BYOD is easy to manage with VDI.

A Simple VDI Solution That Solves the Challenges of BYOD Effectively for Both End-users and Administrators.

bantoe

BYOD is Easy to Manage with VDI.

A Simple VDI Solution That Solves the Challenges of BYOD Effectively for Both End-users and Administrators.

Table of Contents

The Demand for BYOD Brings Risks for IT

As if challenges with security, software cost and complexity, and support and control of desktop systems are not enough, IT now faces another burgeoning issue: the consumerization of IT. Workers increasingly enjoy high-end consumer devices and anywhere, anytime connectivity outside the workplace. Now they are bringing those devices, and expectations, to work. Layer in the changes occurring in devices utilized by end-users, Forrester predicting the growth of wearable devices for example, and the complexity grows.

The bring-your-own-device (BYOD) trend means that users now want access to the Internet, along with corporate email, applications and data, from every mobile device they own. In many cases, IT does not issue or control those devices. Rather, users purchase them for personal use, then expect the same access that they enjoy at the office to be available anywhere outside the workplace. Enterprises, government agencies, and educational institutions are responding by allowing employees to connect personal devices to the corporate network.

Forrester reported in their 2013 Forrester Mobile Security Predictions that personal devices will be the norm for enterprise computing. More than 70% of organizations have some form of a BYOD program. Their Forrsights Workforce Employee Survey identified that 62% of those who use a smartphone for work and 56% of those who use a tablet for work purchased the device themselves.

Similarly, a 2013 Virtual Bridges survey of IT professionals found that the number of devices in the office is growing rapidly, with 70 percent of users carrying 3 or more devices and 26 percent carrying two devices. Only 4 percent reportedly carried a single device.

In addition to demands from the end-users, the consumerization of IT is being linked to improvements in productivity, nabbing the attention of department and business leaders. (Watch this TrendMicro video that identifies competitive advantages of supporting BYOD.)

Clearly, mobility and network access from anywhere has become increasingly critical and accepted–not just for employees, but for partners and customers as well.

At the same time, high-end mobile devices bring a host of risks that IT must move quickly to manage. Risks are inherent in network management, but BYOD raises the bar, calling for more secure access to applications and data, along with consistent performance on a variety of devices, and business continuity and support regardless of the user's endpoint device.

Typically, traditional IT management methods, already teetering under the stress of managing thousands of diverse desktops, cannot scale to manage the additional load of a BYOD environment effectively. Recognizing that, companies are moving to virtual desktops. The Gartner study found that, over the following 12 months, the vast majority of respondents planned to transform their desktop PC client environment to hosted virtual desktops.

The right VDI solution mitigates BYOD risks and addresses employee needs effectively. For all of its potential headaches, the consumerization of IT also offers considerable benefits to the enterprise. IT organizations can reduce capital expenses when employees elect to use their own mobile devices and access plans. Accommodating personal devices in the workplace can extend worker productivity, since it allows employees to access devices, email and data at more times and places. With access to their desktops from anywhere, workers can collaborate with others without constraint.

Carefully crafted BYOD policies that regulate security and data access, along with the right VDI solution to help IT bring devices under control, help to control the inherent risks of BYOD, cut capital expenses and enhance employee productivity while keeping the network functioning and secure.

How VDI and Virtual Bridges Address BYOD Risk

The incursion of consumer devices changes the enterprise landscape for IT, bringing increased pressure to bear on network management issues. The right VDI solution can help by addressing three key areas of risk in particular: Security threats, business continuity and support challenges, and operational efficiency issues that can derail performance on any device.

Done properly, VDI can address each of these BYOD risks, turning the challenge of the consumerization of IT into a sustained benefit for the enterprise.

Risk 1: Security Threats

Solution: Deliver pixels, not actual data, to users; so that data remains in the data center

Security is an ongoing challenge for any enterprise, and consumer devices on the corporate network up the ante by requiring IT to attempt the impossible–to keep permanent enterprise data off endpoint devices.

Even with strict policies and data encryption, corporate security risks ratchet up under a BYOD program.

