White Paper

Mobile Access to Business Applications

AG Series Secure Access Gateways & DesktopDirect

Introduction

Smart mobile device adoption continues to increase globally. In 2019, smartphone shipments are projected to exceed 1.8 billion units[1], and tablets to surpass 180 million[2]. A proven winner in the consumer market, smartphones and tablets have made significant inroads in the enterprise due to their portability and their ability to provide instant access to applications and information in a broad range of business situations.

For example, it is not practical for a doctor on the move between exam rooms, rounds and clinics to carry a heavy laptop that is constantly starting up, connecting, sleeping or shutting down. In contrast, a smartphone or tablet is highly portable and provides an always-on experience with information and applications immediately available at the doctor's fingertips. This ability to enhance worker productivity and improve quality of work gives smartphones and tablets the potential to foster tremendous growth in the enterprise through improved worker productivity and availability.

The consumerization of IT is under way. Workers want smartphone and tablet access to business applications, often from their own personal devices. However, VPNs are not a complete solution for secure mobile connectivity. Remote desktop access is a more secure, less expensive approach to smartphone and tablet access to business applications and data that is easier to deploy, manage and use.

Smartphone & Tablet Deployment Challenges

Initially designed as consumer devices, smartphones and tablets faced significant challenges to becoming full-fledged solutions for business productivity. Chief among them are security, application availability, device management, cost and time.

Security

First and foremost is security. Consider the cost and effort necessary to ensure the security of SSL VPN access: laptops, client software, anti-virus, anti-spyware, hard-disk encryption, multifactor authentication and the list goes on. The thought of a similar scenario driven by the influx of personal or business-owned smartphones and tablets in the workplace can seem daunting. What's more, smart device access is complicated by Bring Your Own Device (BYOD), the desire of many workers to use their personal device. Personal devices and content can create a lot of problems; for example, running standard VPN clients on a smartphone or tablet can change device behavior – a scenario that employees will not accept and which will create additional burden for IT. Further, personal devices are more likely to be lost or stolen, and create a situation where music, pictures and personal content resides on the same device as confidential enterprise data.

[1] IDC: Global smartphone shipments forecast from 2010 to 2020

[2] IDC: Shipment forecast of laptops, desktop PCs and tablets worldwide from 2010 to 2020

As IT attempts to protect corporate data without disturbing personal data, significant risk can result if security is traded to achieve a more user-friendly experience. Unfortunately, the organizations that stand to gain the most from the benefits of smartphone and tablet access, such as financial services and healthcare, are the same organizations that stand to lose the most in the event of data leakage.

Application Availability

Tablets access the Internet, run consumer apps and without too much trouble can be configured to provide access to corporate email systems. Out of the box, this is about the extent of a tablet's capabilities for conducting business. Tablets typically don't run Windows, or any of the business applications developed for native Windows. This is to say, there is a large gap between what employees are accustomed to using and what is available on tablets. There are certain native apps that can be purchased, but since tablets are often private devices, it doesn't make sense to re-purchase apps that are already available on employee desktops. Additionally, because tablets are consumer devices, employees will commonly switch from one platform to another, increasing the number of application environments that must be purchased, deployed and managed.

