



## DesktopDirect

---

### Remote Access for Business Continuity

Remote access for business continuity has requirements that far exceed traditional remote access. Learn why VPN will not scale in terms of security, cost, ease-of-use or performance and why remote desktop access is a superior choice for enterprise-class business continuity planning.

# TABLE OF CONTENTS

<b>Introduction</b>	<b>3</b>
<b>Considering the Risks</b>	<b>3</b>
Maintaining Compliance	4
Competitive Pressure	4
<b>The Enterprise Workforce</b>	<b>4</b>
<b>Remote Access Options for Office Workers</b>	<b>5</b>
<b>Remote Desktop Access for Office Workers</b>	<b>5</b>
Zero Service Interruption	6
<b>DesktopDirect – Remote Desktop Access for BCP</b>	<b>6</b>
Security	6
Cost	6
Productivity	7
Return on Investment	7
<b>Array Business Continuity (ABC) Pre-Paid Licenses</b>	<b>7</b>
<b>Summary</b>	<b>7</b>
<b>About Array Networks</b>	<b>8</b>

### Introduction

Unexpected business disruptions take many shapes and forms, spanning minor events to extreme disasters. Inclement weather, labor actions, cyber attacks or public health issues - no matter the nature of disruptions, they all have the potential to prevent employees from getting to their place of work.

Dealing with these disruptions requires business continuity planning (BCP) to avoid loss of productivity or revenue, and the planning must include a detailed remote access strategy. Traditional VPN solutions provide business continuity for executives, road warriors and home office workers, but there is not always time or budget to scale existing remote access solutions for the average office worker.

More significantly, existing remote access solutions are not necessarily the right answer for office workers, who make up the bulk of the enterprise workforce. Traditional VPNs, designed and built for those on the go, do not provide the same level of security, cost-effectiveness and productivity gains for office workers.

To understand why traditional VPNs are not ideal for augmenting remote access and enabling business continuity for office workers, we must consider the nature of disruptive events, the nature of the enterprise workforce and the critical deployment criteria that should be examined when evaluating remote access options for BCP.

According to 'Ten Remote Access Failures to Avoid in an Emergency' by Gartner analyst John Girard, "The most critical success factor to any business continuity plan is fast re-establishment of business processes. However, if your disaster recovery plans do not include remote access coordination steps, no amount of cool technology will save your operations."

### Considering the Risks

By the time disruptive events occur, it's too late to implement a business continuity solution and the result will be lost productivity and revenue. For example, during the 48-hour London Transit Strike of June 2009, unrecoverable business losses were estimated at \$164 million, according to the London Chamber of Commerce. A few years prior, Hurricane Katrina in New Orleans was another significant case of extreme disruption, displacing thousands of businesses throughout the Gulf Coast for months and causing undetermined revenue and productivity loss during recovery efforts.

Minor disruptive events also have the potential to prevent employees from getting to their place of work. These include snowstorms, electrical storms and power outages, flooding, wildfires, health alerts and transit strikes. During transit strikes in Los Angeles in 2000, New York City in 2005, Toronto in 2006 and London in 2009, hundreds of thousands of business commuters lost access to buses and trains for days, causing unrecoverable revenue disruption in respective local economies.


Most of these losses could have been avoided with BCP strategies that took into account the possibility that employees throughout the organization might need to work remotely. Even a cursory look at potential negative impacts to the bottom line makes it clear that BCP must be dealt with proactively, not reactively. Without protective measures in place, businesses will inevitably lose significant productivity and significant revenue.

### **Maintaining Compliance**

Regulatory compliance and government mandates require many companies to have secure, auditable access to key information, even during unanticipated events. Mandates like Sarbanes-Oxley, HIPAA and others remain in effect, even if an organization is working under less than ideal conditions. Consider a health insurance provider that suffers a business disruption that forces key employees to work from home. If those employees access sensitive data, HIPAA remains in effect and the company must be able to prove authorized access and that data leakage prevention mechanisms were in place. While audit trails and safeguards may exist at corporate headquarters, companies must also ensure they exist for employees accessing data remotely. Compliance is one reason government agencies now mandate credible BCP implementations for the private sector organizations with which they do business.

