



DesktopDirect

Large-Scale Remote Access & Mobility

Today, secure remote access must support the increased demands of productivity, mobility and business continuity. Learn why traditional VPNs are not up to the task and why remote desktop access is superior for cost-effectively achieving enterprise-wide remote access and mobility.

TABLE OF CONTENTS

Introduction	3
Business Drivers for Enterprise-Wide Remote Access	3
Impact of Remote Access on Speed of Decision Making	3
Impact of Business Disruptions on Revenue	4
Impact of Business Disruptions on Productivity	4
Cost of Security Lapses and Compliance Violations	5
Organizational Preparedness	5
Popular Approaches	6
VPNs	6
Server-Based Computing	7
Virtual Desktop Infrastructure (VDI)	7
A New Approach	9
Appliance-Based Remote Desktop Access	10
Security	10
Performance & Scalability	11
Mobility	11
Return on Investment	12
Productivity	12
Vs. VPN	12
Vs. Server-Based Computing (XenApp)	13
Vs. VDI (XenDesktop)	13
Vs. Cloud-Based Solutions	13
Energy Savings	13
Summary	14
About Array Networks	15

Introduction

Prior to 2006, the number of employees that worked remote remained stable at less than 20%. Now, according to Forrester Research, 62% of knowledge workers in the U.S. and Europe routinely conduct at least a portion of their work offsite. The Aberdeen Group reports that 84% of today's organizations are deploying a form of remote, mobile and wireless access, and that over 58% of organizations said their greatest pressure was propagating the benefits of remote access beyond the executive suite and field sales to the broader organization. In government, the Telework Enhancement Act of December 2010 recently passed its six month mark and is already delivering improved business continuity, management efficiencies and employee satisfaction.

Remote access and mobility is on the rise, and in the not too distant future may be required enterprise-wide for many organizations. This document looks at the business drivers fueling mobilization, analyzes the suitability of established solutions with respect to enterprise-wide remote access, and introduces a new approach to enterprise productivity and business continuity – pioneered by Array Networks – purpose-built for cost-effective large-scale enterprise-wide remote access and mobility.

Business Drivers for Enterprise-Wide Remote Access

According to the Aberdeen Group, increases in the speed of decision making are directly related to the prevalence of remote access within an organization. A recent Microsoft study found the average teleworker spends four days per month working from home and many more workers log back in at night and on weekends. Clearly, an increased level of remote access leads to a more productive organization capable of making more well-informed decisions at a faster pace than the competition.

Impact of Remote Access on Speed of Decision Making

Enterprise Classification	Employees with Remote Access	Increase in Speed of Decision Making
Best-in-Class (Top 20%)	88%	18%
Average (Middle 50%)	44%	15.7%
Laggards (Bottom 30%)	10%	5.7%

*Aberdeen Group

Making remote access available to workers so they can perform their duties remotely provides significant benefits not only in mitigating business continuity scenarios, but also in mitigating more mundane issues such as car trouble, a sick child, deliveries, repairs or rushing to pick up a child from school or day care. In these instances, remote access can mean the difference between a task that is completed poorly or not at all and a task accomplished in a more flexible manner with better quality. Moreover, the monetary impact on an organization as a result of unplanned PTO and routine business disruptions is far greater than one might suspect.

The potential will always exist for pandemics, natural disasters and terror strikes to impact business operations, revenues and customer satisfaction, but more common are medium-scale events – such as snow days, transit strikes and “spare-the-air” days – that occur at least once or twice a year and can affect a significant number of workers at the same time.

Recognizing the combined impact and risks of unplanned time off, medium-scale business disruptions and the potential for large-scale business continuity events, the business case for expanding remote access to boost productivity and mitigate disruptions becomes quite compelling. Assuming 250 business days per year, we can compute average losses for a business in the case of various disruptions by using the simple equation of revenues divided by total working days per year.

Impact of Business Disruptions on Revenue

Total Annual Revenue	\$500,000	\$5,000,000	\$1,000,000,000
Revenue Loss Per Day	\$2,000	\$20,000	\$4,000,000
Transit Strike – 2 Days Lost	\$4,000	\$40,000	\$8,000,000
Natural Disaster – 1 Week Lost	\$14,000	\$140,000	\$28,000,000

*Based on 250 business days per year

The average revenue per employee of a Fortune 500 enterprise is \$400,000, while smaller organizations average about \$100,000 per employee. It is true that not every employee generates the same amount of revenue, but we are discussing mundane business disruptions that happen to all of us once or twice a year and so it is appropriate to look at average productivity. Using the same 250 days per year, it is clear that days lost multiplied by the number of employees in an organization can result in a huge loss of productivity, not counting soft benefits associated with employee satisfaction, better customer service and faster, more accurate decision making.