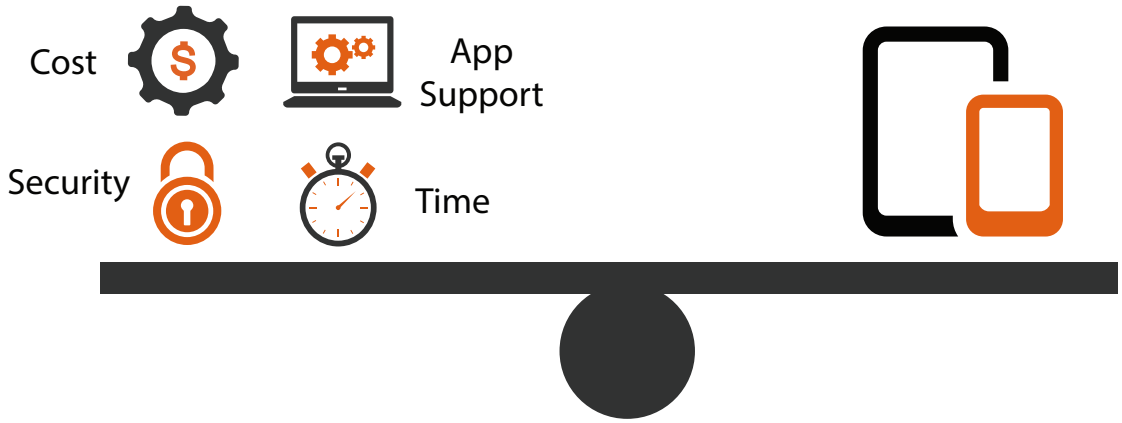

Figure 1: Balancing smart device access versus corporate concerns

Device Management

In organizations deploying a form of managed smart devices, IT typically looks at different solutions for Mobile Device Management (MDM) to deal with the issue of security and lost or stolen tablets. While remote wipe and reset capabilities are available, personal data on devices can be a problem if it causes the enterprise to take responsibility for the backup and restore of personal data. As with security, without any real alternatives, IT is forced to spend a considerable amount of time and money locking down and managing this new class of device. For those organizations opting to support a BYOD strategy, unmanaged devices cannot go completely unmanaged; organizations must still determine an approach to providing limits on personal smart devices, without impacting their usability as a consumer device.

Cost

As with any business or IT investment, benefits and gains must outweigh costs. While executives and employees may be clamoring to use the latest and greatest technology, or the benefits of smartphone and tablet access may be clear, in the end, costs must be factored in and the solution must make business sense. Considering the challenges posed by security, application access and device management, the cost consideration is not trivial and can include duplicate application environments, duplicate security environments, development of native applications and investments in server-based computing, not to mention the costs of the smartphones and/or tablets themselves, should an organization decide to deploy managed devices.

Time

Last is the challenge of time. Security, application availability and device management challenges not only impact cost, they also introduce significant barriers to deploying smart device access in a timely manner. Developing native apps and installing new application infrastructure can take months, as can bringing together all the pieces necessary for successfully delivering enterprise applications to smart devices. Organizations are well advised to allocate sufficient time for implementing a smart device strategy and to seek out more efficient alternative approaches to mobile application delivery.

Approaches to Smartphone & Tablet Access

To determine the best approach or mix of approaches for any organization, it is necessary to evaluate the pros and cons of all solutions and compare them against the needs of the particular business. Three common approaches for providing smartphone and tablet access to corporate resources and applications are the use of SSL VPN and native applications, server-based computing and managed services.

VPN & Native Apps

A common approach to smartphone and tablet access is to leverage existing VPN infrastructure and provide the workforce with instructions for installing the VPN client on their mobile device. The benefit here is that it is a fast, down and dirty way to enable smart devices in the enterprise, at the extra cost of new licenses and additional appliances. However, these VPN clients are intrusive apps, and installing them on private devices can cause potential instabilities and support problems that are not acceptable.

Security is another drawback of this approach. In its most basic implementation, the only thing that is secured is the connection between the smartphone or tablet and the corporate network. Like a laptop, a smart device is able to download, store, copy, paste and send all the data it wants; unlike a laptop, it is not managed and is far more likely to get lost or stolen. This opens the door to other challenges such as the cost and complexity of purchasing corporate-owned and managed devices, or investing heavily in mobile device management software, or both.

The other challenge of simple VPN access is application availability. Tablets and smartphones may not run Windows, and neither may support most enterprise applications. This creates a significant gap between the use of smartphones and tablets as consumer devices and their use for business. To close

this gap, organizations are turning to developing or purchasing native applications, in essence creating a duplicate application environment specifically for smart device access for a select number of core applications.

A benefit of native apps is that they can be developed from the ground up for usability on a mobile platform. This is an important consideration, as applications will differ as to how well they behave in the mobile environment. There are, however, downsides and limitations to developing native apps. For one, it is time consuming and expensive to develop and support multiple application environments. Considering the number of applications in use in the typical enterprise, developing or purchasing native apps may not make sense beyond a core set of business-critical applications. Secondly, developing or purchasing native apps might lock enterprises into specific smart device platforms, eliminating the ability to support a flexible BYOD strategy.

In the end, an approach based on VPNs and native apps can deliver a highly-productive user experience for select applications, but at significant expense due to security, mobile device management and the need to develop, purchase and support secondary application environments. Also, because data is allowed to reside on the smartphone or tablet, data leakage can never be fully prevented; moreover, native apps are not aligned with a flexible BYOD strategy as they require organizations to develop to specific platforms.

Server-Based Computing

Server-based computing runs applications and desktops in the data center and delivers them to client devices on demand. Just as these virtual applications and virtual desktops can be delivered to PCs either locally or remotely, today, providers of server-based computing offer client applications that make it possible to deliver applications to tablets and smartphones.

