FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

Advantages of Appliance-Based Remote Desktop for Secure, Enterprise-Wide Remote Access and Mobility

A Frost & Sullivan
White Paper

www.frost.com

CONTENTS

INTRODUCTION

The effect of mobile devices on the modern workforce is undeniable. With the explosive growth of Apple and Android devices, average workers have unprecedented computing power at their fingertips. Consequently, these devices have found their way into the fabric of nearly all organizations and have opened the potential for employees to conduct work at any time from any location.

While the potential for increased connectivity and productivity is appreciated by employers, securing data as its flows outside the walls of the organization and beyond corporate devices is a difficult challenge. Staggering statistics around data breaches—26,935,587 records reported lost in 2010 alone[1]—and increasing fines associated with non-compliance have caused IT professionals and management to be rightfully cautious.

Many organizations are evaluating their options for tapping the potential of mobile access as well as supporting the broader requirement for increased remote access, only to find that solving these challenges is both difficult and expensive. What is desired are solutions that are secure, flexible, cost-effective, easy to deploy and compatible with the wide variety of configurations found in the wild.

Many secure access solutions excel at solving a slice of the remote access puzzle, but as mobility evolves, organizations must look at approaches that provide a more unified framework for supporting enterprise-wide remote access and mobility. This note explores one such technology—remote desktop access—highlighting the impact of mobility on security and drawing comparisons between remote desktop access and alternative solutions to illustrate the advantages of this approach and why it may be poised for resurgence in enterprise secure access.

THE EXPLOSIVE GROWTH AND DANGERS OF MOBILE DEVICES

The mobile device explosion has been in the works for a number of years. Increasing processing power and decreasing prices have made laptops appealing to both consumers and business users. For less than $1,000, organizations can equip employees with a laptop that is just as powerful as an equivalently priced desktop computer.

Tablet and Laptops are Dominant

In 2009, laptop sales outpaced desktop sales, heralding in a new era in mobile computing. Moving forward to the present, Apple and Google have continued to drive the demand for mobile devices.

The growth rates of mobile devices are staggering. Apple released the iPad in 2010, and as of June 2011 had sold 25 million units. This was only the start of the general acceptance of

[1] http://datalossdb.org/yearly_reports/dataloss-2010.pdf

tablets. Frost & Sullivan research predicts that tablet sales in 2011 reached 44 million units and by 2016 will grow to more than 215 million units.

Data Loss and Theft

Unfortunately, the move to mobile devices has increased the difficulty in securing data. As evidenced by the following data breaches, the problem is monumental:

- In 2006, a laptop was stolen from a database administrator's home. That laptop contained information for 26 million veterans. This was one of the first instances of lost records and remains one of the highest recorded breaches. [2]

- In 2009, a file containing identifying information for every physician in the country contracted with a Blues-affiliated insurance plan was on a laptop computer stolen from a BlueCross BlueShield Association employee. The file included the name, address, tax identification number and national provider identifier number for about 850,000 doctors.

These are only two examples of many serious breaches that have occurred due to employees taking data with them on mobile devices.[3]

Compliance Violations

Related to data loss and theft is the challenge of maintaining compliance. Whether mandated by industry or geography, there are few businesses not affected by regulatory or industry compliance directives. The requirements for data and client security are similar regardless of company size. As a result, even the smallest companies find the need to adhere to the alphabet soup of regulations. A list of notable examples of global regulations is summarized in Table 1 below:

Table 1: Security Regulations

Regulation	Objective	Regulated Entities
Health Insurance Portability and Accountability Act (HIPAA)	Protect patient personal health information (PHI) and personal identifiable information (PII) from misuse and improper disclosure	Any organization in the healthcare field, including but not limited to: clinics, hospitals, doctor offices, healthcare facilities in schools, pharmacies, insurers, and pharmaceutical companies
Payment Card Industry Data Security Standards (PCI-DSS)	Protect the private information of credit card account holders (account number, name, service code, and expiration date) from unauthorized disclosure	Physical and online retailers, merchants, and payment card processors and clearinghouses

