fast track

securing the new workspace

New devices such as smartphones and tablets can help employees be more productive, but it is essential to have a comprehensive security strategy to protect the business from malware and data leakage.

Business has changed dramatically over the last decade with workers now routinely working outside of the office and using a wide variety of devices for work. According to analyst Gartner, Inc., around 75% of workers now qualify as mobile workers with some 60% of them likely to have access to corporate resources from their smartphones by 2015.

This digital revolution has overwhelmed many IT departments, who are trying to deal with the tide of devices with strategies such as bring your own device (BYOD) and company owned personal enabled (COPE). According to Citrix, some 61% of employees now use their personal smartphones at work, with few having any coherent controls over their use.

Unchecked, this situation will spawn all manner of security problems. Key among these are data leakage and malware introduced inadvertently via compromised apps. But controlling new devices requires a fresh approach and new tools.

We suggest seven steps you should take to minimize risk to your organization and secure the new workspace.

Business Services

orange™

seven steps to new workspace security

1. audit devices in use

The first step in getting your devices under control is to undertake an audit of what is being used by employees to access corporate resources. This is likely to be a mix of both company-owned and personal devices. Irrespective of whether it is a corporate device that being used for leisure activity or a personal device used for work, it is essential to segregate the device into enterprise and personal areas.

2. use MDM to manage apps and devices

Set up an enterprise app store with mobile device management (MDM). This allows you to test and distribute corporate apps to mobile devices, keep them updated and enforce your security policy. MDM also provides functionality such as remote lock and wipe, which prevents confidential corporate data from falling into the wrong hands if lost or stolen or when the employee leaves the company. Note that it is essential to have corporate and personal data partitioned on the device, otherwise you will also wipe personal information.

3. use containers or app wrappers

There are two different approaches to accommodating both personal and corporate use on the same device. The first is to install a secure area on the device, known as a container, to contain all enterprise apps and data. The second is to have an app wrapper, which keeps data and processing away from the rest of device, around all business apps on the device. There is some cross-over between the two, because you can use an app wrapper within the container, for example.

4. secure employees, not the perimeter

Users need to be secured on any device whether they are inside the enterprise, traveling or at home. Any connection to company resources needs to establish not only the identity of the user, but also the device they are using. MDM is essential to ensure that all devices connecting to the network meet certain levels of security before they are allowed access to company data.

5. secure remote access

Despite the growth of cloud services and mobile apps, users still need to access some enterprise resources from the corporate network and data center. This secured connection is provided by Flexible SSL. In addition, Flexible Identity Bronze will authenticate the user before providing access.

6. integrate the cloud transparently

The cloud is a fundamental part of the new workspace. Your remote workers need transparent access to data and resources from any device, whether located in the cloud or on the device itself. Flexible Identity Silver provides identity federation to manage employee access to the cloud directly from the corporate directory. In addition, data stored in the cloud will need additional protection provided by an enterprise-class encrypted cloud storage service or via a third-party blind storage security solution.

7. prioritize transparency and usability

Once you accept that the devices will be used for personal tasks, users need to know the terms of use for devices at work, and MDM can enforce this policy. Usability is key to the success of any security strategy. If your solution is not usable or forces users away from their familiar way of working to a worse alternative, then your users will look for ways to circumvent your plans, placing the enterprise at risk.

our solution

Securing the new workspace requires multiple solutions to address the multiple challenges. However, note that technology alone isn't enough, because the new workspace changes user behavior. The main Orange technology solutions are:

- **Flexible SSL:** remote access functionality to access corporate resources on the network
- **Flexible Identity Bronze:** identity and access management to authenticate users remotely
- **Flexible Identity Silver:** identity federation that allows users to access cloud services through their corporate login
- **Device Management Premium:** MDM solution to secure and manage employee devices

to find out more about cloud security, contact your local account team or visit us at **www.orange-business.com**

Business Services

orange™