Protecting Content and Securing the Organization Through Smarter Endpoint Choices

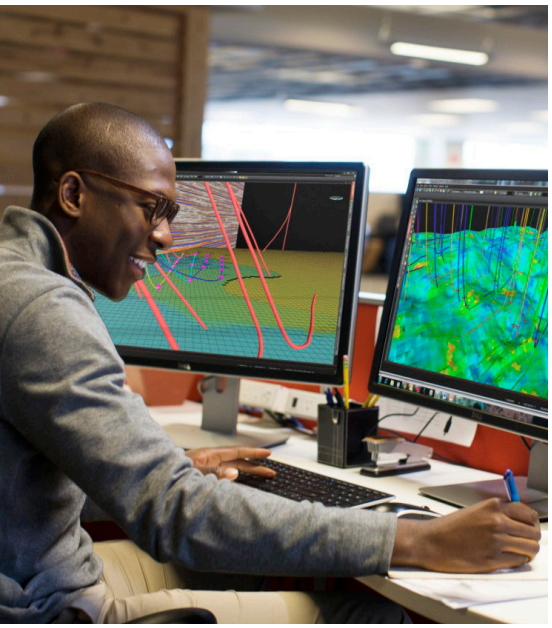
Prepared by Dan O'Farrell—Dell Cloud Client-Computing

Finally – a practical approach to protecting content and securing desktops

Organizations of all sizes face a continual challenge to protect corporate-owned content while still providing their people the tools and freedom to be at their most productive. Driven by the growth in big data, an expanding mix of applications including multimedia and increasing user mobility over a broader range of endpoints, many organizations are moving to desktop virtualization to regain the upper hand in securing content and managing access to applications.

With desktop virtualization, applications and data are moved from individual physical desktop systems into a central datacenter. By centralizing apps and data in a managed datacenter where disaster recovery and automatic backup processes already exist, the tasks of truly securing data and managing application access can become much more achievable. And the recent trends of bring your own device (BYOD), telecommuting and worker mobility continue to escalate, making content protection and desktop security more critical than ever. Desktop infrastructure is especially vulnerable. Human error, email attacks, network-borne viruses and malware, infected websites and downloads put data at risk every day – potentially on every user desktop.

Virtual desktop infrastructure (VDI) is less vulnerable because data resides in a secure datacenter rather than on endpoint devices, with strict security and access policies easily applied and managed from a central location. Compliance with government or industry-mandated regulations is also much easier with VDI, because IT maintains complete visibility and control over network and file access, data storage and system maintenance.



Solving the data and access protection puzzle with Dell cloud client-computing

Wyse thin and zero clients from Dell are ideal for any virtualized or web-based infrastructure in environments that require high security and reliability. With Dell cloud client-computing, IT staff can customize policies to define the performance, security and functionality profile of a virtual desktop for any user, from mobile workers to power users to support staff, and adapt to various business initiatives, including off-shoring, mergers and acquisitions, and branch expansion.

With an open, scalable and proven architecture, Dell simplifies management, support and integration, while providing a completely secure, reliable computing platform that meets even the most rigorous security and compliance requirements.

Solution at a glance

Dell cloud client-computing approaches the security challenge in three distinct areas:

1. A broad portfolio of software, hardware, and services to allow organizations to easily and effectively adopt desktop virtualization and enable users to access key apps and content in the secure, highly reliable datacenter.
2. Management applications that enable simple yet highly powerful user/device policy setting and enforcement to protect who, how, where, and when applications and content are accessed.
3. Wyse thin and zero clients that function as stateless, diskless user endpoints. Wyse zero clients and ThinOS-based thin clients offer zero attack surface, thus rendering them immune from virus and malware attacks.

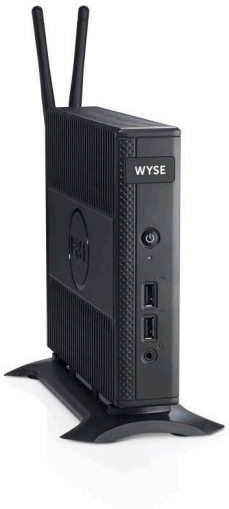
Common endpoint security pain points

- Difficulty maintaining consistent, compliant endpoint OS and application images across hundreds or many thousands of desktops
- Ensuring appropriate access rights to applications based on user profiles (function, department, location, etc.)
- Endpoint vulnerability due to malware, viruses, theft and hardware failure
- Difficulty of securing hundreds or thousands of PCs with the most recent patches and updates to consistently meet compliance requirements
- Proliferation of tablets, smartphones and laptops introduced to the network as a result of workplace trends such as telecommuting, temporary workers and BYOD
- Time and effort required to add single sign-on or second-order strong user authentication to individual PCs in highly secure locations