Impact of Business Disruptions on Productivity

Total Employees	5	1000
Average Revenue Per Employee	\$100,000	\$400,000
Productivity Per Day Per Employee	\$400	\$1,600
Yearly Cost of 2 Unplanned PTOs Per Employee	\$4,000	\$3,200,000

*Based on 250 business days per year

Adding mobility into the equation, Apple is expected to sell over 44 million iPads in 2011 and the total number of tablets sold in 2011 is expected to surpass 60 million units – a staggering year-over-year growth of 275%. Apple tablet shipments are expected to reach 120 million units in 2015, and with Android tablets rapidly increasing their share, total shipments for the same period are expected to reach 275 million. These trends are being heralded as the “Post-PC” era.

Too often, tablets are not subject to the same level of scrutiny and central management as is common for laptops, desktops and smart phones. In many ways, it seems that tablet adoption is the reverse of smart phone adoption: adopt first, manage later. Anecdotal observation shows that smart phones had to pass rigor with IT before they were permitted into the workplace. Tablet adoption, on the other hand, appears to be driven by a combination of ‘top-down’ usage by boards of directors and the C-suite and ‘grass-roots’ usage by thought leaders and today’s younger generation.

Even among best-in-class organizations, security for tablets is implemented about half as frequently as smart phones. Ironically, tablets are being used in many cases because of the greater level of interaction with company data and back-end services encouraged by their larger screen sizes. Another significant challenge brought about by tablets is the trend towards “consumer IT” or Bring Your Own Device (BYOD), where workers use any number of different employee-owned tablet platforms for both personal and business use – thereby creating tremendous challenges in supporting remote access while securing corporate data.

Cost of Security Lapses and Compliance Violations

Violation	Mean Risk Per Security Lapse
PCI DSS	\$491,684
HIPAA	\$147,485
Tax Implications of Stolen Device	\$13,429

*Applies to violations and security lapse on any device, including PCs, tablets and smart phones

The mean risk per security lapse for a PCI DSS violation is \$491,684. HIPAA violations have a mean cost of \$147,485. Tax implications of employee reimbursement on a lost device average \$13,429. Tablets and BYOD make the probability of violations that much higher. As a result, organizations must take a serious look at their remote access strategy in order to implement a scalable architecture that meets employee demands while compensating for the increased risks of a more mobile workforce.

Organizational Preparedness

While the need and benefit of enterprise-wide remote access is clear, providing it would cause most remote access infrastructures to crumble. This is because traditional VPNs were built using the old 80-20 rule where those needing remote access accounted for 10% to 20% of the organization. VPNs were also created with the old notion that securing the connection was enough, ignoring the fact that data leakage is the number one risk of enabling remote access. As a result, VPNs now require client software, managed laptops and additional security to mitigate data leakage and thus are not flexible enough to deliver safe access from home PCs or personal mobile devices. Moreover, because many remote access solutions were implemented prior to the influx of smart phones and tablets, it is not uncommon for organizations support remote access and mobility independently, perhaps utilizing a mobile access gateway that offers authenticated, encrypted wireless access, but only to one kind of smart phone.

Consider the example of remote access for productivity and business continuity at an Array customer that is a top-10 financial services organization headquartered in New York. The organization routinely reports a 500% spike in remote access traffic during snow storms, and Fridays also show significant spikes in remote access traffic as many people work from home.

Think about the implications of so many office and field workers needing remote access at the same time; relying on a traditional remote access architecture, there would be performance degradation at a minimum and, more likely, a large chunk of users that would not be able to log in at all. Think about the implications of office workers attempting to use VPN technology for the first time during a business continuity event; how will this impact help desk calls and the effectiveness of the overall solution? What are the risks of data leakage for enterprise-wide, network-level remote access in both day-to-day and business continuity use cases? How will providing sufficient bandwidth for enterprise-wide VPN access impact the budget?

Without careful consideration, deploying an enterprise-wide solution for remote access and mobility can quickly turn risky, costly and complex, without the desired returns in productivity and business continuity.

Popular Approaches

So far, we have made the case that there is a need for expanded remote access driven by advances in mobile technology and an expectation of geographic flexibility in the modern workforce. It is also clear there are significant competitive advantages to driving remote access deeper into the organization. On the flip side, providing remote access enterprise-wide is easier said than done. To determine the best course of action for scaling remote access, a logical place to start is understanding of the limitations of today's most prevalent remote access solutions.