Advantages of the server-based computing approach are multifold. First, any application that is running in the server-based computing environment can be made available to smart mobile devices, eliminating the need to develop native apps and support multiple application environments.

Second, because end-users are simply manipulating files, applications and desktops that reside in the corporate data center, the server-based computing client app can be configured such that data never leaves the corporate network. With the ability to prohibit copy and paste, local printing and screen capture, and without the possibility of corporate data residing on smartphones or tablets, the possibility for data leakage can essentially be reduced to zero.

On the other hand, while many enterprises have deployed server-based computing for key applications for key user groups, 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 simply too steep, resulting in most enterprises deploying server-based computing for no more than a small percentage of their overall workforce.

In short, while this approach can be highly-secure and highly-flexible for users and applications already supported by server-based computing, the time and expense required to extend the solution enterprise-wide makes it highly impractical.

Managed Services

Many providers of managed services for remote desktop access now tout the ability to access desktops and applications using smart mobile devices. In theory, providing smartphone and tablet access to office desktops using remote desktop technology makes a lot of sense. If the service provider provides controls for managing end-points and disabling copy, paste, print and screen capture, and the user is simply operating his or her primary work environment using a remote device, data will not be able to leave the corporate network.

What's more, because users are accessing their primary work environment, they have access to the full range of applications they require to be productive. Because the solution leverages existing infrastructure, and because service providers offer support for a wide range of devices, the managed services approach is relatively cost-effective and at the same time can support a BYOD strategy.

In reality, however, enterprises are not comfortable exposing sensitive data and the enterprise network to a third party. For these managed services to function, thousands of permanent connections must be established from the corporate network to a broker on a third party network – a network that supports many other businesses as well as individual consumers. Enterprises have been unwilling to use these services to provide remote access to office PCs from traditional devices such as home desktops and laptops, and in all likelihood will have the same apprehensions about using managed services to provide tablet and smartphone access to corporate applications.

Comparing the three approaches, no single solution provides a perfect combination of data leakage prevention, application availability, affordability and usability. Enterprises will either have to select a solution that is the best fit for their particular environment, or look beyond these three solutions to find a new approach that eliminates the trade-offs between security, application availability, cost and usability.

DesktopDirect – A New Approach to Smartphones & Tablets for Business

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

In a smart mobile device access environment, the DesktopDirect appliance is installed in the corporate network and integrates with Active Directory (or similar) to establish user credentials for secure access. 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 (ART). For smartphone or tablet access, users download a free app from an App Store, App Marketplace or similar to their corporate or personal device. From there, users launch the DesktopDirect application, log in using their single sign-on credentials, and make a selection from their list of registered desktops.