### **Competitive Pressure**

No company can afford to let inclement weather inhibit its ability to respond to customers, suppliers and other partners. For example, if a sudden snowstorm should rage on for days, competitors will likely capitalize on the effected company's lost momentum. Without a BCP implementation that automatically, securely and cost-effectively accommodates surges in usage, companies may find themselves expending unnecessary cycles and resources playing catch-up.



One of the great challenges in mitigating unexpected events is selecting the correct remote access solution. The solution must not only increase productivity while satisfying a full range of employee requirements, it must also cost-effectively leverage existing investments and address sudden usage bursts and in a way that requires no additional effort to implement.

## **The Enterprise Workforce**

The enterprise workforce consists of two main types of employees. The first type is the user on the go, for whom traditional VPN technology solutions were developed. These workers – typically executives, road warriors and home office workers – usually have corporate-issued laptops or PCs and are accustomed to working over the WAN.

These workers are the small fraction of the workforce that utilize remote access on a daily basis; for them, VPNs provide an adequate solution for ensuring business continuity during disruptive events.

The second type of employee is the office worker. These workers are situated in the office during the workday, usually sitting at their desktop PCs. When office workers are away from the office, they usually do not have access to a corporate device or to the corporate network. Moreover, when they use corporate applications, they are accustomed to a fast user experience – essentially LAN speeds. Because office workers do not have VPN accounts for remote access, they have no experience with remotely accessing corporate resources. Thus, office workers have very different remote access requirements as compared to traditional VPN users, especially in the areas of security, compliance, user experience and training.

### Remote Access Options for Office Workers

Two common ways to remotely connect office workers both involve using traditional VPN. The first option involves enabling office workers to connect to traditional VPNs from employee-owned PCs. This, however, opens up many problems associated with security, compliance, application availability, quality-of-experience and ease of use – all areas that are critical for the remote user to be productive.

For example, office workers connecting via VPN and employee-owned PCs could pose security risks to the network. Thus, they are unlikely to comply with corporate security policies and it is unlikely they will gain network access. There are other issues with using employee-owned PCs; for instance, they usually do not have the right corporate applications and getting these applications installed incurs significant license and helpdesk costs.

From a quality-of-experience perspective, office workers who are accustomed to LAN speeds could get frustrated and give up while working remotely over the WAN. Additionally, these workers' lack of experience with VPN solutions would require significant training and support to overcome inevitable login and navigation problems.

The second option involves traditional VPN connectivity from corporate-issued PCs and laptops, an approach that introduces significant security risks and significant costs associated with laptop deployment and support. First and foremost, there is the increased risk of theft or data leakage that results from laptop deployment. On average, 12,000 laptops per week are lost in US airports, and the annual average cost of data leakage in 2008 was US \$1.82 million per organization.

In addition to the security risks of laptops, quality-of-experience issues persist, as do the high TCO per laptop and the much higher training and support costs associated with traditional VPN deployments. Furthermore, because office workers make up the bulk of the enterprise workforce, IT must be highly conscientious about scalability when evaluating remote access strategies for business continuity.

### Remote Desktop Access for Office Workers

A third option for office workers involves innovative use of standard Remote Desktop Control (RDC) technologies. This concept, known as Remote Desktop Access (RDA), is ideal for office workers from all critical perspectives – security, cost and productivity. RDA provides effortless extension of compliance already on office desktops, and data sources are maintained on the corporate network, thus eliminating security risks.

RDA is implemented with existing technologies, no additional laptops or licenses are needed; moreover, RDA eliminates the need for IT to support multiple application environments per user. From a ROI perspective, RDA enables office workers to access their desktop from anywhere, as if in the office, providing immediate productivity without the need for investments in hardware, software or support.