VPNs

The most common approach to providing remote access is the Virtual Private Network (VPN) – usually based on IPSec or SSL. While VPNs provide excellent encryption for data in transit, they do nothing to protect against leakage once data reaches the end point. Ironically, it is endpoints that are the most vulnerable when it comes to security. And because VPNs make remote devices a part of the corporate network, they have the potential to open up thousands of attack vectors and security gaps. To compensate, many organizations implement more security software on the endpoint such as disk encryption coupled with data leakage prevention. These additional technologies bring additional costs. They must be supported with enterprise key management and mobile device management for remote wiping and lockout. Because the enterprise is vulnerable to viruses, worms and other such infections caused by unauthorized end-user activities, IT must also install personal firewall, anti-virus, anti-spam and other malware protections to guard the organization from rogue devices and guard end-users from the possibility of an infected enterprise.

As compared to IPSec, SSL VPNs are capable of providing ubiquitous access from any Web browser, making it appear well adapted to flexible, large-scale remote access. But the ability to provide connectivity from both managed and unmanaged devices requires even greater end-point security, including host checking, cache cleaning and virtual sandbox environments. Since these interfere with productivity, many organizations do not utilize these features and end up with a VPN solution that is more flexible but also more susceptible to data leakage.

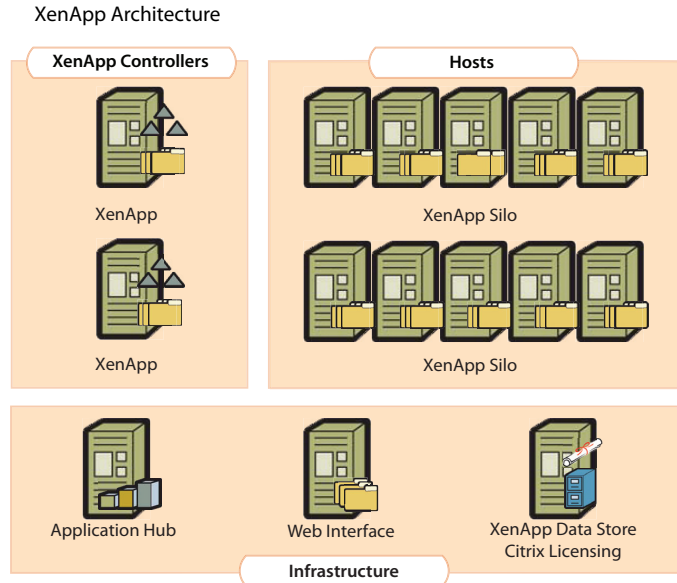
Whether based on IPSec or SSL protocols, VPNs must always transfer data to the endpoint and utilize endpoint applications to consume data – meaning data has left the enterprise. When laptops, tablets or smart phones are lost or stolen, it does not matter if they are encrypted or not – time and effort must be spent in accounting for them and reporting what data was present in order to satisfy compliance authorities.

According to Gartner, a well managed PC costs roughly \$3400 per year, while a well managed laptop costs about \$7000. By virtue of being mobile, the usable life of devices such as laptops, tablets and smart phones is usually one or two years shorter than that of stationary devices such as desktop PCs. And while the price of laptops has come down, and many organizations have issued laptops to a large number of their employees, the disparity in cost between supporting a desktop and laptop remains sizable and contributes heavily to the cost of scaling VPN access.

Taking into account the time and expense of laptops and end-point security, the security implications of enterprise-wide Layer-3 network exposure and the fact that VPN access from tablets and smart phones exacerbates these issues, it is hard to rationalize expanding VPN use beyond the initial 20% of field users, power users and road warriors for which it was designed.

Server-Based Computing

Server-based computing has been in existence for well over a decade. Citrix®, for example, has offered XenApp (formerly Presentation Server and Metaframe) for over 15 years. XenApp is an application publishing solution and therefore requires servers, access gateways and other elements to securely deliver applications. To access published applications, clients are required on all end-point devices, including home PCs and tablets. In addition, a basic XenApp deployment will also include XenApp controllers, application hubs, Web Interfaces, XenApp data stores, Citrix licensing servers and hosts.



The benefits of server-based computing are straight-forward. Applications can be managed centrally to reduce costs and can be delivered anywhere to improve productivity. It is a flexible approach, in that the client may be deployed on any type of device, managed or unmanaged, including laptops, desktops, tablets, smart phones and home PCs. It is also a secure approach, as users are merely controlling and manipulating applications and data residing in the corporate data center. The client can be configured such that data cannot be copied, pasted, printed or otherwise captured, preventing data leakage under virtually any circumstance.

The downside of server-based computing is best illustrated by looking at typical enterprise Citrix deployments where XenApp is usually deployed only for select employees and applications, as larger deployments simply do not make economic sense. Delivering the benefits of server-based computing requires a tremendous amount of server infrastructure, as well as associated management overhead in maintaining the infrastructure.

The recent experience of an Array customer makes the point. According to Buckingham Research Group, upgrading 100 users from XenApp 4.3 to XenApp 5.0 was required to enable the tablet access they desired. However, the move to XenApp 5.0 also required upgrading servers, operating systems, licenses, memory and CPU to the tune of roughly \$300K and a deployment schedule spanning 9 months.

