



Building the  
Business Case:

# How Remote Access Solutions Deliver Business Value in UNIX/Linux Environments

Enterprises of nearly all sizes and industries are undergoing significant changes in how, when and where their employees work, largely due to both new technologies and the realities of global commerce and collaboration. Business leaders are pushing their IT departments to come up with new solutions to help their employees be more productive, while IT leaders strive to ensure that corporate systems are secure, available and delivering a superior user experience.

One issue that has caused some challenges for global organizations is weighing the needs of remote workforces against the technical limitations of a data center infrastructure running on UNIX and Linux operating systems. Business-critical workloads often run on UNIX and Linux servers, but traditional remote access tools often are inadequate to meet the requirements of employees who need access to these applications.

Many remote access solutions suffer performance degradation over wide area networks (WANs), especially in network latency and quality of service. Traditional solutions such as virtual network computing and its derivatives—based on data streaming technology—

**OPENTEXT™**

 **TechTarget Custom Media**

typically consume substantial network bandwidth and often encounter performance problems in high-latency/low-bandwidth scenarios. This, in turn, can cause the user interface to become unresponsive, resulting in a degraded user experience.

Of course, this has significant impact on IT organizations that need to ensure reliable and secure delivery of data over WANs—often with multiple projects contending for precious bandwidth. Take the example of engineers who may lose up to 20% productivity because of unresponsive programs. Multiply that by the number of engineers affected throughout an organization, and it will quickly add up into significant cost implications.

Another problem is stability. Consider companies in the electronic design automation marketplace; they run extensive, time-consuming simulations that take 10 days to complete. What happens if their session suddenly crashes on day eight of the simulation?

In the face of these challenges, there are many reasons why organizations adopt remote access solutions for UNIX and Linux environments:

- **Endpoint consolidation.** By replacing UNIX/Linux endpoints with central applications servers that can serve hundreds of users simultaneously, organizations are able to remove the costs endured by maintaining UNIX/Linux workstations. By replacing them with Windows endpoints, these organizations can move to a remote connectivity solution to link to application servers in the data center.
- **Server consolidation.** Reducing the number of physical servers in the data center helps to reduce capital expenditures and software licensing costs. High-performance remote access software requires fewer server computing resources, which has a significant ripple effect that results in simplified management as well as cost savings.
- **Mobility.** Trends such as bring your own device and easy user access to cloud-based services mean that employees want and need to do business anywhere, and at any time. This need for pervasive mobility puts enormous pressure on organizations to ensure suitable performance over long distances; reliable access to services, data and applications; and robust security.
- **Support for high-quality graphics.** Many X servers do not render UNIX graphical applications accurately, and since the Windows environment is based on the X Window standard, X-based instructions need to be emulated and rendered using a different graphics library. This often leads to drawing inaccuracies.
- **Focus on reducing both capital expenses and operating costs.** It's no longer only the CFO who wants to save money on IT expenses; line-of-business managers whose budgets often bear the costs of equipment purchases, software licenses and other subscription-based services are looking for ways to support global productivity without busting the budget.

- **Avoidance of costly and complex operating system migration efforts.** Many organizations learned valuable—and, at times, costly—lessons when migrating from Windows XP to Windows 7 and/or to Windows 8. OS migration is expensive and time-consuming, and organizations are looking for alternative ways to modernize IT architecture without affecting access to production systems and essential workloads.
- **Security and intellectual property protection.** Moving to a centralized access methodology is a big step forward in protecting sensitive data. Keeping that sensitive data in the data center adds an essential layer of protection by requiring all appropriate staff with requisite privileges to securely access it through a firewall.

Finding the right remote access to UNIX and Linux environments has not always been easy. As mentioned earlier, traditional remote access solutions for UNIX/Linux-based systems have often come at the price of performance degradation, higher CAPEX and OPEX costs, diminished quality for graphical applications and increased security risks.

Fortunately, there are effective and innovative solutions to consider.

## Why a New Class of Remote Access for UNIX and Linux Makes Sense

Building the business case for investing in remote access solutions for UNIX/Linux applications requires a thorough analysis of both the business and technical advantages of such an approach. It also means that IT organizations and their business counterparts need to develop a clear checklist of capabilities and features in a solution that enables reliable, secure, high-performance access to Linux and UNIX applications over a broad geographic area.