RDA, however, is not without a few challenges. The large number of office workers – typically non-technical – demands centralized control, scalability, ease-of-deployment and an extremely intuitive user experience in order to avoid high training and support costs. There is also the need to prevent data leakage, which is amplified by a large number of users, and since RDA accesses desktop PCs, there is a need to ensure all users can access their PCs even when they are shut down.

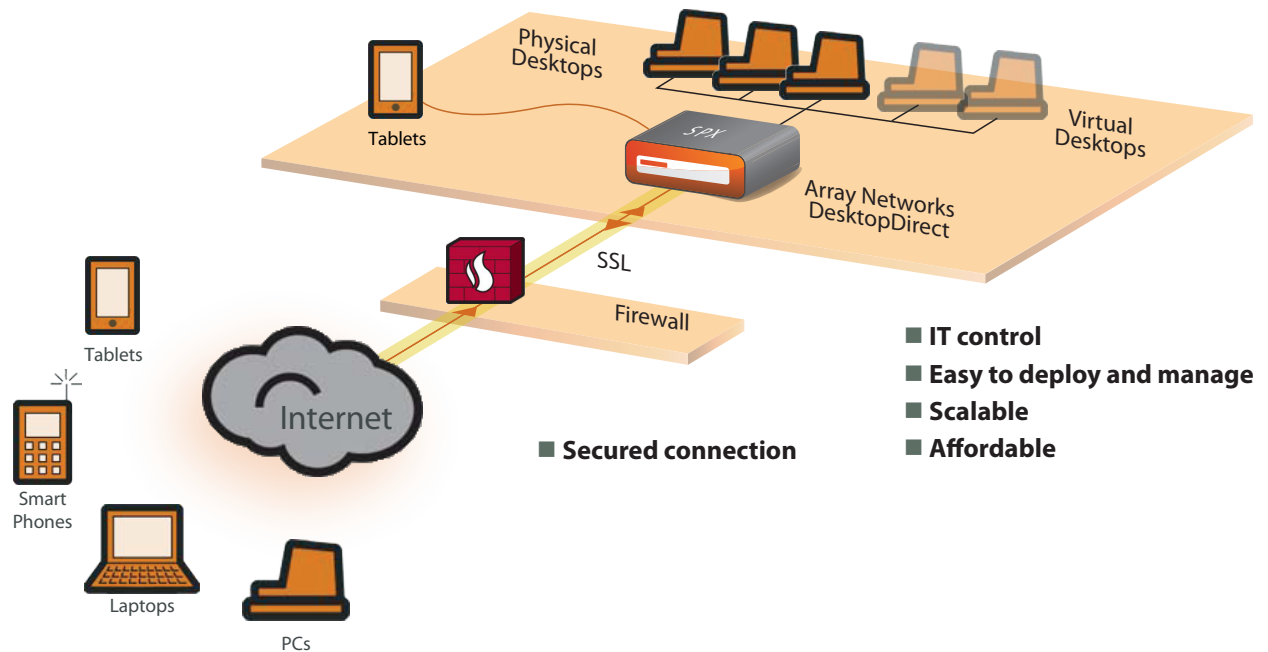
Thus, remote access for office workers is a balancing act between security, cost, and productivity and the ideal RDA solution will not require any compromises between these three requirements.

### Zero Service Interruption

In addition to a no-compromise RDA component, a proper remote access solution for BCP must also be able to work without IT intervention of any kind. That means the business continuity plan will not rely on employees being able to reach the IT department when a disruptive event occurs. And the plan will not assume that workers or IT will be able to add any additional hardware that may be required. To be truly effective, the business continuity plan must provide the capacity and performance required with no IT intervention and no downtime.

### DesktopDirect – Remote Desktop Access for BCP

DesktopDirect from Array Networks is the only complete BCP remote access solution developed specifically for office workers. DesktopDirect provides simple, secure access to Microsoft desktop environments, and its ease-of-use and straightforward, premise-based architecture make it an ideal solution that meets all RDA and BCP requirements without compromise.