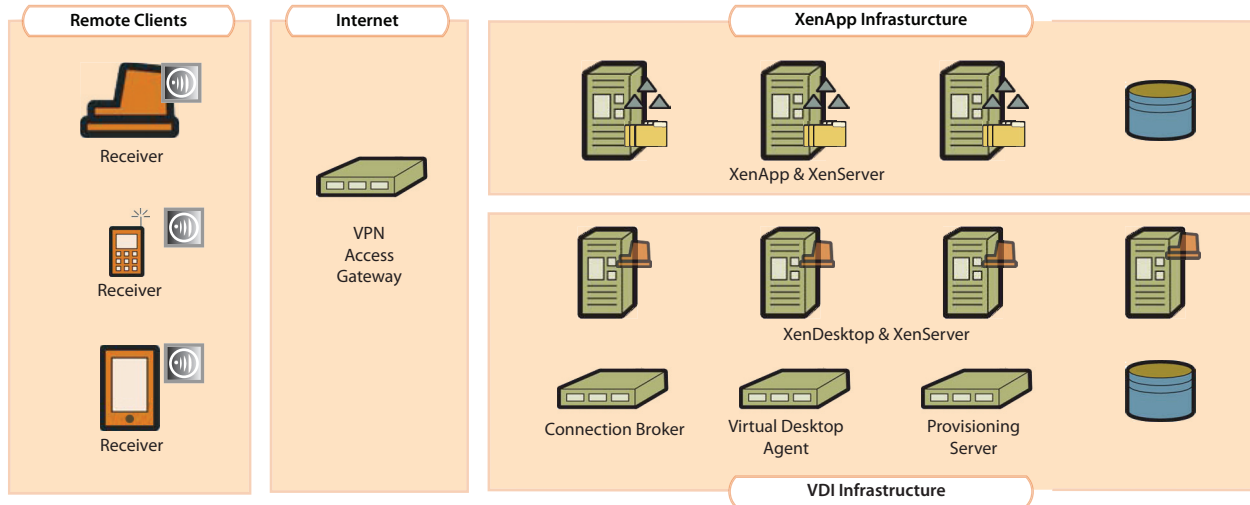
Cost and complexity rapidly sky rockets in Citrix environments, and while server-based computing can address the flexibility and security requirements of scaling remote access enterprise-wide, from a cost perspective it is all but unfeasible.

Virtual Desktop Infrastructure (VDI)

Many organizations have explored virtual desktops as another alternative. Lured by the promise of reduced operational support – and the ease of management brought about by a centralized infrastructure – numerous businesses have started VDI initiatives only to later discover hidden costs that hamper wider deployment. Similar to server-based computing, VDI is secure and flexible; VDI also addresses the issue of some applications being

present on a physical PC and other applications being published, as is often the case with server-based computing. With VDI, desktops and applications are all hosted centrally and may be delivered to any user, on any device, anywhere. The tradeoff is that VDI is even more expensive and more complex than server-based computing.

XenDesktop Architecture



According to Gartner analyst Mark Margevicius, typical VDI capex is 1.5 times that of PCs, and according to Forrester, an average VDI deployment costs roughly \$860 per virtual desktop provisioned, excluding the cost of networking, storage and remote access upgrades which themselves can be quite significant.

Citrix XenDesktop and VMWare View run on hypervisors tuned for CPU-oriented workloads – not storage and retrieval – and thus cause write cycle delays that limit the number of available sessions that can be run in parallel. Memory dedicated to virtual machines is also a critical component of VDI scalability, as is the number of virtual CPUs devoted to applications with varying workloads. To support as many virtual desktops as possible, servers utilized in VDI environments commonly run dual multi-core CPUs and up to 128GB of memory, in addition to very fast RAID storage or SSD.

