Ultimate Flexibility: Trusted Endpoints for Secure Remote Access

CITRIX Ready

DLS® | CITRIX®

The workforce is becoming increasingly mobile, with more employees working remotely than at any time in history. Advances in technology have enabled remote access capabilities that permit work and workers to escape the physical bounds of an office. It is a technological leap that offers great opportunities and conveniences for employees and employers alike. Likewise, the potential benefits of bring-your-own-device (BYOD) programs offer new opportunities both employees and employers, including enhanced productivity, lowered costs and greater employee satisfaction.

But both mobility and BYOD depend upon one critical component: a trusted endpoint. Without trusted endpoints, mobility and BYOD morph from beneficial technological advancements into stark threats to organizational security. Without trusted endpoints, both mobile devices and unmanaged devices are security breaches waiting to happen.

Most companies have struggled to find a way to assure that endpoints are kept secure. Some have even abandoned the benefits of BYOD because of the difficulty of maintaining secure endpoints. This paper discusses how vKey software on a bootable device provides a plug-and-play, reliable, trusted endpoint — from anywhere on any device. Also described is the ability of vKey to integrate with Citrix products in enabling secure remote access for mobile and BYOD workforces.

Business Challenge Summary

In 2013, Gartner released a report extolling the revolutionary benefits of bring-your-own-device (BYOD) programs. "BYOD strategies are the most radical change to the economics and the culture of client computing in business in decades," the report stated, noting that "The benefits of BYOD include creating new mobile workforce opportunities, increasing employee satisfaction, and reducing or avoiding costs." [1]

Gartner went so far as to predict that half of all employers would require employees to provide their own devices for work-related tasks by 2017.

Fast-forward a few years.

All the potential benefits of BYOD programs happened — slashed operating costs, enhanced productivity, increased employee satisfaction. Yet many companies have decided to forego all those benefits by opting out of BYOD programs. A *Computerworld* article, in fact, reports

[1] http://www.gartner.com/newsroom/id/2466615

that more than half of U.S. companies have enacted all-out bans against BYOD — an ironic juxtaposition to Gartner's earlier forecast. [2]

Why are so many companies depriving themselves of the benefits of BYOD that seemed so promising only a few years ago — and are still available?

The answer is simple: Fear.

Companies that have enacted BYOD programs are confronted by the fact that each user-provided device represents an untrusted endpoint over which the company exerts little control. Essentially, each untrusted endpoint represents great risk to the company, providing a gateway through which malware and viruses may flow in to infect company systems.

Multiply the risk of a single untrusted endpoint by hundreds, thousands or tens of thousands of devices deployed by the workforce of a single company, and the potential risk is staggering — and terrifying.

But the benefits of BYOD are just as real as the risks. Intel, for example, has reported productivity gains in the range of 5 million hours yearly.[3] And a Cisco study has reported that BYOD can enhance the value of mobile employees by as much as $3,150 per employee, per year.[4]

It is obvious that companies stand to gain much from the benefits of BYOD. The clear need is for a remote access solution that can transform each untrusted endpoint — across a wide range of devices — into a trusted endpoint, maximizing the benefits of BYOD while simultaneously enhancing enterprise security. The deployment of a secure, device-independent operating system is the best way to achieve that goal.

