Connecting the Untethered Employee

Organizations want to empower their employees to be more productive, accessing their desktops, applications and online services from any location—all though a single workspace and with a few simple clicks. The F5 BIG-IP platform enables simplified remote access, optimizing the VMware End-User-Computing experience and ensuring maximum performance, availability, scalability, and security.

White Paper

by F5

A day in the life

Meet Erin—a Philadelphia-based sales rep. At home preparing for a customer visit, she opens her laptop to check email and connect to her company's CRM system to make a few necessary updates. She lets the dog out, makes a cup of coffee, and before long realizes she's already running late. She'll need to finish her CRM entry during the Uber ride using her mobile device.

Halfway across the country in Chicago, John, an IT lead at the same company, is logging in at corporate headquarters. Managing mobile access and devices for over 500 employees, his job sometimes feels like a balancing act—make sure all the devices and data are secure, ensure regulatory compliance, provide employees with what they need, when they need it, wherever they are.

At the same time on the West Coast, the company's CFO, Scott, is leaving a hotel in Los Angeles to catch a flight back to Chicago for an investor's meeting. Constantly traveling, he uses his tablet to do prep work during his flight. He routinely needs to access sensitive financials, which makes him a bit uneasy—how secure is the connection, and what if he loses his tablet or it's stolen?

These scenarios are common in today's workplace. Employees are increasingly untethered from desks and more connected through smartphones or tablets. Demand for corporate access from their mobile devices is rising, and that's fueling today's "bring your own technology" (BYOT) movement. A transformative force in today's modern enterprise, BYOT promises to deliver many benefits, yet it also introduces new considerations and complexities.

Benefits and risks of BYOT

How do organizations provide easy, secure access to virtual desktops, applications, and online services? How does IT simplify management while ensuring availability and security? Many enterprises are struggling to support the increasing mix of corporate-issued and personal computing devices and also ensure those workers have appropriate secure access to the resources they need to do their job while on the go. This includes email, CRM, ERP, and any other sensitive internal resources that are critical to the day-to-day business operations. While these represent huge challenges for IT departments, ease of access also opens the door to new opportunities for increased employee productivity, improved client satisfaction, faster time to market—greater competiveness.

For mobile and remote employees like our Philadelphia-based sales rep, Erin, a corporate-issued laptop and a personal smartphone are typically used for work. That requires traditional VPN access for the laptop and a mobile device management (MDM) or enterprise mobility solution for the smartphone. For users like our CFO, Scott, sensitive data loss is a primary concern. On an IT-issued laptop or mobile device, a VPN client is typically provided so that a certificate, registration key, or some other digital identifier can be used to authorize access to appropriate systems. However, when Scott uses a personal tablet, the security of the data, device, and applications become a chief consideration. Personal mobile apps must not have access to sensitive business information and, in case a device is lost or stolen, the ability to remotely secure or wipe data is critical. Add to all this the need to access information on other systems, including cloud applications, which bring federated identity and SSO into the picture.

A key challenge with many BYOT implementations is that they impose enterprise controls over all applications and information—so, personal as well as work-related data. For example, an employee leaves a company and his personal device is wiped by the organization, so he loses family photos along with enterprise data and applications. In addition, there are privacy concerns when an employee uses the same mobile app, for example, email, for both corporate and personal messages.

From an IT perspective, organizations agree—they don't want to concern themselves with personal data and applications. As soon as IT manages the entire device or simply connects that device to the corporate network via VPN, the personal traffic on that device becomes an IT problem. In Scott's and Erin's case, many personal items would be intermingled with corporate information. This can be a corporate risk if sensitive data is leaked and a personal risk if family pictures are deleted.

IT administrators like John are focused on controlling the devices—corporate-issued or personal—connecting to their network. This includes tracking the inventory, monitoring for threats and vulnerabilities, and protecting corporate information. At the same time, IT administrators must simplify the process of provisioning devices for Wi-Fi and VPN while also configuring access to email, contacts, calendars, and other essential communication tools.

These IT administrators need to support multiple employees at multiple locations with multiple devices. They must also limit the burden associated with securing and controlling personal mobile use and data, and safely separate personal use and data from corporate oversight. This includes managing devices globally, by groups or individual devices, and pushing policies and configuration requirements to company divisions quickly and easily while enforcing compliance. IT administrators also require tools that interoperate with a heterogeneous device environment that includes platform as different as Android, iOS, Windows Phone, and others.

The flipside to the convenience and flexibility of BYOT is the risk that is introduced to the corporate infrastructure when allowing unmanaged and potentially unsecured personal devices to access sensitive, proprietary information. Applying security across multiple vendors' devices that all run on different platforms is becoming increasingly difficult.