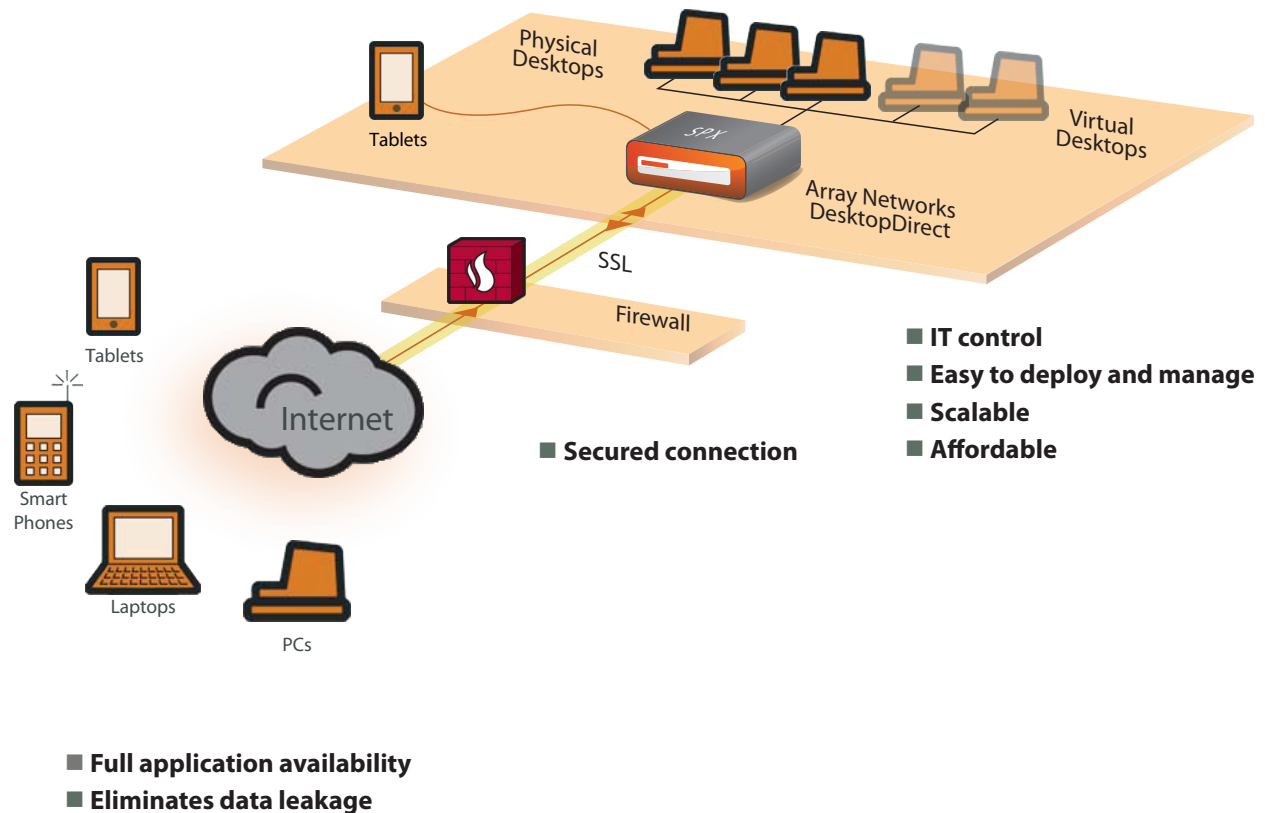
These servers cost between \$15K to \$20K each and typically support no more than 40 VDI instances. Furthermore, enterprises are required to pay license fees for each virtual desktop to the tune of roughly \$300 per year. Add in \$100 per license for Microsoft Terminal Services, \$300 to \$400 per user for hardware and the bandwidth required to stream desktops to remote users, and it is easy to see how Forrester computes capex of \$860 per virtual desktop.

Though VDI vendors tout lowered opex in years two through five, they often ignore hidden costs of network, storage and server upgrades. There's the premium for IT personnel capable of managing centralized infrastructure, which must scale in proportion to the deployment. Bandwidth can also be an issue; for example, VMware View running PCOIP is a known bandwidth hog. In addition, because all VDI access is remote access, organizations must invest in access infrastructure that can provide the right trust model and audit capabilities and can also provide the ability to scale on demand.

In the end, much like server-based computing, VDI is best suited for select projects where ROI can be more readily calculated and is far too costly and complex to serve as the foundation for an enterprise-wide architecture for remote access and mobility.

A New Approach

Now let's look at remote desktop access, a proven technology with tremendous potential for solving the challenges of large-scale remote access and mobility. What if we could leverage existing, wide-spread investments in physical desktops and laptops? What if we could use these existing investments in hardware, software, security and applications to gain the benefits of server-based computing and VDI, without the cost and complexity? It is possible and the approach has several advantages – first and foremost being familiarity with the environment. Employees use their desktop environment day in, day out and do not require additional training. If the access aperture can be controlled such that remote users are not able to perform clipboard operations such as cut and paste, or transfer of files between a remote device and the office desktop, remote desktop can give IT immediate control over data. Data never leaves the corporate network – only screen, keyboard and mouse movements are ever transmitted back and forth. In essence, this approach brings the security and flexibility benefits of virtualization to physical desktops without the additional costs of centralized infrastructure. What's more, it gives organizations an alternative to VPN and virtualization that allows these technologies to be used when and where they make technical and economic sense.