How Dell cloud client-computing addresses these endpoint pain points

- Wyse Device Manager (WDM) software centralizes desktop image management for complete visibility and control over end user device access and use, regardless of the access device or location
- WDM enables rapid, cost-effective and consistent updates and patches to ensure device security and software image and application consistency
- Wyse Configuration Manager (WCM) software makes it easy to configure Windows Embedded thin clients, and replicate those configurations across the network with the ease of a file drag-and-drop, thus eliminating human error
- WCM allows IT personnel to “lock down” any Windows Embedded thin client into a single-purpose endpoint such as a kiosk for example, and nothing else

- Wyse Cloud Client Manager software enables policy setting and enforcement of application access rules based on user, device, location, and access method across a broad range of iOS and Android tablets and smartphones, as well as Wyse thin clients, as a cloud-based service
- These management software platforms simplify policy administration for consistent compliance with various industry and governmental regulations
- Wyse thin and zero clients enable enhanced security at the network edge by integrating with a variety of single sign-on, strong authentication devices for enhanced security when necessary
- Dell cloud client-computing significantly reduces the threat of data loss through malware, viruses, or theft of hardware failure, because all data and applications are stored in the secure datacenter - where it belongs



The benefits

Highly resistant to attack – unlike traditional desktops

Dell removes the security vulnerabilities and maintenance issues associated with traditional desktops. With no local hard drive, all data and applications are stored safely in a secure datacenter, reducing the risk of data loss, theft or tampering.

Wyse ThinOS - the virus-immune thin client operating system designed to protect your endpoints

As the only thin client operating system developed solely to offer complete thin client security with automatic management and extreme ease-of-use, Wyse ThinOS stands alone as the thin client operating system of choice for organizations looking to eliminate endpoint security concerns for good.

With no published API or user accessible file system, Wyse ThinOS lacks the vulnerabilities and excess overheads of traditional general purpose operating systems. Its "zero attack surface" means IT teams can finally get out of the constant challenge of maintaining anti-virus signatures on endpoints. That equates to enormous amounts of time saved while a huge endpoint security concern burden can finally be eliminated.

Since Wyse thin and zero clients are managed centrally, administrators can define and enforce security policies and procedures consistently across the organization.

Secure your desktops without breaking the bank

With Wyse thin and zero clients from Dell, the time and cost of securing traditional desktops is practically eliminated, because the data and applications are stored and managed in the datacenter. The normally tedious task of ensuring consistent OS images and applications by user type across the enterprise becomes as simple as a file drag-and-drop on the server. Remote management reduces travel associated with equipment maintenance and system enhancements in remote locations and branch offices, saving money and freeing up IT staff to focus on other projects and initiatives.

BYOD, mobile and remote access, minus the worry

With Dell cloud client-computing, IT staff can maintain full control over any device accessing network resources. This gives employees, partners and visitors the freedom to bring their own devices to work without fear of compromising security or intellectual property policies. Dell's cloud-based Cloud Client Manager service allows organizations to inventory, set and enforce usage policies, and locate mobile device assets based on user or group-based policies. Lost or stolen devices can even be "wiped clean" of all corporate-owned content in an instant.

Security and more

In addition to creating a highly secure environment, Dell cloud client-computing offers many advantages over traditional desktop computing, including:

- **Increased business agility:** Virtual desktops are rapidly deployable and easily maintained and updated
- **Data recovery:** Because of redundancy and disaster recovery procedures in the secure datacenter, the risk of data loss as a result of security breaches, natural disasters, or failed hardware is significantly reduced
- **Improved business continuity:** A more secure desktop with easy, consistent desktop image updates means fewer security breaches, which can be costly and result in network disruption and downtime
- **High availability:** Because they're centrally stored and managed, applications can be delivered – and updated – on demand
- **Lower TCO:** Wyse thin and zero clients have lower capital and operational costs than traditional PCs, because they are extremely simple to deploy and manage, require minimal maintenance, consume roughly 90% less energy, and have a lifespan that is twice as long as PCs

Protecting vital content and securing user/device access has never been more challenging. The continued growth in how people access apps and content, the devices they use to do so, and the trend in matching work-style to lifestyle all contribute to the complexity. This is where Dell cloud client-computing and desktop virtualization can help immensely. Dell can offer guidance on how to best move to virtual desktops, and with the broadest selection of products and services, we can help you ensure that your apps and content are secure and accessed only by those who should be accessing them, and only in the right way.

Dell cloud client-computing – enabling any user to access any app from any device – securely.

About Dell

Dell Inc. listens to customers and delivers innovative technology and services that give them the power to do more. For more information, visit www.dell.com.

Dell cloud client-computing

One Dell Way
Round Rock, TX 78664
www.dell.com/wyse

Refer to our website for regional and international office information.