### Security

DesktopDirect fully extends desktop compliance and its enterprise-class security capabilities make it ideal for BCP. Key features include industry-standard 256-bit AES encryption, FIPS compliance, integration with existing AAA architectures, real-time session control and data leakage protection. An on-premise hardware appliance with administrator-configurable data leakage protection, DesktopDirect enables administrators to provide business continuity for every office worker without introducing new attack opportunities.

### **Cost**

DesktopDirect is the most cost-effective BCP solution available today, as it relies on existing infrastructure (such as desktop PCs) and provides power management capabilities to reduce power consumption and deliver remote access in an eco-friendly manner. DesktopDirect's streamlined architecture and intuitive user experience also make it painless to deploy and easy to support, eliminating costly setup time and training costs. Packaged as a hardware appliance, Desktop-Direct delivers ROI in as little as six months, and enables a highly scalable architecture for the entire enterprise workforce, supporting up to 64,000 concurrent users on a single system.

### **Productivity**

DesktopDirect power management is capable of booting up powered-down desktop PCs, enabling office workers to access their familiar corporate desktop PC environment without having to remember to leave their PCs on at the end of the day. This is critical for BCP, as there is often no way to predict when the next snowstorm or other disruptive event will suddenly occur. DesktopDirect delivers full application transparency in a highly available clustered hardware platform, providing the industry's most consistent, high-quality user experience. DesktopDirect's extremely intuitive "click and work" login process with SSO eliminates the need for training, even for the most non-technical user.

### **Return on Investment**

Return on investment is a key measure of success for any IT department, and with DesktopDirect return on investment can be seen in as little as six months. During a recent snowstorm in the Northeast, a global top-7 financial services company used DesktopDirect to provide secure remote access to 12,000 office employees. At an average productivity of \$2,400 per employee per day, the financial services firm prevented the loss of over \$10 million dollars of productivity with no disruption to client services.

## **Array Business Continuity (ABC) Pre-Paid Licenses**

Array Business Continuity (ABC) Pre-Paid Licenses mean businesses always benefit from zero service interruption in the event of an emergency. The ABC Pre-Paid License enables additional users, beyond those covered under a day-to-day concurrent user license, to log in as needed, without any phone calls or other actions on the part of IT.

Each ABC Pre-Paid License provides 10 non-consecutive days of bursting capability. Customers predetermine the number of additional concurrent workers they will need to support in an emergency, and purchase an ABC Pre-Paid License that enables the DesktopDirect device to allow bursting up to that pre-determined number of workers. In the event of an emergency, users log on seamlessly, immediately access their office desktop PCs and get to work. For each day that bursting occurs, the remaining balance on the ABC Pre-Paid License decreases by one day. Because the ABC Pre-Paid License is loaded on the DesktopDirect hardware at the time of purchase or via upgrade, bursting is automatic when needed, without requiring any IT intervention.

### Summary

Coupled with ABC Pre-Paid Licenses, Array DesktopDirect delivers the industry's only comprehensive BCP solution for augmenting existing VPN remote access. DesktopDirect is the only Remote Desktop Access solution that enables office workers to immediately get to work during disruptive events, without forcing compromises on IT or the corporation as a whole.

DesktopDirect's security capabilities protect data, users and corporate resources, ensuring that providing BCP for the entire organization will not cause any new security risks. DesktopDirect's cost-effectiveness makes it the ideal solution for organizations concerned with adhering to budgets, remaining eco-friendly and maintaining a complete BCP architecture for the organization as it scales.

DesktopDirect's intuitive "click and work" login process ensures immediate productivity for everyone in the entire organization, regardless of location or technical expertise. Last but not least, Array Business Continuity Pre-Paid Licenses eliminate the need to react to disruptive events, delivering a smooth transition into and out of emergency situations so there are no losses in productivity or revenue.

### 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.com.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.

1) Gartner, November 2005 2) MSNBC, <http://www.msnbc.msn.com/id/31194425/> 3) CSI/FBI Computer Crime and Security Survey, 2008 4) Ponemon Institute, June 2008 5) McAfee and Data-monitor, April 2007