Appliance-Based Remote Desktop Access

DesktopDirect is an innovative, appliance-based remote desktop access solution. Unlike VPNs, DesktopDirect enables employees to get to their office computers from any remote location — whether they be at their home office, at a customer or partner site, at a public Internet kiosk, or even from their iPhones and iPads. DesktopDirect uniquely leverages proven and scalable technologies to deliver the industry's most secure enterprise-class solution for remote desktop access and control.

The DesktopDirect appliance is installed in the corporate network and integrates with Active Directory or similar, as well as dual factor authentication such as RSA, to establish user credentials for secure access. On the corporate network, either physical or virtual desktops may be registered for users, a process that can be accomplished by the administrator manually or via a database, or by end-users using Array Registration Technology.

On the remote device, DesktopDirect launches an easy-to-use portal in either a standard Web browser or mobile app environment and displays icons for the desktops the employee has registered. For tablet access, users download a free application from an App Store, App Marketplace or similar to their corporate or personal tablet.

Users can name their desktops with personalized monikers that are easy to remember, thus avoiding the need to remember IP addresses and machine names which are difficult for the average user to recall. Clicking a desktop icon within the DesktopDirect portal engages single sign-on and seamlessly launches the user's desired work environment, making the solution extremely intuitive for office workers, day-extenders and even first-time business continuity users.

Security

In contrast to VPNs, DesktopDirect does not allow client devices to be present on the corporate network; employees simply control their physical or virtual office PCs using a remote device. Because data leakage prevention is a primary consideration, DesktopDirect has administrative controls that prevent clipboard operations such as cut and paste and disable printer redirection for remote devices. On the remote device, anti-key logging and anti-screen capture further bolster DesktopDirect's data leakage prevention capabilities. Over the Internet, traffic is encrypted using SSL for secure transmission from the remote device to the corporate network. On the corporate network, DesktopDirect leverages access infrastructures such as Active Directory, LDAP and RADIUS – as well as two-factor authentication including RSA SecurID, Vasco, Swivel and SSL certificates – to ensure access to office PCs is granted only to authorized remote and mobile users.

Running industrial-strength RSA/DES/3DES/AES 128-bit/256-bit key exchange and 1024/2048-bit encryption, DesktopDirect is a true enterprise-class access gateway. Leveraging tight integration with Active Directory, LDAP and RADIUS and two-factor authentication systems, DesktopDirect is capable of providing copious amounts of data to SIEM infrastructure, such as RSA Envision, to create a diagnostic dashboard of user activities and network vulnerabilities.

Unlike cloud-based services for remote desktop, DesktopDirect is an on-premise gateway that does not require organizations to expose their corporate directory to a third-party service. Typical cloud services also depend on client software running on host PCs and require host PCs to remain connected to the third-party service 24x7. As an enterprise owned and operated solution, DesktopDirect has no such requirements and fully eliminates security risks associated with this type of network exposure.

Performance & Scalability

In addition to security, supporting enterprise-wide remote access for productivity, business continuity and mobile access requires that the remote access architecture be highly scalable and highly cost-effective.

DesktopDirect runs on Array's high-performance line of SPX Series hardware. Tackling SSL bulk encryption and key exchange in hardware, Array SPX Series appliances provide the best performance available on the market for processing high-volume secure access. In customer tests, a single high-end SPX appliance running DesktopDirect could maintain over 10K concurrent remote desktop sessions, each with sufficient bandwidth and minimal latency. To ensure virtually unlimited scalability, up to 32 SPX Series appliances can be clustered to provide a level of performance and scalability – a magnitude of order better than competing solutions – that allows DesktopDirect to dramatically reduce capital and operational expenditures for enterprise-wide remote access and mobility.

In order for any customer to take advantage of DesktopDirect's industry-leading capacity and headroom, Array provides special business continuity licenses that allow organizations to purchase standard licenses for day-to-day use and purchase lower-cost, time-bound licenses as insurance against seasonality or unforeseen events.

The top-ten New York financial services firm – cited in the 'organizational preparedness' section – supports 35,000 employees on DesktopDirect. The solution has stood the test of time for over 6 years, and has come through for both productivity and business continuity in the face of hurricanes, storms, snow days, transit strikes and traffic spikes. "Another big day passed without much incident, thanks to Array" was the comment from their IT manager after a recent snow storm which saw spikes of 40% in daily usage. The additional productivity of several thousand users who would otherwise have been unable to come to work that day was estimated in the range of 10+ million dollars.