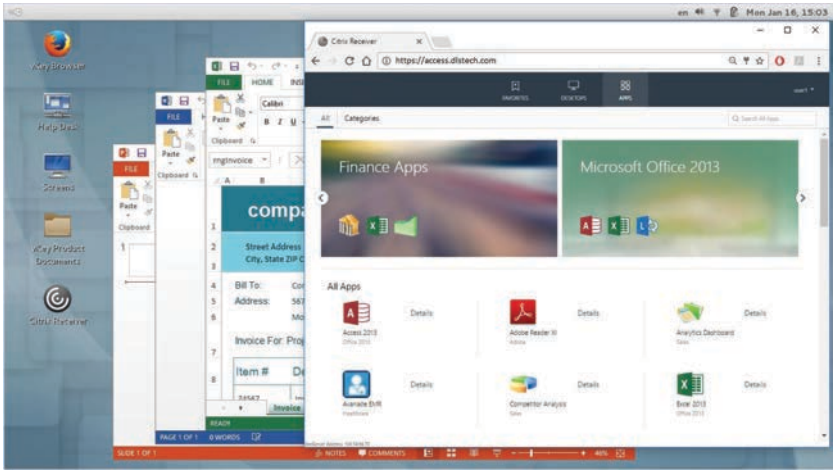
[2] http://www.computerworld.com/article/2948470/byod/the-bring-your-own-device-fad-is-fading.html
[3] http://www.computerworld.com/article/2948470/byod/the-bring-your-own-device-fad-is-fading.html
[4] http://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs

Top Five Features to Consider in a Secure Remote Access Solution

Maximizing the benefits of a secure remote access solution requires the installation of a system that delivers a full range of key capability and usability features, along with security enhancements.

The following, in particular, should be considered must-have features for secure remote access solutions undergoing evaluation for deployment in any organization:

- **Security:** Enabling remote access to enterprise systems and data is not difficult. A plethora of hardware options exist for achieving remote access. But enabling remote access while maintaining or even strengthening organizational security is considerably more difficult. Each device used to remotely connect users with enterprise systems represents a potential threat to enterprise security. A truly secure remote access solution must enable the use of the many hardware devices that make remote access possible, while simultaneously eliminating the risk that those devices present.
- **Flexibility:** The primary purpose of remote access is to enhance productivity. It is a rather strange irony, then, that many remote access solutions present users with very little flexibility in the deployment and use of those solutions. A remote access solution that can offer users a wide range of choices, both in devices and access methodologies, fulfills the true potential of remote access.
- **Asset Life Extension:** Aging laptop and desktop PC assets remain useful well beyond design life when used for secure remote access. Aging assets can efficiently run newer operating systems they wouldn't otherwise be able to use thanks to optimizations in client and desktop virtualization; enabling greater ROI realization.
- **No End User Installation Required:** Relieving users from the chore of performing software installations enhances user acceptance, reduces demand on administrative and helpdesk resources, and speeds the deployment process.
- **BYOD and SRA Support:** A solution that fully supports secure remote access must also support BYOD while maintaining acceptable security standards — especially important in consideration of the reality that BYOD is an integral component of the remote access program for many organizations.



CITRIX® XenDesktop

CITRIX® XenApp

CITRIX® XenMobile

CITRIX® ShareFile

CITRIX® NetScaler

Citrix Ready Secure Remote Access Program Overview

Citrix solutions deliver a complete portfolio of products supporting the secure access of apps and data anytime, at any place, on any device and on any network. These include:

1. XenApp and XenDesktop to manage apps and desktops centrally inside the data center
2. XenMobile to secure mobile applications and devices while providing a great user experience
3. ShareFile to provide controlled and audited data access, storage and sharing, both on-premise and in the cloud
4. NetScaler to contextualize and control connectivity with end-to-end system and user visibility

Citrix solutions also integrate with third-party security products to provide advanced levels of system management and identity, endpoint and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to smoothly integrate with Citrix products, and that work to enhance Secure Remote Access by adding extra layers of security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, DDoS and other security attacks that may be perpetuated via Remote Access.

Citrix advises that organizations can best defend against security attacks that might occur through Remote Access by following five best practices — pillars of focus that support enterprise security:

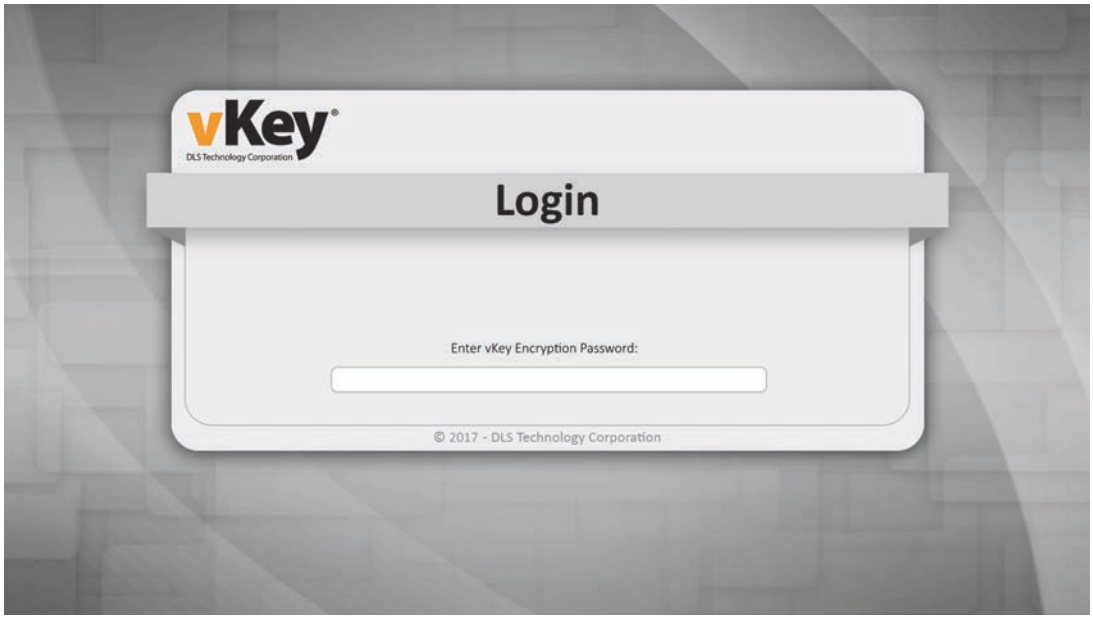
1. **Identity and Access**: Administrators must be able to confirm the identity of users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, two-factor authentication offers a vast improvement in the ability to properly confirm user identity in requests for access. The degree of access granted to each individual user should be based on context. The principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs.
2. **Network Security:** The growing demand for remote access complicates the process of securing a network. Yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multi-layer approach helps to boost network security while ensuring availability.
3. **Application Security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created many additional points of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams can help to reduce app-related security vulnerabilities.

4. **Data Security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data by enforcing secure file sharing (to reduce data loss) and by the containerization of data (both in-transit and at rest).
5. **Monitoring and Response:** Vigilance and fast action are required to successfully counter the attacks that most enterprises face on a daily basis. A rapid response to breaches is also critically important, given that even the most secure systems are not completely invulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and help to limit susceptibility to imminent additional attacks. End-to-end visibility into application traffic supports faster identification of security breaches and system anomalies.

The Benefits and Burdens of Remote Access

Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word "workplace" must be redefined to be less location-specific and more worker-specific. The adoption of mobility enhancing tools such as tablets, smartphones, thin clients, and other devices has transformed many enterprise roles into an anyplace, anytime proposition. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps of productivity that remote access enables.

But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of virtual public networks (VPNs) over unsecured networks, for example.



While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justifies the need for an increased focus upon security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above while meeting the skyrocketing demand for more remote access capabilities.

DLS has been selected to participate in the Citrix Ready Secure Remote Access program. DLS's vKey unique independent operating system has demonstrated the ability to consistently conform with and support the five security pillars of the Secure Remote Access program. Unlike any other remote access solution, vKey enables remote access through virtually any type of device using Intel or AMD processors.

Overview of DLS and vKey

Founded in 2000, DLS Technology Corporation (DLS) is an IT system integration service and product development company based in Ottawa, Canada. Over the last 16 years in the industry, DLS has become a value-adding technology solutions and service company that fulfills market needs for large enterprises, public sector clients and SMBs. DLS focuses on secure virtualization and integration with the end-to-end design, deployment, and support for: secure remote access, mobility, BYOD, cloud computing, endpoint protection and business continuity.