Fortunately, VDI already supports a highly secure infrastructure. By definition, virtualized desktops mean that no data resides on any endpoint device. Much like the “screen-scraping” technologies used with mainframe computers, desktop virtualization means that only a representation of the screen appears on any device. Whether users access corporate data and systems through desktop PCs, notebook computers, tablets or phones, the process is the same. Pixels, not data, flow to the user; no actual data is delivered to the device, and all data remains in the data center. A misplaced, lost or stolen device does not compromise data. Without appropriate access such as user ID and password, there is no access to the backend server, and thus no access to enterprise data.

Furthermore, VDI means that virus protection resides on the server rather than on individual devices, making device security in a BYOD environment far easier to maintain. IT keeps virus software current, maintains one set of rules and restrictions, and monitors one set of security software. Users access their desktops from any device, unaware of the protections in place.

Tracking the flow of data for compliance purposes is easier with VDI. Industries such as healthcare and finance are among those at the forefront of embracing the promise of consumer mobile devices in the workforce. Those industries, however, must also follow a myriad of data privacy and security regulations, including HIPAA for healthcare and Gramm-Leach-Bliley for financial institutions. Again, because virtualization means that data never leaves the server, there are no issues with tracking data dispensed to individual devices, thus eliminating one of the potential trouble spots in compliance for IT.

Risk 2: Loss of Business Continuity

Solution: Sessions that run in the data center, not on devices

With an increased number of devices vying for network access and IT support, business continuity can be a risk for any BYOD program. The risk of employee downtime increases when there is a greater number and variety of devices to track and support.

VDI already addresses business continuity issues by maintaining control of the desktop at the server level. Users who connect to their desktops via mobile device are connecting to a session running on the corporate servers, much as someone using a cloud-based application connects to the cloud. With VDI, control remains in the data center–as long as the connection in available, so is the desktop session.

Further addressing the risk of an interruption in business continuity, VERDE offers seamless roaming capabilities between offline and online user sessions. Users connect to a single desktop during a session. There is no need for IT to support various versions of applications for various devices, since software runs at the server level using integrated elements.

All VERDE servers are stateless; each has a unique address assigned to it but is otherwise identical to every other server. The unexpected loss of a number of servers simultaneously may slow the network, but the cluster continues to operate. When servers are back online, they begin working automatically after automated deployment, without human intervention or an extensive setup process.

Backing up consumer devices, another business continuity challenge, is not a concern with VDI, since data never leaves the data center. IT handles backups, not users, so that the malfunction, loss or destruction of a mobile device does not result in data loss.

Risk 3: Performance Hits

Solution: Move processing closer to mobile devices in the field

With an influx of new devices that demand network access around the clock, BYOD can adversely affect network performance. Users, increasingly attuned to high performance on personal endpoints outside the office, bring those expectations to the workplace along with their devices. The burden then falls on IT to meet those expectations.

VERDE avoids performance issues through a unique, decentralized design. VERDE Cloud Branch technology, in which desktops are hosted on branch servers and managed from the data center, puts VDI processing closer to mobile devices in the field. That avoids the latency issues that can arise when mobile users connect back to a remote data center. VERDE's decentralized structure also can provide access to applications on mobile devices even when the data center itself is unreachable. VERDE's built-from-the-ground-up design yields tight integration and a small footprint, further assuring users a high-quality connection and performance regardless of the device users choose to use.

Summary: Bring BYOD Risks under Control with VDI

BYOD can empower your end-users and provide an advantage is today's competitive arena by offering the ability to work anywhere, anytime–greatly improving productivity and increasing collaboration. Recognizing that, more and more companies and government agencies are allowing employees to connect their personal mobile devices to the network. However, BYOD introduces risks as well, including the security challenge of managing data on a range of end-points, potential performance issues with far-flung mobile devices, and business continuity challenges.

Virtual desktop technology is tailor-made to help manage the challenges of BYOD. The right VDI technology and approach can address the inherent risks of a BYOD program in an efficient and cost-effective manner. Whatever your enterprise's desktop management strategy and BYOD policy, Virtual Bridges offers a solution to help mitigate the risks of BYOD.

Additional Resources

Understanding Successful VDI Implementation
White Paper

Linux and VDI Security for the U.S. Department of Defense
Case Study

See How Easy VERDE is to Use
Video