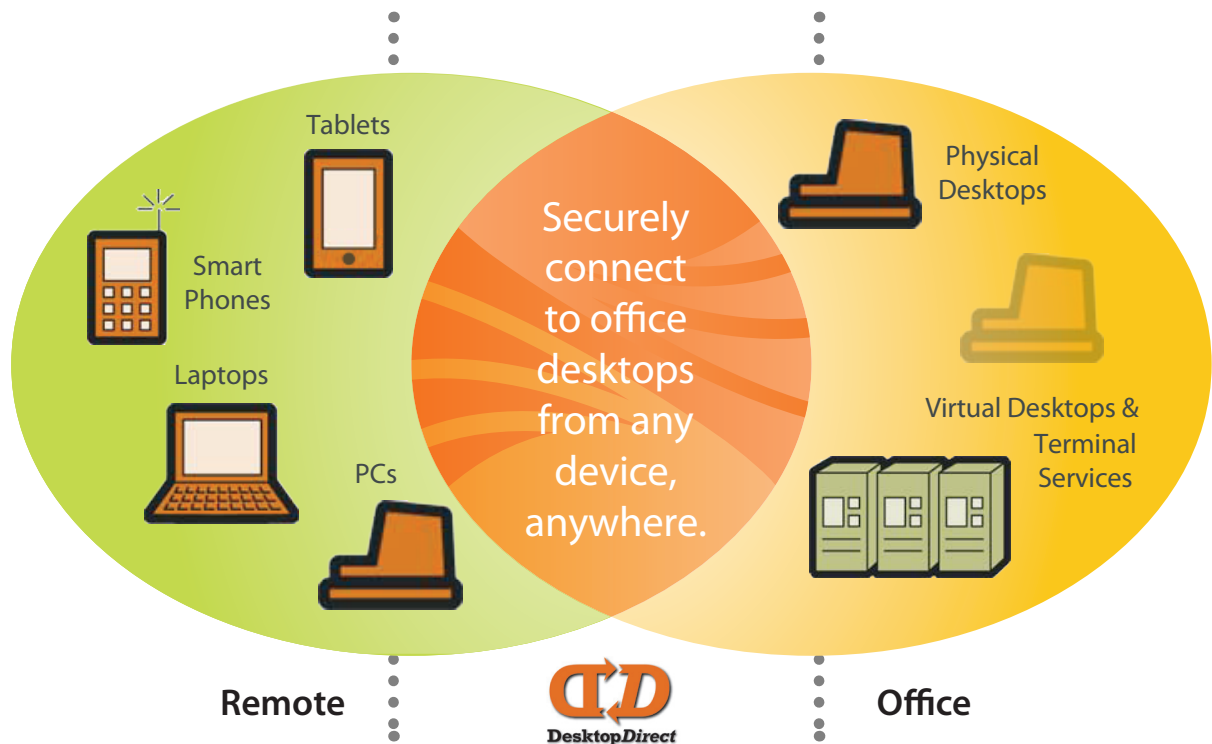
Mobility

The line between remote access and mobility is blurring, as workers want to be able to work anywhere, at any time, on any device. As noted earlier, any enterprise-wide solution for remote access and mobility must address the issues of security, application availability, cost and complexity as they relate to today's new breed of smart phone and tablet devices.

DesktopDirect comes complete with apps for iOS and Android that can be downloaded free of charge from Apple iTunes or the Android Marketplace to extend any enterprise application to any tablet environment without the risk of data leakage. Employees are able to utilize all of their existing Windows, Windows-based and proprietary applications without needing to re-purchase or port applications for the tablet environment. DesktopDirect also eliminates the security implications of developing applications for the tablet as well as the performance implications of moving data between the enterprise and the tablet. By bringing tablets and smart phones under the same framework as PCs, organizations can instantly gain control over enterprise data and alleviate concerns about corporate data intermixing with personal data on personal devices.

The moment the DesktopDirect app is closed on a tablet, the window to the enterprise is gone and the user has to re-authenticate before picking up where they left off. Advantages such as state maintenance and resilience can be provided without the extra costs normally associated with this type of functionality. Moreover, because there is no extra cost for the tablet apps, DesktopDirect represents a tremendous value to the organization. Using DesktopDirect to provide tablet access to business applications, enterprises can eliminate the cost, complexity and risk associated with attempting to repurpose VPNs, VDI, server-based computing or managed services.

In the example where upgrading 100 users from XenApp 4.3 to XenApp 5.0 for tablet access was going to cost Buckingham Research \$300K and take 9 months – using DesktopDirect, the firm was able to meet their requirements at a cost of \$30K in the span of only 3 weeks. DesktopDirect was able to achieve a ten-fold reduction in both cost and time for deploying mobile access for iPad, with full application availability and zero data leakage.



Return on Investment

The cost of an entry-level DesktopDirect appliance for providing secure access to desktops is \$140 per concurrent desktop on a 25-seat perpetual license, with prices-per-concurrent desktop dropping significantly as the user base grows. For enterprise deployments of 1,000 concurrent seats or more, DesktopDirect becomes orders of magnitude less expensive as compared to competing secure access solutions.