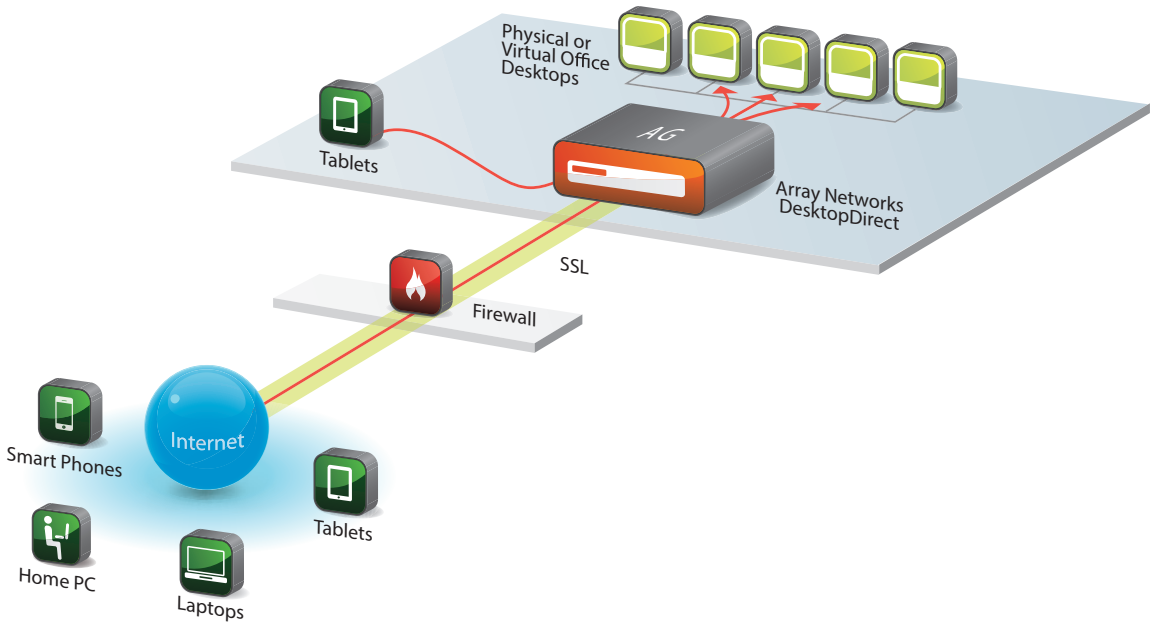

Figure 2: Typical AG Series and DesktopDirect deployment

- Data Leakage Prevention – DesktopDirect is a dedicated or virtual appliance-based solution that is enterprise owned and operated. Unlike managed services, DesktopDirect is under full enterprise control and does not open the corporate network to third-party networks. DesktopDirect also ensures that mobile devices never become a part of the corporate network; because end-users merely use their mobile device to control their office desktop, data never leaves the corporate network and cannot be left behind on tablets or smartphones. Connectivity from the DesktopDirect appliance to end-user devices is encrypted using SSL, and controls for copy, paste, print and screen capture eliminate any remaining chance of data leakage.
- **Full Application Availability** – DesktopDirect leverages existing desktop, application and security infrastructure. Unlike server-based computing, a traditional and familiar PC work environment is provided to nearly all employees. Without any need for new hardware or software, licenses or application environments, employees enterprise-wide can be provided with full application availability.
- **Time & Expense** – As compared to the time and expense of developing native applications or deploying server-based computing, DesktopDirect is highly cost-effective. Unlike managed services that charge indefinitely, right-sized DesktopDirect hardware and software license packs are an affordable one-time purchase. DesktopDirect can be set up in as little a few hours and is capable of achieving ROI in the time it takes just to set up alternate solutions.

- **Usability** – While DesktopDirect cannot provide the user experience of a dedicated native application, it goes a long way toward creating a PC-like experience for smartphones and tablets that retains the usability of office applications. Wake-on-LAN (WoL) capability allows office-based laptops and desktops to be powered down at night, over the weekend or anytime they are not needed, and powered up remotely by users via their smart devices.

Figure 3: DesktopDirect allows enterprises to enhance business productivity without compromising security

By deploying DesktopDirect to enable smartphone and tablet access for employees, enterprises get a cost-effective solution that is fully secure and fully under IT control and at the same time provides full application availability, supports a BYOD strategy and is simple to deploy, manage and use. What's more, DesktopDirect simultaneously creates a remote access solution for productivity and business continuity, allowing users to log into their office desktops from any remote device, anywhere.

	VPN & Native Apps	Server-Based Computing	Managed Services	DesktopDirect
Data Leakage Prevention	Fair	Excellent	Fair	Excellent
Application Availability	Fair	Excellent	Excellent	Excellent
Time & Expense	Poor	Poor	Fair	Excellent
Usability	Excellent	Fair	Fair	Good

Summary

Selecting the right approach to providing smart mobile device access may not be an either/or proposition, but might, in fact, include a mix of the approaches outlined in this document. For instance, a particular application may not translate well from a PC environment to a smartphone or tablet environment, and the decision is made that a native application must be developed. Or an application is so essential to the core business that getting the best possible user experience is worth the expense of developing a native app. Likewise, organizations with a large investment in server-based computing will still want to make these resources available to tablet and smartphone users.

DesktopDirect is equally at home providing a full mobile access solution or working in conjunction with alternate approaches to smart device access. If an enterprise has hundreds of applications, native apps may be developed for five to ten of them, with DesktopDirect providing a catchall to provide secure smartphone and tablet access to the remainder of the organization's applications. Or, the rapid nature of deploying DesktopDirect can be leveraged to provide smartphone and tablet access to critical applications while a native app is under development. Because DesktopDirect supports access to both physical and virtual desktops, organizations can quickly and cost-effectively deploy a secure mobile access solution that incorporates their investment in server-based computing.

Ultimately, each organization has to bear in mind their requirements for data leakage prevention, application availability, time and expense and usability and select the approach or combination of approaches that best meets their business needs and provides the strongest ROI for their environment.

About Array Networks

Array Networks is a global 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 headquartered in Silicon Valley, is backed by over 250 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, IDC 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

EMEA
rschmit@arraynetworks.com
+32 2 6336382

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

France and North Africa
infosfrance@
arraynetworks.com
+33 6 07 511 868

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

Japan
sales-japan@
arraynetworks.com
+81-44-589-8315

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

Mar-2017 rev. a