they access their operating systems from locked "gold images" stored in a centralized data center.

Thin clients typically use a slimmed down, onboard OS such as Windows Embedded or Linux and create virtual drives in local memory to cache temporary files. Even so, the risk is that some thin clients with a browser can connect to the Internet and download or access applications containing malware or viruses.

Figure 2: Ten Steps of a potential web based security attack

1. The user starts out accessing a normal webpage.
2. The content of the page is downloaded into the local memory. The webpage contains a link which looks like the content the user is looking for.
3. The user selects that link and does not realize that link is directed to another website containing malware.
4. This website serves the malware onto the local computer.
5. Because the malware in this example is looking to gain access to the user's banking records. It starts a scanning process.
6. The malware then scans other sections of memory looking for webpages which might be the user's bank website.
7. The malware also installs a keylogger which will eventually capture ID and password information.
8. Once potential data is collected, it is transferred back to the malware control site.
9. A software robot tries the various combinations to gain access to the user's bank website using the stolen information.
10. Once a successful connection is established, the software bot transfers the user's money to a bank account in another country where the funds are quickly withdrawn.

The most secure and efficient thin client OS is Dell Wyse ThinOS, which is custom-tailored for Dell thin client environments and built with embedded security features, performance optimization, and a low memory footprint.

Because the System Master template presents an additional vulnerability, it is important to load anti-virus software prior to production and ahead of applications that may launch after the image is created. Without proper screening, malware may also be present on applications or documents launching from a USB drive or downloaded from infected sites. Once in place, they may remain dormant in the master system, and only show up after that template has been distributed to users.

Traditional anti-virus and malware protection often concentrates on scanning the file system to identify unapproved applications or improper file extensions. These packages can also check the contents of data during I/O and validate it before proceeding with the appropriate action.

Document files found to be infected are generally quarantined and in some cases can be retrieved. The inherent shortcoming however is that these applications rely on signatures which need to be regularly updated. The other issue is that traditional virus scans can impose significant system load while files are being scanned against the database of definitions.

Zero clients are the most secure by design since they usually do not have system files and maintain a small addressable footprint. Further, they typically run on proprietary operating systems such as Wyse ThinOS and their APIs are generally not publicly available for virus-writers to exploit.

Further, the inability to run user level programs on zero clients makes them less of a target for hackers. Even so, this does not mean they are completely immune to attacks. It is important to make sure endpoints cannot be compromised by users booting from a USB key or other external device.

Dell's added value

Very few VDI solution providers have designed a complete end-to-end data security solution. As a result, some customers are left to consider cobbling together solution elements from disparate vendors. These piecemeal solutions provide little to no integration, nor are they particularly effective in identifying potential vulnerabilities or threats. Dell, however, has created an advanced security solution optimized for virtual desktop environments and thin clients.

Dell Data Protection | Endpoint Security Suite Enterprise protects virtual desktops as well as traditional physical PCs from advanced threats and commodity malware. The suite contains advanced threat protection, data-centric encryption, and hardened authentication.

Its management console makes it easy for IT admins to manage physical PC and VM security and to create compliance reports, all from a single pane of glass.

Dell Data Protection | Threat Defense protects thin clients running Windows® Embedded Standard™ (WES) or Win10 IoT Enterprise, as well as physical desktops, Mac OSX systems, and Windows servers from advanced threats and malware. Threat Defense uses a cloud-based management console to provide simplified management.

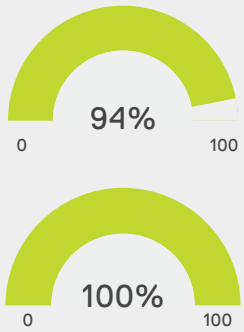
Securing the Data Center

A virtual machine running from a PC image in the data center has many of the vulnerabilities of a traditional desktop and needs to be protected accordingly. For this reason, cloud-based solutions are only as strong as the weakest link connecting users to the network. Common threats to consider include:

- **Zero-day attacks.** Much like endpoints, browsers within a VDI environment can be vulnerable. Increasingly, executables launched by an unsuspecting user's mouse click can trigger network breaches.
- **USB drives and portable storage vulnerabilities.** Network data is at risk of being copied by end users using unapproved/infected USB drives and other portable storage devices. IT departments can eliminate this potential problem by disabling all external transfer capabilities and thereby limiting the use of external storage, including from thin and zero client endpoints.
- **Personal cloud storage accounts.** These are a common way that users store data between work and home. However, these accounts can put data at risk of being intercepted either by unauthorized access or so-called "man-in-the-middle" attacks. Because this data is typically not encrypted and can potentially be intercepted on the download side at home – say through an insecure wifi connection – or by viruses or malware on a user's home PC, enterprise data can be put at risk.

Given today's persistent threat environment, the best approach is to take what might feel like an extra step and encrypt user data using a sophisticated enterprise security solution. Dell Data Protection – Endpoint Security Suite Enterprise (ESSE) and Advanced Threat Protection can accomplish that, offering protection against viruses, malware or zero day threats on virtual machines.