[2] http://datalossdb.org/incidents/289-names-social-security-numbers-and-dates-of-birth-of-26-5-million-u-s-military-veterans-stolen

[3] http://datalossdb.org/blotter/536-laptop-theft-gives-850-000-doctors-the-blues

Regulation	Objective	Regulated Entities
Sarbanes-Oxley Act (SOX)	Protect non-public financial data and intellectual property (IP) from improper disclosure	All companies publicly traded in the U.S.
Gramm-Leach-Bliley Financial Modernization Act (GLBA)	Protect the security and confidentiality of client non-public personal information	Financial services firms, including banks, financial institutions, insurers, and security brokers
State data notification and privacy laws. Notable examples: California SB 1386 and Massachusetts Data Protection Law 201 CMR 17.00	Protect personal identifiable information (PII) as defined by the state	Organizations conducting business with customers in a covered state
Basel II	Protect non-public financial data and intellectual property (IP) from improper disclosure	Global financial services organizations, specifically internationally active banks
CJIS Security Policy	Protect data in the FBI Criminal Justice Information System	State and local government agencies accessing the FBI Criminal Justice Information System

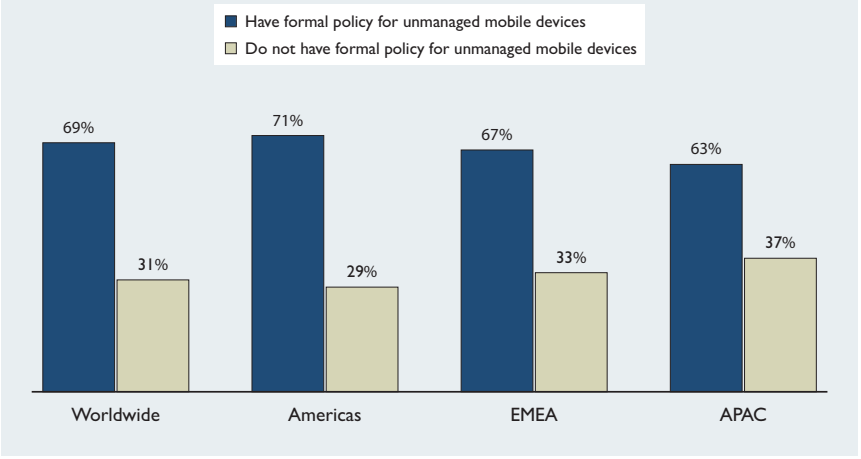
WHY TRADITIONAL APPROACHES TO MOBILE SECURITY ARE NOT ADEQUATE

Security professionals understand the risk of mobile devices to the organization. As seen in Figure 1, a 2010 survey of Information Security professionals illustrates awareness of this risk. Information Security professionals worldwide rated mobile devices as the number two threat to organizations. More eye-opening is the fact that 70 percent of professionals reported already having a formal policy in place for mobile devices, even if that policy is simply to disallow the use of unmanaged personal devices (see Figure 2).[4]

Figure 1: Top Risks to Organizations

[4] The 2010 Global Information Security Workforce Survey – www.isc2.org

Figure 2: Formal Policy around Mobile Device Usage



Frost & Sullivan believes that these findings illustrate not only the difficulty involved in securing mobile devices, but also the lacking nature of existing solutions. Below is a list of commonly implemented secure access solutions. Each one has at least one serious shortcoming that limits the effectiveness of the solution for enterprise-wide remote access and mobility.

Virtual Private Networks (VPNs)

A common approach to securing mobile device access is to leverage the organization's existing VPN infrastructure and provide the workforce with instructions for installing the VPN client on their mobile device. The key benefit of this approach is that it leverages existing technologies and infrastructure. Unfortunately, VPNs do not adequately solve the problem. Generally, the only data that is secured is the connection between the mobile device and the corporate network. The data itself is not secured and could be accessed, copied and lost.

The other challenge of simple VPN access is the availability of applications. The wide variety of mobile devices creates a situation where not every VPN or device has an available application. While many vendors are addressing this challenge, it will still exist for the foreseeable future. The only other options for enterprises are to either purchase and support duplicate application environments or create their own applications—a challenging and potentially expensive proposition.