DLS' flagship endpoint protection product, vKey, is a software-based solution stored on a portable media that can be booted from any computer to create a secure and independent Linux and/or Microsoft operating system (OS) environment. vKey's bootable OS runs independently from the hard disk of the hosting computer in a zero-footprint environment. Almost any modern Intel or AMD-based computer (PC or Mac) can be used as the host computer. With vKey, users can access their organization's network, applications and data from any host computer without changing how they work, and without compromising corporate network security.

vKey is the ideal endpoint protection solution for:

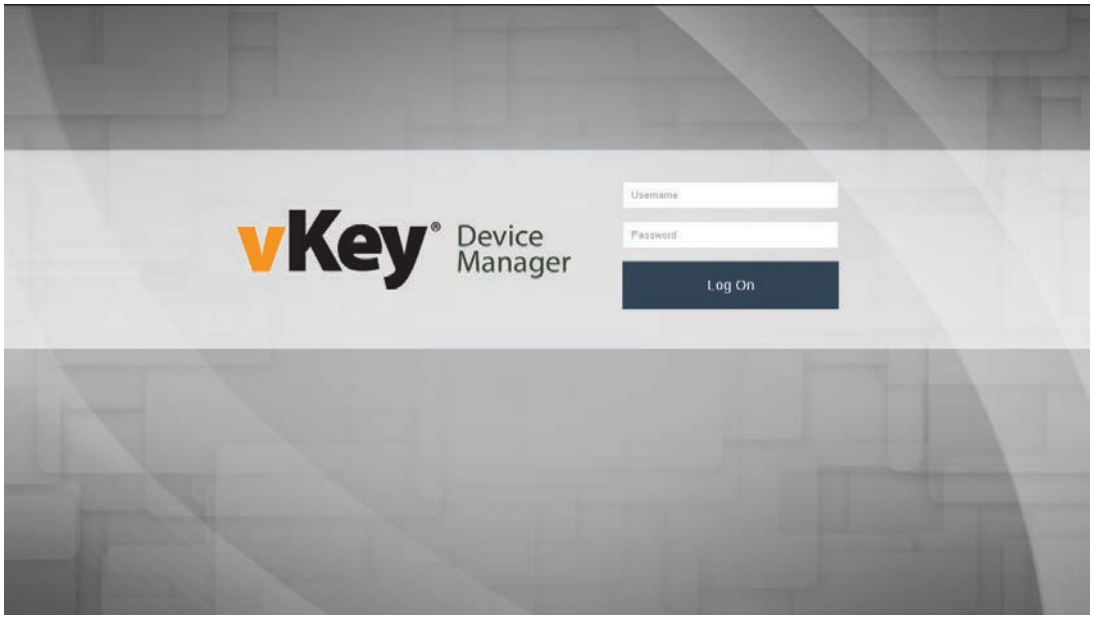
- **Protecting** sensitive security environments
- **Evading** malware
- **Supporting** remote/mobile workers
- **Providing** whitelisting devices
- **Accommodating** contractors requiring temporary access
- **Working** from home or any other remote locations
- **Enjoying** improved performance from aging systems
- **Testing** new systems

vKey takes a unique approach to endpoint protection. vKey is software that can reside on a variety of highly portable forms of bootable media devices, such as USB sticks, BlackBerry devices, micro SD cards, or external hard disks. Users simply plug a device containing vKey into the computer they wish to use and power-on the computer. vKey's operating system boots up and takes control of the host computer for connecting to the desired system.

But unlike other remote security solutions, vKey does not interact in any way with the hosting computer's hard drive. Instead, vKey uses other components of the host computer while substituting vKey's virtual operating system for the host computer's operating system.

Bypassing the hard drive of the host computer assures absolute endpoint security. Even host computers that are known to be infested with multiple forms of malware can be safely used as endpoints, since the "brain" of the computer, in which the malware resides, is never activated. This unique approach to endpoint security also eliminates concerns about whether a host computer is up-to-date with the most recent operating system releases, making an older, out-of-date computer perfectly suitable for use as a vKey host computer.

