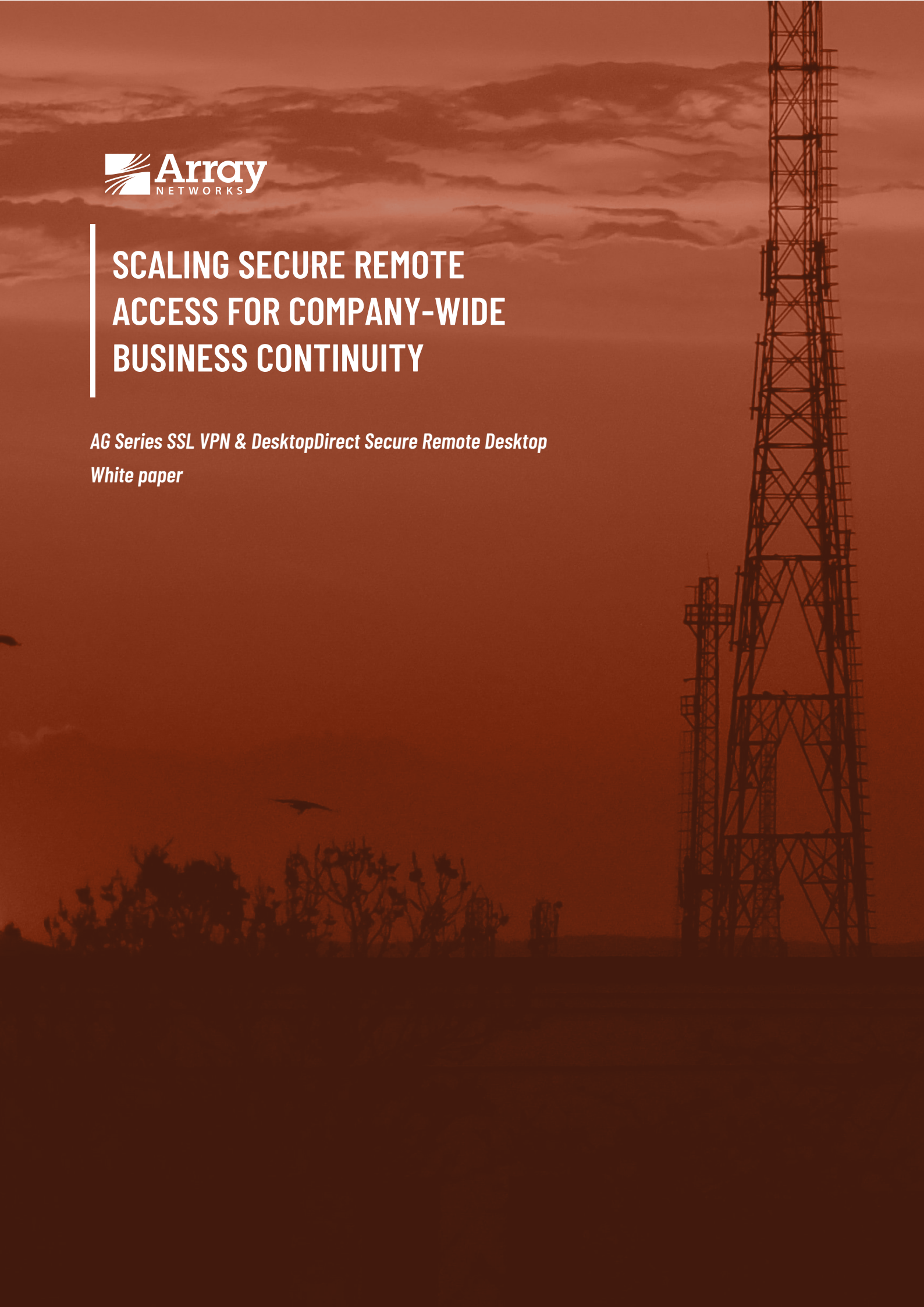


SCALING SECURE REMOTE ACCESS FOR COMPANY-WIDE BUSINESS CONTINUITY

AG Series SSL VPN & DesktopDirect Secure Remote Desktop

White paper

TABLE OF CONTENTS

INTRODUCTION

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

Dealing with such disruptions requires proper Business Continuity Planning (BCP) to avoid productivity and revenue loss. Proper BCP must include detailed remote access plans. Traditional VPN solutions typically provide business continuity for a portion of the workforce, but there isn't always time or budget to scale existing remote access solutions for the in-office employees in the event of business disruption.

More significantly, existing remote access solutions are not necessarily the right answer for in-office employees, who make up a large segment of the corporate workforce. Traditional VPNs, designed and built to support power users, do not provide the same level of security, cost-effectiveness, and productivity gains for in-office employees.

In order to understand why a traditional VPN is not an ideal BCP remote access augmentation strategy, we must consider the nature of disruptive events themselves, the enterprise workforce as a whole and its constituents, and the critical deployment criteria that should be examined when evaluating a solution.