In the end, an approach based on VPNs can deliver a highly productive user experience for a select set of users, devices and applications, but at significant expense due to security, mobile device management and the need to develop, purchase and support secondary application environments. Because data is allowed to reside on the device, data leakage can never be fully prevented.

Server-Based Computing

Server-based computing involves running applications in the data center and delivering them to client devices on demand. These virtual applications can be delivered to PCs either locally or remotely, and vendors such as Citrix and VMware offer client applications that make it possible to deliver applications to tablets and smart phones.

There are many advantages to the server-based computing approach:

- Any application that is running in the server-based computing environment can be made available to tablet devices, eliminating the need to develop native apps and support multiple application environments.
- Since end users are working directly on files and applications that reside in the corporate data center, the server-based computing client applications can be configured so that data never leaves the corporate network. With the ability to prohibit copy and paste, local printing and screen capture, the exposure of data can be limited and the possibility for data leakage can essentially be reduced to zero.

While server-based computing provides better mobile device security than VPNs, server-based computing has its challenges. Many enterprises have deployed server-based computing for key applications for key user groups, but very few have deployed server-based computing as the primary environment for users and applications across the organization. The cost of servers, software, licenses and deployment is steep, with most enterprises deploying server-based computing for no more than a small percentage of their overall workforce.

Virtual Desktop Infrastructure (VDI)

Similar to server-based computing, many organizations have also explored virtual desktops as another alternative. VDI promises reduced operational support and improved management from a centralized infrastructure and, as a result, numerous businesses have started VDI initiatives only to later discover that there are additional costs that can strain deployments: the cost of servers themselves, licensing fees, additional bandwidth and storage all add to the costs of a VDI deployment.

Endpoint Protection

Traditional endpoint security products are widespread and offer a longstanding history of protecting end users against virus threats. These solutions are being constantly updated against the latest threats and many of these products are available for mobile devices. Additionally, many endpoint security products have begun incorporating features such as endpoint encryption and content awareness to address the potential for data loss and theft.

Unfortunately, endpoint security products come with a lot of overhead. Since mobile users may spend days not connected to the corporate network, gaps may occur in coverage and the end user could still be susceptible to attack. The solutions themselves tend to cause overhead on the endpoint, and many newer mobile devices such as tablets do not have available solutions.

Endpoint solutions, while protecting against the virus threat, do not readily protect the data itself or the connections back into the organization's headquarters. What's more, by definition, it is impossible to support an endpoint protection strategy on unmanaged devices.

Mobile Device Management (MDM)

Mobile device management products can be deployed throughout an organization to manage the types of devices, applications, and actions that can take place on the network. Many organizations are turning to MDM products to ensure that only corporate-owned devices are allowed on the network, or to require that devices have a security policy readily available. Custom app stores are also another key feature of MDM products.

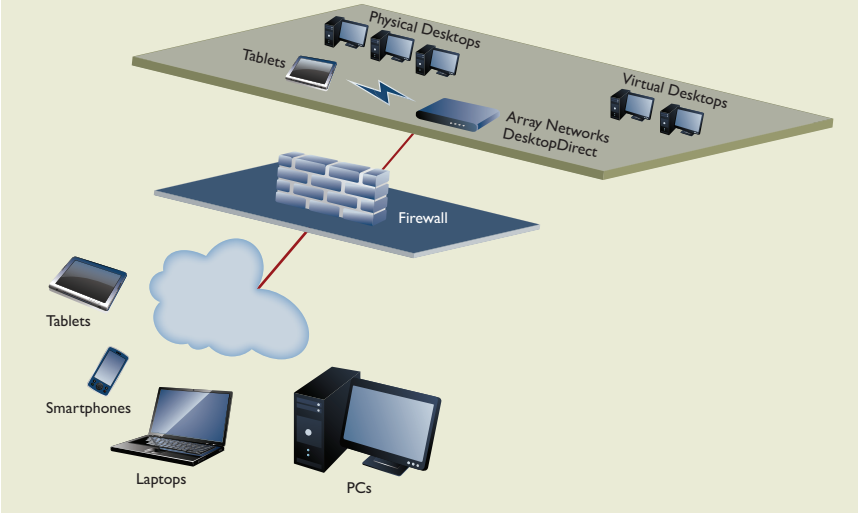
MDM products suffer from the same shortfalls as endpoint security products. Most MDM solutions are aimed to control devices on the network and user behavior around applications. Most MDM solutions are not designed to implement policies around data control.