Here are some specific capabilities to look for, and how they can help justify the investment in money, time and resources to implement a remote access solution for UNIX/Linux environments:

- **Lower capital and operating expenses.** Of course, everyone wants to make sure that they are getting the most from their tight budgets, so investing in a new remote access solution has to cost-justify itself by allowing the organization to cut back on capital expenses, operating expenses or both. Your remote-access solution needs to ensure that you don't compensate for network bandwidth problems or latency issues by forking over more money to buy more network infrastructure. It also needs to ensure that organizations don't spend more money on network and systems management tools to overcome problems with existing remote access solutions.
- **Support for global workgroups.** Global collaboration isn't just for multinational corporations; midsized and even relatively small companies increasingly need to support workgroups in different locations that require access to the same content, applications or services. If workgroups and teams operating in different regions have predictable performance and an improved user experience, it will increase collaboration and result in more efficient project completion.

- **Improved graphical renderings and performance over WANs.** As more organizations move to graphics-based data formats (file transfer, streaming video, rich web content, etc.), it puts more pressure on the IT infrastructure to deliver bigger and more complex data sets, especially over wide areas. Not all remote access solutions can reliably process very large, graphically oriented data sets over wide areas without requiring additional infrastructure or a reduction in the use of graphics files during peak network bandwidth consumption. Look for a solution that supports server-side rendering of complex graphical applications as well as an X-style graphics rendering instruction model with a high amount of compression for less complex applications.
- **Robust security.** Whether it's identifying and remediating potential security breaches or ensuring conformance to compliance mandates, security is paramount. The main requirements of a top-notch remote access security framework are protecting intellectual property by preventing copying from the data center via screenshots, file copying and data stream recordings; preventing access to secure systems by unauthorized users or hackers; complying with ISO 27001 privacy guidelines; and having sensors and alerts in place to notify an administrator of potential breaches. Additionally, the remote access solution should be able to encrypt and authenticate all connections, with support for FIPS 140 and 201 standards for government organizations and their contractors.
- **Alignment with corporate moves toward data center consolidation.** As mentioned earlier in this paper, more and more enterprises are looking to consolidate numerous and often far-flung data center operations into a centralized resource when possible. Think of the dramatic savings in infrastructure spending, power and cooling costs, systems management and physical real estate if your remote access solution helps downsize or even eliminate remote data centers.

## Why You Should Consider Exceed™ Virtual Access TurboX from OpenText

OpenText's solution for UNIX/Linux remote access, OpenText™ Exceed™ Virtual Access TurboX (ETX), is designed to accelerate employees' productivity, wherever they conduct business.

Compared with alternative solutions, ETX offers significantly better performance, particularly over wide area networks. ETX enables organizations to virtually deploy UNIX/Linux applications to users by keeping them running on UNIX/Linux servers while allowing users to remotely access those applications through a web browser on Windows, Macintosh and Linux PCs as well as through an iPad application. It removes limitations and complexity normally associated with other remote access methods by offering the fastest connectivity and a uniquely intuitive user experience.

Exceed VA TurboX is deployed as a centralized, web-based portal for launching applications and to handle all administrative tasks; among its essential management functions are user access control, monitoring and email alerts. It also supports an innovative load-balancing feature that ensures that sessions begin on the most lightly loaded application server.

Stability and resiliency are critical elements to any remote access solution; ETX can be configured as a highly available solution, with all critical server components providing failover capabilities. ETX is designed for high availability, with graceful failover of all server-side components. The ETX core engine is extremely stable and is backed by 25 years of experience. Remote sessions are frequently left running for months or even years at a time, without disconnects or crashes.

As business demands dramatically increase, especially for workloads spanning wide geographic areas, ETX offers adaptive performance tuning under a wide range of network conditions and application requirements. ETX also supports wide-area collaboration by allowing users to share screens with colleagues in other locations. It even supports your mobile workforce through an intuitive iPad application.

Exceed VA TurboX provides a highly secure environment with TLS and SSH encryption across all communications, and uses FIPS 140-2 certified cryptographic libraries. The web-based management interface provides a variety of enterprise authentication options as well as fine-tuned user access management and application permissions.

Exceed VA TurboX is backed by OpenText's extensive track record of success in enabling worker productivity with high-performance, reliable solutions, along with a global support organization to help enterprises get the most from UNIX/Linux applications over broad geographic areas.

**For more information on OpenText Exceed VA TurboX, please visit**  
**[www.opentext.com/campaigns/exceed-va-turbox](http://www.opentext.com/campaigns/exceed-va-turbox)**