■ **Productivity** As demonstrated in the 'business drivers' portion of this paper, reclaiming two unplanned PTO days per worker can save a small business with 5 employees \$4,000 per year. For an enterprise with 1,000 employees, reclaiming two unplanned PTO days per year per worker can save an enterprise over \$3,000,000. This does not include additional productivity gains associated with expanded remote access and losses prevented in the case of medium and large-scale business continuity events.

■ **Vs. VPN** Beyond the cost of hardware and license costs for scaling VPN infrastructure, VPNs require corporate owned and managed laptops – averaging \$3,800 a year each – to enable secure remote access. DesktopDirect eliminates the need to purchase and manage new laptops enterprise-wide, providing both a better, more secure solution at a considerably lower price.

■ **Vs. Server-Based Computing (XenApp)** For organizations looking to publish access to Microsoft applications, DesktopDirect can provide cost-effective access to office PCs and terminal services, providing similar functionality at dramatically lower price points versus XenApp. Likewise, DesktopDirect can provide a more cost-effective approach to expanding existing XenApp deployments and can reduce costs for Citrix customers with large deployments and the burden of annual licenses.

■ **Vs. VDI (Xen Desktop)** DesktopDirect is a more scalable solution that requires fewer components and less management and leverages existing investments in hardware, software, applications and security. As a result, DesktopDirect is considerably more affordable as compared to virtual desktop solutions that typically cost around \$700 per user.

■ **Vs. Cloud-Based Solutions** Most enterprises will simply not consider managed services or cloud-based services for enterprise-wide remote desktop access because exposing the corporate network to the degree required is simply too risky. In any event, cloud-based offerings charge yearly license fees of \$150 - \$200 per year per user and incur an additional \$150 - \$200 per year per user in power consumption costs to keep PCs powered-up 24/7. An amount far in excess of the one-time cost of Array hardware and perpetual user licenses.

Array customer Needham Bank, a community bank in Massachusetts, switched from an online service to DesktopDirect and not only gained significant savings but also gain outsized returns in productivity. According to James Gordon, VP of IT, "Once we switched to DesktopDirect, we saw the stats for remote access went from 3 users per month to 33 users per month, and total remote access went up from 4 hours to 468 hours per month, a whopping 120x increase in remote productivity."



■ **Energy Savings** According to the 2007 PC Energy Report prepared by the Alliance to Save Energy and IE, "a mid-sized company wastes more than \$165,000 a year in electricity costs for computers that have been left on overnight. By turning these computers off, an employer can also keep more than 1,381 tons of carbon dioxide (CO₂) out of the atmosphere."

DesktopDirect allows users to shutdown their desktops when they go home and use Wake-on-LAN (WoL) technology with the click of an icon to remotely power up desktops when they are needed, reducing the cost of powering office PCs by 70% and resulting in an average of \$172 per desktop per year in power savings.

Summary

In summary, the demand for remote access and mobility is increasing, driven by personal needs for professional flexibility, technological advancements such as smart phones and tablets and enterprise imperatives such as increased productivity and the need to mitigate the effects of business disruptions. While there are many remote access solutions that are good in their own right, most are designed to serve a particular purpose and none have been designed from the ground up to address the security, flexibility, scalability and cost requirements of enterprise-wide remote access and mobility.

Leveraging proven remote desktop access technology, DesktopDirect provides a new approach to remote access and mobility that leverages existing infrastructure to reduce cost and complexity while gaining all the security and flexibility benefits of cutting edge solutions such as virtual infrastructure. With DesktopDirect, businesses can connect any user, anywhere, on any device to physical desktops, virtual desktops and terminal services, enabling full application availability with zero data leakage – at a price that makes enterprise-wide remote access and mobility a technical and economic reality.

About Array Networks

Array Networks is a global leader in application, desktop and cloud service delivery with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore™ software, Array solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 300 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, Red Herring and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

Belgium
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France
infosfrance@arraynetworks.com
+33 (0) 180 886 086

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@arraynetworks.com
+81-45-664-6116

Korea
array-sales@arraynetwork.co.kr
+82(2)3461-8124

Taiwan
support.taiwan@arraynetworks.com
886-2-7718-2750

UK
infoeurope@arraynetworks.com
+44 (0) 7717 153 159



To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866 MY-ARRAY (692-7729) or authorized reseller.

Nov-2011 rev. b

© 2011 Array Networks, Inc. All rights reserved. Array Networks, the Array Networks logo, AppVelocity, NetVelocity, DesktopDirect and SpeedCore are all trademarks of Array Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Array Networks assumes no responsibility for any inaccuracies in this document. Array Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

XenApp, XenDesktop, Presentation Server, Metaframe and Citrix Receiver are all trademarks of Citrix Systems, Inc.
Apple and iPads are registered trademarks of Apple, Inc.
Google and Android are registered trademarks of Google, Inc.