To solve these types of challenges, organizations need dynamic policy enforcement to govern the way they now lock down data and applications. As is the case with laptops, if an employee logs in to the corporate data center from a compromised mobile device that harbors rootkits, key loggers, or other forms of malware, then that employee, who has direct access to the corporate data center, becomes as much of a risk as a hacker.

While Bring Your Own Device/Technology is a hot topic, it is only one part of an overall secure mobility strategy. As seen in the above scenarios—from our sales rep to our IT lead and CFO—today's corporations need to support a mix of managed and unmanaged devices on their network. The question is, where to start?

Several considerations, one unified solution

Organizations looking to get a handle on their enterprise mobility challenges often seek multiple solutions to solve pieces of the puzzle since building an end-to-end solution often requires a multi-vendor approach. An organization could use a classic remote access solution to allow VPN access from corporate and personal computers, laptops, and mobile devices. It could also use a mobility device management (MDM) solution. Both solutions need to easily integrate with an organization's existing infrastructure, especially the directory services.

F5 and VMware have thoroughly tested and documented the benefits of using F5 Application Delivery Networking (ADN) solutions with the VMware End User Computing (EUC) platform to address needs for secure access, a single namespace, load balancing, server health monitoring, and more. Let's explore this collaboration in more detail.

VMware's EUC platform addresses three core areas:

- **Application and desktop virtualization.** Deliver virtual or remote desktops and applications on demand through a single platform.
- **Mobile management.** Manage and protect mobile devices, applications, email, and content while accelerating the mobile strategy.
- **Content and collaboration.** Enable colleagues to have secure mobile access to documents and private social networking anytime, anywhere.

Top BYOT Challenges

- Separating personal and business data and apps on personal mobile devices
- Providing fast, secure access to resources
- Unifying disparate services
- Providing employee privacy
- Ensuring mobile device and corporate data security across public WiFi
- Enforcing company compliance
- Eliminating risk of exposed data
- Providing granular access policy control, management, and enforcement
- Enabling interoperability

Collectively, the VMWare suite of solutions—VMware Workspace Portal, VMware Horizon, and AirWatch by VMware—combines application, device, and data management with centralized identity management and policy enforcement. Both Horizon and Workspace Portal enable secure, streamlined, and simple access to applications across a variety of devices, helping drive anywhere productivity and collaboration from a centralized web portal. **The VMware Workspace Portal** itself works as a service aggregator, which lessens the burden on John, and provides Erin with centralized delivery and management for all her corporate apps across multiple devices. Together with an F5 BIG-IP solution, VMware Workspace Portal delivers all the critical business services Erin needs—more reliably and with greater performance. **VMWare Horizon** enables John to protect corporate information and ensure regulatory requirements by delivering secure remote access across mobile devices.

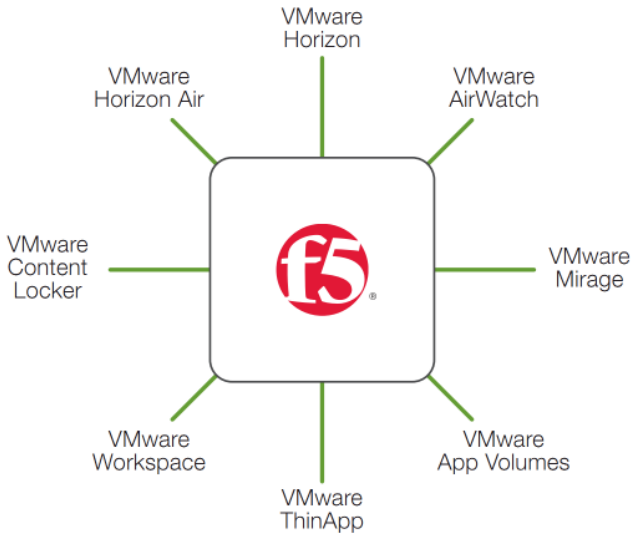

Figure 1. F5 Brings Value to EUC

To support workforce mobility, **AirWatch by VMware** provides a simplified, efficient way to view and manage all devices from the central admin console. John can manage, monitor, and secure all the mobile devices requesting access, pushing VPN, email, and Wi-Fi settings to devices and also locking, tracking, and wiping devices as needed. Auto enrollment for Erin ensures her devices are compliant with corporate policies. Additionally, John can choose to manage just the corporate information being accessed from devices and leave the personal data alone.

How it all works—the technical details

With AirWatch by VMware, IT staff can drive secure access to corporate resources by enabling consistent policies across all the devices in the enterprise. These devices can be managed globally, by groups or individually, and IT can push policy and configuration requirements to company divisions quickly and easily while enforcing compliance. Additionally, integration with BIG-IP® Access Policy Manager® (APM) allows employees to register their mobile devices and get access without involving IT.