If a bootable device loaded with vKey is lost or stolen, there is no cause for concern; vKey is encrypted to AES-256 standards, an encryption algorithm recommended by the U.S. National Security Agency.[5] It would take cybercriminals decades to crack the encryption of a stolen vKey.



Ultimate security is assured through vKey Device Manager (vDM). vDM enables complete control over every single vKey deployed throughout an organization. vDM typically resides in an organization's network DMZ, or perimeter network, and provides administrators with the ability to:

- Remotely monitor the network connection of each vKey device
- Remotely wipe or disable vKeys thought to be lost or stolen (disabled vKeys can easily be returned to service)
- Health check and performance monitoring of each vKey device
- Link vKey devices to Active Directory users
- Create new vKey devices from regular portable storage media

Integration with Citrix products is sheer simplicity; users can access Citrix services directly from the vKey operating system. Once vKey is booted and the virtual operating system launched, the typical user will launch a browser from the vKey desktop. The browser is pre-configured so

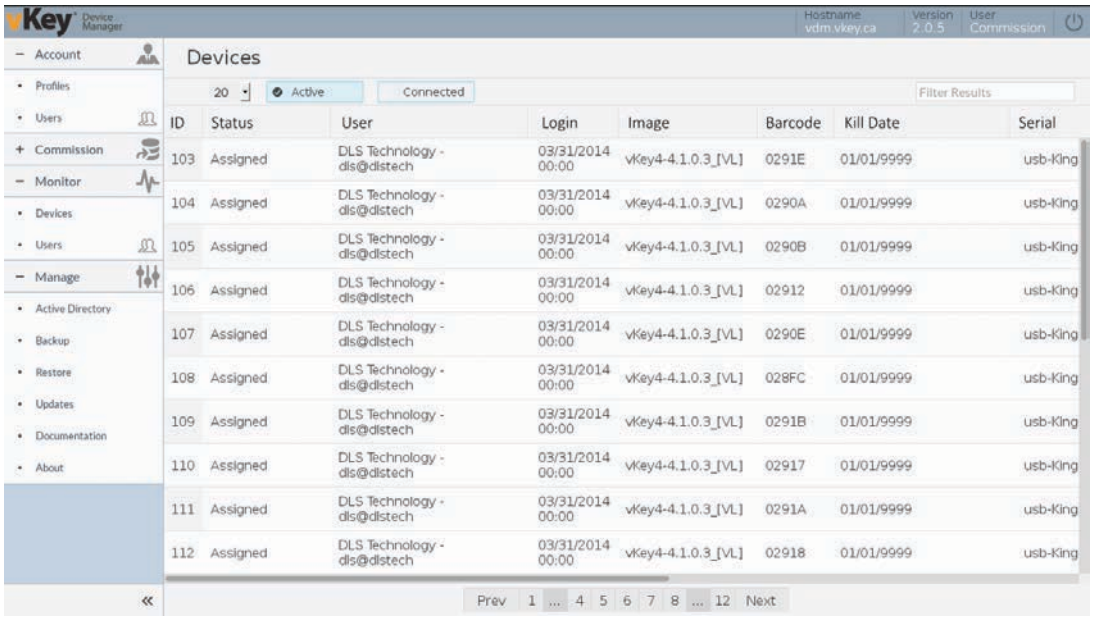
[5] https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/compliance-checklist-dar.pdf.

the user will only be required to enter a password to gain access. vKey enables Secure Remote Access to Citrix applications or products through two options:

1. Browser direct connection to the organization's Secure Remote Access site
2. Standalone Citrix Receiver on the vKey desktop that can be configured to connect to the SRA site

vKey also enhances compatibility with Citrix products by supporting the use of any peripheral software or devices users require (smartcards, webcams, microphones, printers, etc.).

vKey is compatible with a broad range of devices. Any modern system, PC or Mac, can be used as a vKey host machine, making vKey completely device agnostic. Accordingly, vKey provides a level of usability and flexibility that is unique among endpoint security solutions.