"The most critical success factor to any business continuity plan is a fast re-establishment of business processes," according to Gartner analyst John Girard's paper, Ten Remote-Access Failures Your Company Could Avoid in Emergency. "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. The end result is lost productivity and revenue. For example, during the two week-long strikes by Bay Area Rapid Transit workers in 2013, the Bay Area Council estimated economic costs to the San Francisco Bay Area were conservatively $73 million a day. A few years prior, the Great Eastern Japan Earthquake and subsequent tsunami was another significant case of extreme disruption, death and devastation, displacing thousands of businesses throughout the entire area for months and causing undetermined amounts of lost revenue and productive time throughout the country.

Another potentially major threat to business continuity is global pandemics, such as the recent novel corona virus COVID-19. Similar to SARS, H1N1 and Ebola outbreaks, COVID-19 is already demonstrating the capacity to severely impact business operations. For organizations without an effective BCP remote working solution, the economic consequence of shelter-in-place, social distancing and lockdown orders will be substantial.

Minor disruptive events also have the potential to prevent employees from getting to their workplace. These include snowstorms, electrical storms and power outages, flooding, wildfires, health alerts, and transit strikes, among others.

1 "Ten Remote Access Failures Your Company Could Avoid in an Emergency" Girard, John; Gartner
2 "Bay Area Council Economic Institute Puts Economic Cost of BART Strike at $73 Million A Day" Bay Area Council, 2013

During the transit strikes of Singapore in 2012, Paraguay in 2013, and Philadelphia in 2016, hundreds of thousands of business commuters lost access to buses and trains for days, causing unrecoverable business disruption to respective local economies.

A great percentage of these losses could have been avoided with proper BCP implementations that account for the possibility that the employees throughout the entire company might need to work remotely. Even a cursory look at such negative impact on the bottom line makes it clear that BCP must be dealt proactively, and not in a reactionary manner – without a protective measure in place, businesses will inevitably lose countless hours of 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. Requirements like Sarbanes-Oxley, HIPAA and others still apply, 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. Should any of those employees access sensitive data that falls under HIPAA regulations, the company must be able to prove those employees were authorized to do so, and demonstrate that data leakage prevention mechanisms exist. While such audit trails and safeguards may be in place at the headquarters office, companies also need to ensure they apply to employees who access the data remotely. Compliance is one reason government agencies are mandating that the private sector organizations with which they do business be able to demonstrate they have credible BCP implementations.

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, unaffected competitors will likely capitalize on the affected 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 to play mere catch-up. The greatest challenge when an unexpected event occurs is to find a trustworthy, proven BCP augmentation solution that not only enables remote productivity while satisfying the full set of requirements for the employee base, IT, and the corporation as a larger entity; but also to find a solution that addresses sudden usage bursts in a way that cost-effectively leverages existing hardware investments, and requires minimal additional effort to implement.

The Enterprise Workforce

The corporate body consists of two main types of employees. The first type is the power user for whom traditional VPN technology solutions were developed. These remote employees typically have corporate-issued laptops or PCs, and are accustomed to WAN speeds. Additionally, power users typically access company resources from remote locations on a regular, daily basis. Power users, however, typically only make up a portion of the corporate employee base. For the mobile workforce, existing VPN solutions already provide an adequate solution for ensuring business continuity during disruptive events.

The second type of employee is the in-office worker. In-office workers are situated in the office during the workday, and sit at their desktop PCs. When they are away from the office, they use non-corporate PCs, and when using office applications, they are accustomed to the quality of user experience provided by the corporate network – they are used to LAN speeds. Because these workers do not have VPN accounts for remote access, they have no experience with remotely accessing corporate resources. Thus, they have very different remote access requirements than power users, especially in the areas of security/compliance, quality of user experience, and training needs.

Remote Desktop Access for In-Office Workers

The two most seemingly straightforward options for remotely connecting in-office workers both involve traditional VPN solutions.

Option 1 Involves enabling the in-office workers to connect to traditional VPN solutions from their personal devices. However, this opens up a host of 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, in-office workers attempting to connect via VPN could add security risks to the network. Thus, non-corporate PCs are unlikely to comply with corporate policies and may not gain network access.

There are other issues with using non-corporate PCs. Non-corporate PCs won't always have the right desktop applications, and getting these applications installed remotely would cost significantly in licenses and help desk support. From a quality-of-experience perspective, non-mobile workers accustomed to LAN speeds could get frustrated and give up trying to work remotely over the WAN. Additionally, non-mobile workers' lack of experience with VPN solutions would require significant training and support to overcome login and navigation problems.

Option 2 Involves traditional VPN connectivity from corporate-issued laptops. However, the security risks and costs associated with laptop deployment and support are significant.

First and foremost, there is the unnecessary increase in risk of theft or leakage of sensitive employee or financial data that results from laptop deployment. On average, 12,000 laptops per week are lost in US airports, and the annual average cost of a data breach (worldwide) in 2016 was $4 million USD .

In addition to the added security risks of laptops, there are the same quality of experience issues as in Option 1, the high TCO per laptop user, and much higher training and support costs associated with traditional VPN deployment.

Furthermore, because in-office workers make up a significant portion of the employee user base, IT must be highly conscientious about the scaling impact when evaluating remote access augmentation strategies for company-wide business continuity.