Threat Protection



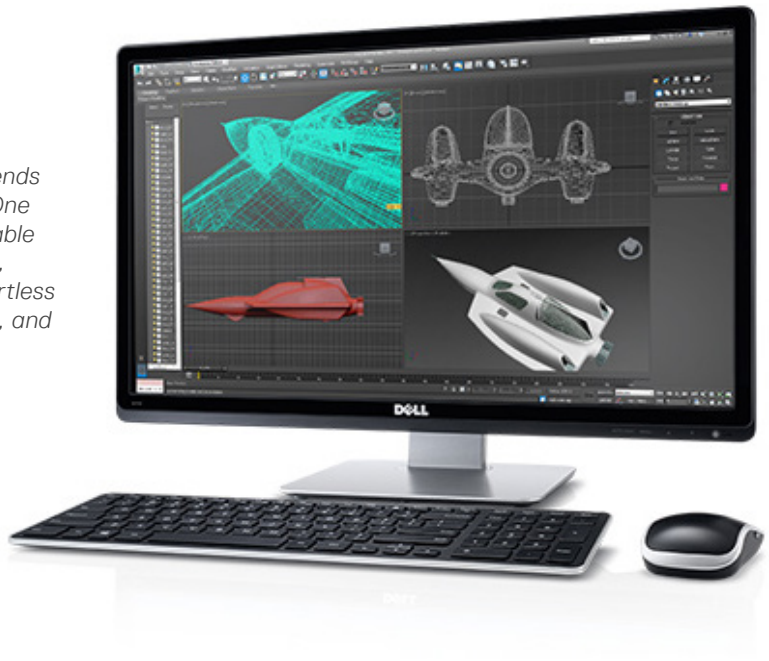
Malware protection is displayed graphically on a Threat Defense management console (i.e. protection is running against 94% of known threats on 100% of your users' registered devices.)

Dell Data Protection | Endpoint Security Suite Enterprise (ESSE) is a full suite containing three features: Advanced Threat Protection, Encryption, and Authentication. Your IT department can use ESSE to protect virtual desktops running from the data center as well as physical PCs (Dell and non-Dell, also Macs), but not thin clients.

Threat Defense comes only with the Advanced Threat Protection feature (without Authentication and without Encryption). Your IT department can use Threat Defense to protect thin clients running WES7/7p or Win10 IoT Enterprise, physical PCs and Mac OSX systems, but not on virtual desktops.

The suite, which is managed by a single console allowing IT administrators to set policies or remediate issues, stops threats within milliseconds before they can cause problems. It does this by leveraging mathematical models and artificial intelligence, looking for sudden changes in steady state, rather than by comparing files with virus definition lists.

Better still, ATP has minimal impact on CPU (1-3%) and RAM and does not degrade performance or user density in VDI architectures. Finally, the ESSE suite also includes data encryption which protects both local drives and external media.



Dell recommends Wyse All-in-One models for cable management, security, effortless management, and scalability.

Conclusion

Data is increasingly under threat. As a result, IT professionals are recognizing that virtual desktop architectures that keep data within a data center and only send pixels to users' endpoints have many benefits including streamlining backups and disaster recovery while maintaining high-availability. However, while desktop virtualization architectures are among safest platforms for securing data in enterprise environments, some vulnerabilities still remain.

Viruses and other malware can still compromise your network if users click on infected links or visit the wrong Websites. Even though virtual machines reside safely in the data center where they are easier to safeguard and back up, they can still become infected.

Generally, virtualization environments have at least two areas of vulnerability: weak endpoints or unprotected virtual machines in the data center. As a result, virtual desktops can become compromised and cause problems, at least until the next anti-virus scan or hard restart in the case of non-persistent desktops.

During each user session, a VM can be vulnerable to being breached via the browser, by compromised passwords, or by other user-facilitated missteps.

Given that Dell is a proven leader in virtual desktop solutions as well as thin and zero client endpoints, we offer a number of additional elements from endpoint to data center protection that can limit the exposure of virtual desktops.

Fortunately, Dell is an industry leader in designing secure virtual desktop solutions and enterprise-grade security options that protect data wherever it resides. Data can be better-protected at the edge by deploying Wyse thin or zero client endpoints which have a limited attack surface and the ability to manage USB ports that might otherwise be used to transfer data to mobile storage.

Because virtual machines can be exposed, Dell offers End Point Security Suite Enterprise which includes Advanced Treat Protection (anti-virus) and Data Encryption. In this way, Dell's security-conscious solutions and Wyse endpoints can help your IT department keep enterprise data safe while it is in the data center or in flight and make sure your users can stay productive.

Related Web Sites:

Dell.com/DataSecurity

Dell.com/Wyse/Shield

Securing the Endpoints

To proactively and specifically protect WES-based thin clients against today's advanced threats and commodity malware, Dell offers advanced threat prevention, with Dell Data Protection | Threat Defense.

Advanced Threat Protection: a revolutionary, preventive approach providing proactive protection by catching 99% of advanced threats, commodity malware and ransomware before they can execute. It uses dynamic mathematical models and artificial intelligence and is able to catch even zero-day attacks. The client runs locally on the physical or virtual desktop with very low CPU and memory usage, thus there is no impact on end user productivity and no need for constant internet connectivity or signature updates.

Encryption: Data-centric encryption protects sensitive data via set-and-forget policies to simplify protection for any sized organization. Dell provides maximum data security by encrypting data, local drives and external media. It is FIPS 140-2 Level 2 validated and also offers Microsoft BitLocker and self-encrypted drive (for physical PCs only.).

Authentication: with physical PCs, the suite enables advanced hardware authentication, such as Dell's fingerprint, smart card or contactless smart card readers. It also supports pre-boot authentication for self-encrypting drives, single sign-on (SSO) and offers additional security for user credentials via Dell ControlVault™. It is also possible to reset a Windows password via an authorized smartphone, minimizing one of the most common reasons for help desk calls.

Centrally managed console: Endpoint Security Suite Enterprise offers a single pane of glass view into all your protected endpoints with an on-premise management console. Detailed compliance reporting is included to greatly simplify security management and compliance.

For more information visit:

Dell.com/DataSecurity

Dell.com/Wyse/Shield

Kenneth Coley,
Principal Engineer
kenneth_coley@dell.com

Rafael Colorado, Product Management Director
rafael_colorado@dell.com