How does this all work? A user accessing an application is first authenticated by BIG-IP APM which, in turn, communicates with AirWatch to validate the request. Once verified, AirWatch pushes down the available apps, the profiles along with BIG-IP Edge Client® and its associated rules. BIG-IP Edge Client is a web-delivered, standalone VPN client that provides location awareness, zone determination, roaming, and automatic connection. Administrators can publish rules per device, per container, and even per app. Once the apps are loaded and the user clicks on one, the BIG-IP Edge Client silently launches in the background and creates a secure, optimized, encrypted tunnel to that application. Users no longer have to specially launch the VPN and then navigate to their favorite app; it's all done automatically and seamlessly for the employee. In addition, this granular control connects only to the specified application. It doesn't allow unfettered network access to the entire infrastructure.

For VMware Horizon instances, remote access is the primary goal. However, the VMware client uses multiple ports and protocols, and requests must be directed to the same View Connection Server for a successful session. While PCoIP is UDP-based, it uses SSL-encrypted TCP connections for authentication and USB tunneling. Administrators can save capacity on the View Connection Servers by offloading this encryption to a BIG-IP application delivery controller.

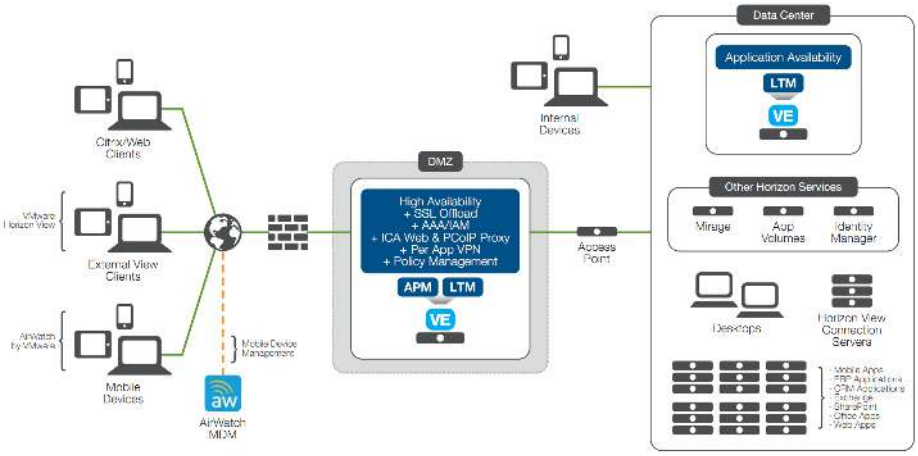

Figure 2. Secure, streamlined, simple EUC access

To route incoming Horizon View connections to the internal network, a PCoIP proxy is needed in an organization's edge network. BIG-IP APM also fulfills this function in a secure and scalable way. By placing APM in front of Windows servers, Active Directory domain-joined servers, and View Connection Servers in the edge network, they're not directly exposed to incoming traffic from the Internet or other untrusted networks. It also eliminates the requirement for VMware Security Servers in the edge network. Instead, the BIG-IP APM appliance proxies the PCoIP connection, passing it to any available Connection Server within the Horizon pod. This provides the scalability benefits of a BIG-IP appliance and gives BIG-IP APM and BIG-IP Local Traffic Manager™ (LTM) visibility into the PCoIP traffic, enabling more advanced access management decisions.

BIG-IP APM protects your public-facing applications by providing policy-based, context-aware access to users while enabling you to consolidate your access infrastructure. Working with or without the BIG-IP Edge Client, BIG-IP APM provides secure remote access to corporate resources—such as Microsoft Exchange, SharePoint, and VDI—from all networks and devices. As the first remote access solution to deliver full support for both IPv4 and IPv6, BIG-IP APM also ensures that your business is ready for the future.

BIG-IP solutions, in conjunction with VMware Workspace Portal, allow organizations to add their own unique applications to a secure web portal. Organizations have the ability to add any application—including Citrix resources—to the secure, IT-controlled environment. Employees can then navigate to their Workspace Portal URI, and in the background, BIG-IP APM provides integrated authentication with Workspace Portal and directs the user to their resources. BIG-IP can also proxy Citrix applications and transparently present those resources to the user within their VMware Workspace. So, Workspace Portal is a single, secure service aggregator for all the needed workplace tools and resources.

BYOT minus the compromise

There's no denying that Bring Your Own Technology has the potential to drive great benefits—from significant cost savings to improved employee productivity—but it's certainly not without some risk. Implementing BYOT requires strategic points of control in the IT infrastructure to realize the promised benefits without compromised security and availability. The advantages of deploying a virtualized solution like VMware End User Computing solutions throughout the enterprise are unquestionable. When deploying the F5 BIG-IP system alongside it, organizations can achieve the higher security, availability, and scalability necessary to protect their investments and their users—all while driving a strong user experience. With straightforward deployment options from F5 and VMware, organizations have the strategic control points they need for mobile applications from the endpoint to the data center and to the cloud.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com