Remote Desktop Access for In-Office Workers

A 3rd option for in-office workers involves innovative use of standard Remote Desktop Control (RDC) technologies. This concept, known as Remote Desktop Access (RDA), is ideal for non-mobile workers from all critical perspectives -- security, cost, and productivity. RDA provides effortless extension of the compliance already established on remote desktops, and data sources are maintained in corporate offices, eliminating security risks. RDA is implemented with existing technologies, no additional laptops or licenses are needed, and RDA eliminates the need for IT to support multiple application environments per user. From a productivity perspective, RDA enables non-mobile users to work from anywhere, as if in the office, and provides immediate productivity without the need to duplicate application environments. In reality, there are challenges associated with RDA. The huge number of non-mobile workers, who are typically non-technical, demands centralized control, scalability, the need for easy deployment, and an extremely intuitive solution to avoid significantly higher training and support levels. There is also a need to avoid risk of data leakage, which is amplified by the large scale 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, it's a balancing act – security, cost, and productivity. The ideal RDA solution will not require any compromises between these three areas.

Zero Service Interruption

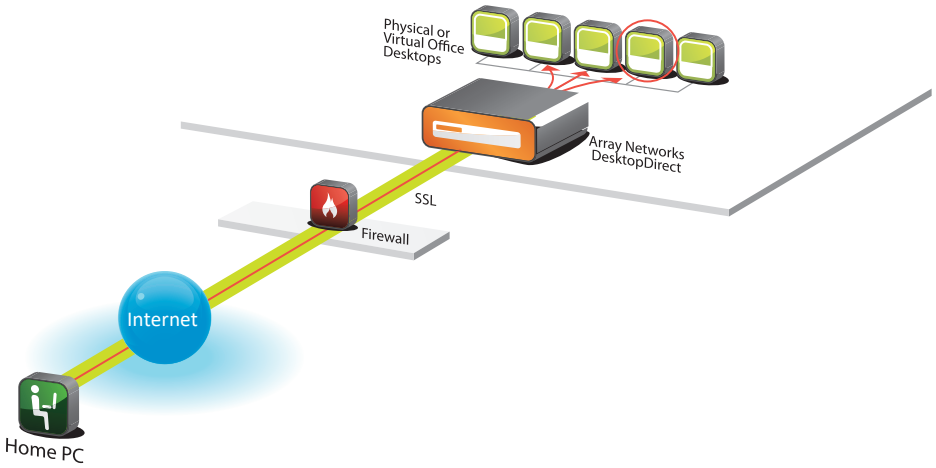
In addition to an ideal RDA component, a proper BCP solution must be able to work without IT help of any kind. That means the business continuity plan will not rely on employees being able to reach the IT department when a disruptive event occurs. And the plan will not assume that workers or IT will 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.

Meeting BCP Challenges with Array DesktopDirect

DesktopDirect from Array Networks® is the only complete BCP remote access solution for in-office workers. DesktopDirect provides simple, secure access to Microsoft desktop environments. DesktopDirect's ease of use and straightforward, premise-based architecture make it an ideal BCP solution for the in-office workforce. DesktopDirect™ alone meets all BCP requirements without compromises:

Security

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



Cost

DesktopDirect is the most cost-effective BCP solution available today, as it relies mostly on existing infrastructure (existing desktop PCs), and uniquely provides power management capabilities to conserve power and deliver benefits in an eco-friendly manner. DesktopDirect's streamlined architecture and intuitive user experience makes it painless to deploy and easy to support, eliminating costly setup time and high training costs. Packaged as a dedicated or virtual appliance, DesktopDirect delivers ROI in under a year, and enables a highly scalable architecture for the entire global non-mobile workforce, supporting up to 130,000 concurrent users on a single platform.

Productivity

DesktopDirect Power Management boots up even powered-down desktop PCs, enabling in-office workers to access their familiar office 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 consistently high quality of experience available today. DesktopDirect's extremely intuitive "click and work" login process with Single Sign-On (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 investment, 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 non-mobile employees. At an average productivity of $2,400 per employee per day our customer prevented the loss of over $10 million dollars of productivity with no disruption to client services.

Array Business Continuity (ABC) Pre-Paid Licenses

The Array Business Continuity (ABC) Pre-Paid License means customers always benefit from zero service interruption in the event of an emergency. The ABC Pre-Paid License enables additional users, beyond those covered under the day-to-day concurrent user license, to log in as needed, in some cases without any phone calls or other actions on the part of IT. Each ABC Pre-Paid License provides ten consecutive or 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 predetermined 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 or software at the time of purchase or via upgrade, bursting is automatic when needed, without any IT intervention required.

Conclusion

Coupled with the ABC Pre-Paid License, 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 in-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 BCP solution for organizations that have concerns with remaining eco-friendly and easily maintaining a complete BCP architecture for the entire organization as it scales. DesktopDirect's extremely intuitive "click and work" login process ensures immediate productivity for everyone in the entire organization, regardless of location or technical expertise.

Array Business Continuity eliminates the need to react to disruptive events, delivering a smooth transition into and out of emergency situations so there are minimal losses in productivity or revenue.

About Array Networks

Array Networks is a leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.