Meeting the expectations of an increasingly mobile workforce has created a host of new security challenges for IT organizations. Enterprise employees now insist on using the devices of their choice for remote access, putting the burden on IT to implement granular and adaptive security and access policies and to deploy tools that protect mobile devices and data.

It’s a huge challenge, not only because the ecosystem of mobile devices and applications continues to grow, but also because remote workers have moved far beyond merely accessing their email and calendars from their smartphones and tablets. Today enterprise employees want to access business-critical data and applications from their mobile devices no matter where they are.

However, mobile networks have lower data transfer rates than Wi-Fi or wired networks, and lower processing power on mobile devices means performance issues for many traditional software applications being accessed remotely. The data, therefore, has to be optimized specifically for mobile networks and devices. Further, traditional remote access solutions do not adequately address security risks related to BYOD and mobile devices.

Given all these complexities, it’s not surprising that some organizations grant only limited access to company resources from a mobile phone/tablet. Less than one-half of respondents to a recent Computerworld survey allow users access to company resources from mobile applications other than email, contacts and calendar. Only 41 percent of organizations let mobile users connect to office productivity applications from a mobile device, while just about one-third give remote access to the company virtual private network (VPN), shared files and file servers, or cloud-based business applications.¹
MOBILE VPN AS A BUSINESS IMPERATIVE

Simply avoiding mobile security isn’t a viable IT or business strategy, especially when the right remote access management tools can enable an enterprise to leverage the numerous benefits of mobile technology, such as increased productivity, collaboration, flexibility and agility.

Many enterprises deploy mobile application management (MAM) and mobile device management (MDM) solutions, and there is growing interest in the mobile virtual private network (mVPN), which is driving new growth in the overall Secure Sockets Layer VPN (SSL VPN) market.

The problem is that traditional VPNs: 1) were not developed for handling and optimizing mobile data; 2) have scalability issues; 3) require separate remote-access points (multiple URLs) for different devices, different locations (home, office or public) and different resources being accessed; and 4) were not designed to deliver Web 2.0 and SaaS enterprise applications. Further, MDM/MAM solutions do not always integrate well with current applications or with traffic management and traditional VPN solutions.

What’s needed today is a delivery network that is seamlessly integrated with an MDM/MAM solution and that also enhances the traditional SSL VPN solutions by addressing both mobile VPN and security needs, while incorporating centralized policy management.

“The challenge is to provide security while still giving the user a choice in terms of what devices and operating systems they use,” says Steve Shah, vice president of product management, Citrix.

WHERE TRADITIONAL VPN SOLUTIONS FALL SHORT

As employees demand the same flexibility and convenience in the workplace as in their personal lives, IT is on the hot seat to provide quality user experiences on mobile devices — from self-provisioning to single sign-on to easy-to-use mobile applications. This requires IT to reexamine the data center approach and move beyond the constraints of fixed locations and standard PCs to deliver all the applications required for true mobility, including mobile, SaaS, Web and virtual desktop infrastructure (VDI).

The use of single sign-on capabilities, for example, can reduce the hassle of multiple authentication checkpoints across different applications that reside in public, on-premise and hybrid clouds.

At the same time, many IT departments struggle with implementing security controls on mobile devices, especially the employee-owned ones, and applications accessed by these mobile devices. The challenge is to access the security posture of any mobile device and implement relevant security and access policies specific to that device.

Traditional remote access solutions — with multiple access points for multiple applications — can’t adequately address the needs of a highly mobile workforce requiring easy and secure application, desktop and data access from anywhere, on any device. It is also very hard to ensure uniform access policies implemented across multiple access points at the same time. Further, these traditional remote access solutions fail to mitigate the risks of providing anywhere access, while increasing the potential for data leaks.

Simply installing applications directly on users’ mobile devices can raise serious security, privacy and compliance risks because users may not exercise judicious security measures on their personal mobile devices. Therefore, IT must be able to provision and de-provision applications of all types quickly, whether to provide new resources or to cut off access when it is no longer needed or appropriate.

REAL REMOTE ACCESS USE CASES, REAL PRESSURES

Today an organization’s secure remote access strategy must account for a much larger and far more diverse population of users and devices requiring highly reliable access to a broader spectrum of resources — including enterprise Web, mobile, cloud and client-server applications; hosted desktops; and data.

Consider these business use-case scenarios and the pressures that mobility places on the IT organization.

1. Deliver corporate applications to a mobile user over SSL.

Organizations need complete coverage for all users, devices, applications and data — all the time. For instance, administrators need to constrain or expand the degree of access provided to align with the trust level of each access session. If a user’s location and device are less trustworthy, such as an airport kiosk, then access needs to be limited to a handful of low-sensitivity resources. If, however, the user is at home on a corporate laptop, then there must be a policy that can dynamically allow access to additional applications and services. IT administrators need to provide mobile users with a secure tunnel that is constrained to a single application and avoids the need to provision full network-level access to potentially compromised devices.
“A mobile VPN solution should enable a seamless user experience that helps people stay productive from anywhere, while delivering secure access to any application for any user, anywhere, on any device.”

— Graham Melville, senior director of product marketing, Citrix

2. Integrate with MDM/MAM appliances to gauge the security posture of mobile devices. Enabling remote access for any user and device to any resource is reckless if it cannot be done in a fully secure and tightly controlled manner. It must be able to verify the identity of corporate-owned, personal and jailbroken devices and determine compliance with organizational security policies, such as the installation of operational and up-to-date antivirus and personal firewall software.

3. Monitor and provide visibility of data. IT administrators require complete end-to-end visibility to all network traffic passing through gateway devices, including granular reporting on users, desktops and applications such as app usage, desktop usage, session reporting, bandwidth consumed, active sessions or latency.