APPLIANCE-BASED REMOTE DESKTOP ACCESS

Because no one solution fully addressed the needs for secure, enterprise-wide remote access and mobility, organizations' thought leaders are seeking out new approaches and alternatives. Interestingly, remote desktop—a technology familiar to many—may in fact be capable of providing a foundation for organizations to provide the accessibility and security necessary for mobile employees and the data they access.

One such solution is DesktopDirect, Array Networks' appliance-based remote desktop access solution. 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 leverages proven and scalable technologies to deliver a secure enterprise-class solution for remote desktop access and control (see Figure 3).

Figure 3: The Array DesktopDirect Solution



The DesktopDirect appliance is installed in the corporate network and integrates with directory services such as Active Directory, 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 location to their corporate or personal tablet.

Improved Security

DesktopDirect eliminates the need for client devices to even 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 concern, 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.

Increased Performance & Scalability

DesktopDirect runs on Array's high-performance line of AG Series hardware. Using customized hardware provides the power to tackle functions such as SSL bulk encryption and key exchanges. In addition to increased performance, up to 32 AG Series appliances can be clustered together, providing a high level of performance and scalability.

True Mobility

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 or smart phone environment without the risk of data leakage. Employees can use all of their existing Windows, Windows-based and proprietary applications without needing to re-purchase or port applications for new environments. 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.

Return on Investment vs. Alternative Solutions

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 less expensive as compared to competing secure access solutions:

VPN—DesktopDirect eliminates the need to purchase and manage new laptops enterprise-wide, providing both a better, more secure solution at a considerably lower price.

Server-Based Computing—DesktopDirect provides cost-effective access to office PCs and terminal services, providing similar functionality to more expensive solutions. Likewise, DesktopDirect can provide a more cost-effective approach to expanding existing server-based deployments and can reduce costs for customers with large deployments and the burden of annual licenses.

VDI—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.

Traditional Endpoint—DesktopDirect addresses the challenges associated with data leakage more effectively than traditional endpoint security products. Organizations still rely on their approved and updated endpoint protection installed on the user's desktop, ensuring continued updates and protection regardless of location.

MDM—DesktopDirect eliminates the need for organizations to control user devices. Since the original policies installed on the desktop still hold true, there is no need to change the end-user device. DesktopDirect also facilitates a secure BYOD environment, allowing the organization to take advantage of this trend.

CONCLUSION

Mobile devices have forever changed the business landscape. Even though devices such as smart phones and tablets are relatively new to the market, their effect on the workforce has been dramatic. These changes are a fact of life for organizations moving forward; thus, providing enterprise-wide remote access and mobility, and security for corporate data as it flows outside the walls of the organization and beyond corporate devices is paramount.

Although many solutions excel at solving a slice of overall secure access challenges, none have proven to have the legs to provide a broader framework for enterprise-wide remote access and mobility. Whether it is VPNs, server-based computing, VDI, MDM or traditional endpoint security solutions, organizations still find themselves confronting the challenges of cost, complexity and the prospect of losing sensitive corporate data. In the search for a better alternative, appliance-based remote desktop has surfaced as an approach the combines the best aspects of security, application support and device support with a framework that is both simple and cost-effective.

Array's DesktopDirect solution provides a unique alternative for organizations seeking to address the challenges of mobility and security. By providing a window into the secure desktop environment, DesktopDirect allows users the ability to stay productive regardless of where they are, while providing the organization the ability to ensure their data is safe and secure, protected by the safeguards already in place. Relying on proven technology, DesktopDirect provides a bridge that leverages the dedicated infrastructure that companies have already invested in to solve the challenges of enterprise-wide remote access and mobility.

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

Auckland
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Dhaka
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Mexico City
Milan
Moscow
Mumbai
Manhattan
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC