# Unleash mobility with agile security.

Mobility offers an unprecedented opportunity for workforce productivity. It provides new avenues of connection with customers and partners and heightens potential for innovation and growth. But mobility also introduces a balancing act between expanding application and data access and maintaining airtight security.

## Four best practices for superior network security

As remote access to corporate information widens and bring-your-own-device (BYOD) programs proliferate, the urgency of network security increases. Key best practices guide IT decision makers to simpler maintenance of sensitive data and easier compliance with regulations.

The best practices outlined here give your organization the power to bolster security throughout its enterprise. They focus on providing more robust security for the network and preventing data vulnerability on every device in the workforce. Under these guidelines, mobile security becomes a key business enabler instead of a process of restriction and denial.

### Build a BYOD network infrastructure

Connecting to the enterprise network through their own devices is great for employees' productivity. But it can severely limit the bandwidth available for work-related tasks. These devices also introduce potential security threats to corporate resources and could put regulatory compliance at risk. Relegating employees to the guest network avoids these drawbacks, but reduces the bandwidth available to customers and other visitors.

You can avoid these issues by creating a network specifically for BYOD traffic. A dedicated network enables employees to stream media without affecting the other networks. It also gives you the ability to validate devices with security compliance requirements before connecting.

### Set up secure mobile access

Many employees use mobile devices for work-related purposes, but unsecured WiFi connections or theft could allow unauthorized users to gain access to sensitive applications and data.

Organizations should set up secure mobile access with context-aware authentication, network access controls and a virtual private network (VPN). These measures enable secure mobile connections to corporate information, even over public networks.

### Inspect all network traffic

As more mobile devices become active within a network, more vectors become available for security and compliance breaches. The corresponding rise in bandwidth-intensive applications can slow performance across the network too. Organizations must monitor and control incoming and outgoing traffic to maintain performance, security and compliance.

Next generation firewalls provide insight into traffic across all ports and protocols. They help identify security threats or applications that consume excessive bandwidth. This insight gives administrators the ability to set granular usage policies to ensure bandwidth prioritization and maximize secure network productivity.

### Establish a security baseline

An effective identity and access management (IAM) solution prevents intrusions that exploit abused or compromised access credentials. A unified approach to IAM that raises all access to a secure baseline mitigates much of the risk associated with heterogeneous access needs. Suitable IAM solutions address identity governance, privileged account management and access management, including single sign-on. These capabilities empower your organization to effectively control access and streamline important operations.

# Seven best practices to safeguard mobile devices

Protecting your enterprise network is only half the battle. Your organization must also prevent data from leaking into the open from unsecured mobile devices. Several best practices lay a foundation for mobile security that addresses the diversity of user work preference, device types, operating systems and enablement strategies employed across your enterprise.

## 1 Institute a password policy

It may sound simple, but organizations should always implement password-governed access to the operating environment of all devices. Doing so buys time during which to report and remotely disable a missing device. Single sign-on unifies application access, which improves security and reduces the need for IT assistance.

## 2 Implement user education programs

Informed mobile and remote users are more likely to avoid basic behaviors that expose devices to malware or allow unauthorized access to corporate information. For example, employees should refrain from using public wireless networks for work unless they are connecting over VPN.

## 3 Keep the OS up-to-date

An effective way to guard against vulnerabilities is to keep current with OS vendor updates. IT groups should regularly install, or require the installation of, OS updates on all mobile devices to avoid the exploitation of flaws in earlier OS versions.

## 4 Encrypt devices and data

Mobile device encryption protects data in the event that it falls into the wrong hands. IT decision makers should deploy encryption solutions that allow administrators to set policies based on user, user group and data sensitivity.

## 5 Create secure containers

A constrained environment, or container, cordons off enterprise applications from personal ones, or an enterprise workspace from a personal workspace. This approach prevents personal applications and data from commingling with corporate information.

Alternatively, desktop virtualization allows your employees to access applications and data directly from a secure data center without moving that data onto a mobile device. Enterprises can also deploy a virtual desktop model that keeps data in motion on a device's container, which allows users to work offline.

## 6 Implement IAM

In the same way that they help establish a secure baseline for enterprise networks, IAM solutions provide a foundation for secure mobile device access that dramatically reduces security breach incidents. IAM ensures that individuals access only the data and applications they need. Doing this avoids unauthorized or malicious access to sensitive data in a wide range of situations, scenarios and use cases.

## 7 Adopt robust mobile security solutions

The right approach to security goes a long way. However, a secure solution also requires the right tools for the job. The comprehensive Dell Mobile Solutions portfolio includes many security offerings that address current and emerging threats. These technologies aid in the implementation of best practices.

# Drive enterprise value with secure mobile connectivity

As the scale and scope of the mobile workforce expands, sound security practices and solutions are the key to prosperous IT. Adopting best practices for network and mobile device security strengthens protection without hindering access.

Dell Mobile Solutions accommodate an ever-expanding array of use cases, device types, platforms and enablement strategies. Combined with best-practice security, they boost employee productivity, accelerate organizational outcomes and ensure complete regulatory compliance.

**Find out more about how Dell Mobile Solutions allow your organization to capitalize on mobility advances and embrace the promise of new technologies at Dell.com/mobility**