Five Tips to Mastering Enterprise Mobility

Red River

Table of Contents

Introduction

Mastering mobility is essential to effectively support today's increasingly geographically-diverse workforce, empower collaboration and foster informed decision-making in the field. Organizational requirements and business demands are often just as diverse as individual end users and the array of mobile devices on which they rely when it comes to enterprise mobility.

To truly master mobility, you must deliver mobility tools, applications and functionality to a wide range of remote workers. This includes establishing the necessary infrastructure and security to support mobility and BYOD initiatives without endangering your enterprise. Doing so may seem daunting, but with the right partner, insight and direction, you'll learn how to tackle enterprise mobility in no time. Read on to learn five key tips to mastering enterprise mobility.

Read the ebook.

Tip 1: Assess Your Environment

In order to successfully deliver the mobile applications and functionality your employees and agency representatives need, whenever and wherever they need them, you must first assess your environment. This means examining the requirements of your workforce as well as your current IT infrastructure.

Before making any investments in or changes to your infrastructure, take the time to interview and understand the mobility requirements of your end users. Every user has unique requirements. Those using mobile devices, including individuals from every organizational unit, such as sales, operations, executive leadership, etc., should inform and be involved in guiding mobile device selections and policy. This will ensure that you are creating an environment that enables the widest variety of

employees and representatives to work remotely and effectively. This will also help you determine the best functionality and candidates for taking advantage of your mobility solutions.

Assessing your current infrastructure is also vital to ensuring that you have the appropriate networking, storage, security and compute capabilities to properly support and successfully deliver critical mobile solutions. Technologies such as VoIP and Virtual Desktop Infrastructure (VDI) require end to end integration throughout the environment to deliver a seamless user experience. Be sure not to overlook device support factors, including support for protocols such as IPV6, 802.1x, and general network capacity to handle increased traffic loads resulting from mobile devices.

Tip 2: Review Security Protocols

As you enable mobility across your enterprise, you should also review existing security protocols to maintain regulatory compliance and protect critical assets. However, it’s all too easy to get caught up in the rush to control every aspect of personal smartphone and tablet usage. Setting the bar too high for securing mobile devices can kill a mobility initiative before it even gets off the ground.

Security should remain a high priority, but self-awareness is essential. This includes recognizing that laptops are remote devices that include a hard drive for storing and moving data outside of the secure enterprise domain. By reviewing existing security protocols for laptops and other remote offerings already in wide use within your workforce, you can set realistic expectations for security across your enterprise and be better prepared to establish effective security protocols for new mobile devices.

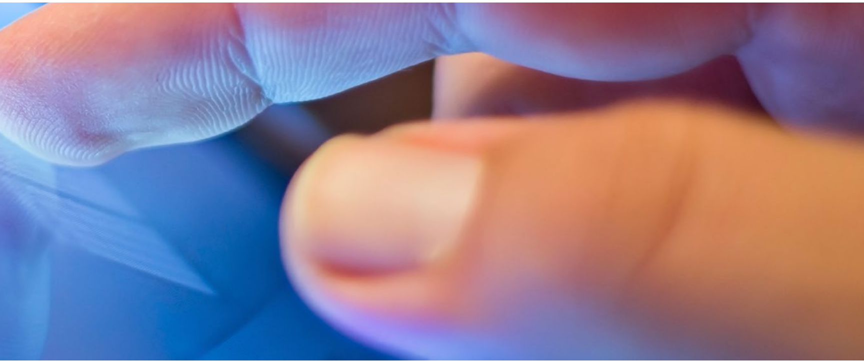
Aside from reviewing current and instituting realistic security protocols, you will also want to examine available tools and practices for enhancing mobile security. Mobile Device Management (MDM) solutions can help you locate, lock and/or wipe mobile devices. To reduce the risk of security breaches and malware infections on the corporate network, make sure that you have tools that allow you to review and restrict access to applications that can be deployed on mobile devices. Consider offering an enterprise-approved app store that allows users to browse and install approved applications. Remote wipe or selective wipe concepts allow administrators to protect against lost or stolen equipment, which may contain sensitive data. And VPN on Demand (VPNoD) provides secure access to internal network resources from any device.

Tip 3: Be Smart About BYOD

Everyone's talking about Bring Your Own Device (BYOD) and employees want to use their own smartphones and tablets on the job as well as for personal activities. However, developing and deploying a customized and secure Bring Your Own Device (BYOD) initiative can be tricky. Even as BYOD empowers productivity and collaboration, provisioning personal smartphones and tablets on your corporate network can put corporate data and assets at risk. So, be smart about BYOD.

Gathering information from your user community during an assessment is an important first step in developing and deploying smart BYOD policies and practices. A thorough assessment will dictate which mobile platforms and solutions will provide a viable experience for end users while meeting the security and compliance directives of your enterprise.

BYOD shouldn't be a free for all. It should translate to Bring Your Own Approved Device. Access control,



which involves authenticating appropriate devices and users, is also essential. Mobile Device Management is critical for end-point security and control. With MDM, you can safely leverage multiple devices and platforms, properly provision devices to separate personal from corporate or agency activity, configure appropriate settings and deliver approved mobile applications. Also carefully evaluate Data Loss Prevention (DLP) solutions as part of a complete enterprise BYOD strategy to protect valuable data assets even when data is in transit.

Tip 4: Consider Customized Mobility Kits

You need to make it as easy as possible for workers to set up home offices or work effectively from remote locations. Consider leveraging complete, customizable and scalable mobility kits, which provide your remote workforce with everything necessary to support working from home or the road.

Optimized mobility kits can and should include the tools required to seamlessly extend your enterprise network and resources to any remote location or device. You should have the flexibility to choose the technology included in pre-packaged mobility kits and they should be accompanied by clear instructions and support.

An assessment will help you determine the requirements of your mobile workers and remote offices. Then you can select the right solutions for kit inclusion to support your mobile workforce, including:

- VoIP Phones
- Workstations
- Desktops/Laptops
- Thin Clients
- Smart Phones
- Mobile Devices
- Tablets
- USB Boot Devices
- Routers
- Headsets
- Monitors
- Multi-Function Printers
- Built-In Applications
- Peripherals
- Much More

Tip 5: Partner With Experts

Not sure that you can tackle enterprise mobility on your own? Partner with the experts. Red River's mobility experts use a proven approach and engagement methodology to ensure that your enterprise and mobile workforce have the right tools, equipment and resources required to solve mobility challenges and meet your mission-critical goals.

Assess. We work closely with you to determine the individualized needs of your mobile workers. We also assess your current infrastructure to ensure that the right equipment and policies are in place to enable secure enterprise mobility and BYOD.

Design. Our engineers work with your IT staff to design custom mobility solutions to address varying work styles, requirements and preferences.

Implement. Red River uses your approved design document to implement custom mobility solutions. We can also implement back-end infrastructure required to support virtualized desktop infrastructure (VDI), remote access VPN and BYOD solutions.

Operate. We help you operate effectively by staying on after implementa¬tions to provide the necessary support and training you need to succeed. With Red River, your IT staff and remote end users have the support they need to troubleshoot problems if they occur. Red River also offers professional and managed services to help you support and extend mobility solutions as the size and density of your network expands.

Red River also has strong relationships with a long list of elite partners, ranging from hardware to services to software, which you can leverage to support mobility initiatives.

Learn more at **www.redriver.com**.

About Red River

Red River is a technology integrator committed to helping customers optimize business processes and maximize the value of technology investments. Widely regarded for our special focus on the U.S. government, Red River has developed a remarkable reputation for delivering technology solutions and services to military and civilian agencies and the companies that serve them. Our core values of hard work and honesty fuel our central mission to make IT personal.

Learn more at www.redriver.com.

RED RIVER
CORP HQ'S
21 WATER ST., SUITE 500
CLAREMONT, NH 03743

800.769.3060 TOLL FREE
603.448.8880 PHONE
603.448.8844 FAX

IT DECISIONS AREN'T BLACK AND WHITE. THINK RED.

Red River