Other unique benefits of vKey include:

- **Superior Compliance Support:** vKey's secure operating system — which cannot be infected with malware that may exist on the host computer — provides continuous and complete compliance with any organizational or government-mandated security protocols. vKey's AES-256 encryption provides an essentially unbreakable level of security that helps to assure ongoing compliance. The administrative ability to manage each individual vKey by disabling and/or wiping eliminates the risk of threats to security protocols through lost or stolen vKeys.
- **Granular Management:** In addition to the ability to disable or wipe individual devices, vKey Device Manager provides extensive management capabilities for all deployed vKeys, including:

  - Monitoring users
  - Managing users
  - Commissioning individual vKey devices
  - Performing vDM database backups and restores
  - Linking Active Directory groups and policies to vKey devices
- **Environment Pre-Configuration:** It is possible to replicate a template to vKey and create an entire, ready-to-use system for new users, or for disaster recovery.

vKey Solution Detail

DLS vKey provides companies with the ability to easily provide trusted endpoints for remote access. Employees can access company systems with their own devices, simultaneously slashing organizational costs while boosting user productivity and satisfaction. vKey also enables endpoint whitelisting capabilities throughout the corporate infrastructure to ensure the integrity of users, systems and information. Put simply, vKey makes it possible for companies to safely tap into the many benefits of BYOD programs.

But even companies that have no interest in BYOD can realize a range of benefits from vKey, all ancillary to the obvious security protections provided by vKey. Corporate computers can remain in service much longer, for example, since security and performance concerns typical with older computers are eliminated. When performing software upgrades, vKey can be used to mirror systems to provide a disaster recovery resource if an upgrade fails. Each vKey can be loaded with multiple operating systems, eliminating the common need among support staff to maintain and carry multiple laptops for compliance and compatibility issues.

And vKey works with any form of bootable media, not just USBs. Organizations also have the option of managing company vKeys from on-site or through the cloud. Ultimately, both for users and administrators, vKey provides a degree of flexibility that simply cannot be matched by any competing solution.

A Proven Partnership that Enables Trusted Endpoints for Remote Access

The lack of trusted endpoints has foiled many organizations' aspirations to realize the benefits of BYOD programs, including lowered operational costs, greater employee productivity and improved user satisfaction. vKey eliminates the security concerns of BYOD by providing a solution that assures all endpoints used for remote access are perfectly secure — regardless of the device through which remote access occurs. Users stay productive while working remotely, and organizational systems and data are kept safe.

The vKey secure endpoint solution is proven to integrate seamlessly and easily with Citrix network security systems to provide a truly secure enterprise remote access platform. DLS's selection to the Citrix Ready Secure Remote Access program provides enterprises with a trusted and reliable remote access security solution for facing the ever-escalating security needs of the modern business environment. For companies seeking to protect themselves

against the modern-day scourge of cybercrime, the partnership of Citrix and DLS offers an affordable, flexible, proven resource for enhanced enterprise security.

For more information about DLS, please visit: http://dlstech.com and http://vkey.ca.

For more information about Citrix NetScaler, please visit: https://www.citrix.com/products/netscaler-adc/

Appendix

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

To learn more about the Citrix Ready Program partnership with DLS Tech, please visit: https://citrixready.citrix.com/dls-technology-corporation/vkey.html

To learn more about security solutions for business enterprises, contact Citrix and DLS.

About Citrix Ready
Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About DLS
Founded in 2000, DLS Technology Corporation (DLS) specializes in system integration and end-to-end architecture design, deployment, services and support for workspace transformation, mobilization, business digitalization and cloud. The company is headquartered in Ottawa, Ontario Canada. Since its inception in early 2000, DLS has become a leading technology solutions service provider fulfilling market needs of public and private sectors in the areas of, virtualization, secure remote access, cyber security, mobility, BYOD, cloud computing, and business continuity. DLS values sustainable relationships with clients, partners, and stakeholders. The company has been proven to commit to long-term client relations by providing and supporting them with partner-backed IT infrastructure design, development, implementation, project management, troubleshooting, and maintenance services.