4. Embrace and enable BYOD. Many enterprises still remain hesitant to support employee use of personal mobile devices. Mostly because of the shortcomings in the current solutions to handle any device, customers worry about data security and privacy issues. They are also concerned with buying a solution just for meeting BYOD requirements, and that means spending lot of money and allocating IT resources just to manage mobile devices. Yet BYOD is now an undeniable reality of enterprise life — with or without IT support. It simply is too late to bar executives, salespeople and other enterprise employees from using the devices of their choice, so organizations must find a way to deal with the BYOD devices already in their environments without increasing risk. Fortunately, 70 percent of IT leaders say they have a BYOD strategy and road map in place, according to IDG Research.² They recognize IT needs to deliver applications to any device, anywhere, over any connection, while empowering users to work easily, securely and seamlessly across any type of device, regardless of ownership.

However, only 11 percent of IT leaders in the same study say they have fully integrated mobile security and management with infrastructure.³ To meet the varying requirements for secure mobile application access, several vendors have introduced both mobile VPN and SSL VPN products. However, many of these mobile VPN/SSL VPN products do not sufficiently address today’s mobile requirements, nor do they provide seamless and secure access. Unless products are closely integrated, key ease-of-use features such as single sign-on, single management UI, granular policies for end-user mobile applications, and easy onboarding of user devices are not possible. Also, the use of an SSL VPN solution for remote access extends the secured network to unsecured, remote devices, thus increasing risk.

AN EFFECTIVE MOBILE VPN SOLUTION SHOULD WORK FOR EVERYONE

In today’s digital workplace, a mobile VPN solution must satisfy both user and IT requirements. Mobile workers require anywhere access to business applications and data, while IT administrators need a high level of control to protect sensitive organizational data and corporate content. IT administrators also need simplified management and flexible deployment options — to quickly and easily deploy and retire applications to accommodate fluctuating business demands without compromising the security of other applications or the network.

Key features and capabilities of an effective mobile VPN or next-gen SSL VPN solution should include: integration with an MDM/MAM solution; security of devices, applications and data; scalability to accommodate an increasing number of devices and applications; visibility of application traffic for monitoring, troubleshooting and planning future application infrastructure; and one URL for end users.

Consider the benefits:

- **End users** enjoy a single, seamless point of secure remote access and single sign-on capabilities to all of their applications and data, allowing them to easily roam across devices and networks without losing their current session.
- **Administrators** benefit from a single point of control and visibility, plus tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise.

“A mobile VPN solution should enable a seamless user experience that helps people stay productive from anywhere, while delivering secure access to any application for any user, anywhere, on any device,” says Graham Melville, senior director of product marketing, Citrix.

The bottom line: Mobile VPN has become a business and technical imperative. It streamlines business operations with easy manageability and lower capital and operating expenses. It also provides a better and more consistent user experience, centralized management of security and application policies, and improved security.

CITRIX: AN END-TO-END SOLUTION

Citrix is the only vendor to provide a complete end-to-end solution including:

- **Virtual desktop infrastructure and virtual applications**: Citrix XenDesktop and Citrix XenApplication provide virtual desktops and virtual applications to users over a cloud, office LAN or from home wireless networks.
- **MAM/MDM**: Citrix XenMobile incorporates MicroVPN technology, which provides secure access from native mobile applications to content hosted in the data center through app-specific VPN connections.
• **Delivery network**: Citrix NetScaler™ with Unified Gateway provides users with secure remote access to business applications deployed in the data center or a cloud across a range of devices including laptops, desktops, thin clients, tablets and smartphones.

• **Collaborative applications**: The suite of integrated productivity applications like Citrix ShareFile and Citrix GoToMeeting work together.

Citrix NetScaler with Unified Gateway solves the challenges of delivering a modern, secure remote access infrastructure by offering enterprises a next-generation solution that unifies the capabilities of traditional SSL VPNs along with modern Application Delivery Controllers and mobile VPNs. NetScaler with Unified Gateway provides users with always-available, high-definition and single point of access to the resources they need wherever, whenever and on whatever device they choose to work. IT, in turn, gains a unified solution for meeting security and remote access requirements for any type of application, now and in the future.

The advantages of using Citrix Netscaler with Unified Gateway include:

• **Single point of access**: One URL for end users to access corporate applications and resources.

• **End-to-end policy management and control**: Restricts application access for unauthorized users.

• **Unparalleled visibility**: IT administrators have a view into the network and applications, wherever they reside (mobile devices, hosted virtual desktops, the cloud, etc.).

• **Reduced TCO**: A single, unified solution meets all of the organization’s secure remote access needs.

• **Improved security**: IT gains centralized, granular and dynamic control of access to essential systems, applications and data.

• **Better user experience and improved productivity**: Users have the flexibility to get work done on their terms — from anywhere, using any device type.

• **Faster response times**: Less time is required to fulfill new requests for remote access services and resolve network and application issues.

NetScaler with Unified Gateway provides an end-to-end secure access solution for applications, desktops and data delivered by XenDesktop, XenApplication and XenMobile, and addresses the requirements of security teams, network architects and server administrators. Additionally, NetScaler MobileStream™ optimization technology improves the delivery of data and applications on mobile devices to optimize mobile streaming.

IT administrators gain granular application-level and device-level policy and action controls over access to corporate content, while users can work from anywhere. Simplified management and deployment options enable IT to easily manage and secure user access to corporate resources regardless of device or location. Security features such as SmartControl, End Point Analysis and XenMobile MicroVPN enable tight, policy-based control and compliance with corporate and government security requirements.

Read more [here about Citrix’s Netscaler with Unified Gateway](#)