Mobility you can trust

Security: A $2 trillion problem and risk by 2019[1]

With a work-from-anywhere workforce, your company's information is at risk. Proactively consider security when mobilizing your work. Learn how to provide trustworthy hardware and mitigate security threats.

Mobility is happening

As the modern workforce embraces mobility, up to 25% of corporate data will flow between mobile devices and the cloud by 2018.[2] You don't want this confidential data to be at risk of a breach.

In today's workforce:[3]

3.7 million
employees work from home at least half of the time.

50%
of them hold jobs that are compatible with telecommuting.

80–90%
of them say they would like the option to telecommute.

Workers who telecommute do so an average of 2–3 days per week.[3] That's a substantial amount of time working outside of corporate perimeter security.

Trust and security go hand in hand:

Companies must trust their workers to use their devices responsibly and safeguard their data.

Workers must trust that employers are supplying them with the most secure devices available.

Yet, mobility introduces security risks

Mobility gives hackers additional opportunities to gain access to your company's sensitive data. Your highly confidential information is at risk.

Recent reports show:

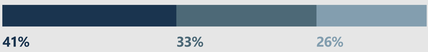
increase in total cost of breaches

The average total cost of a data breach is $3.6 million. That figure is on the rise: Since 2013, the cost of data breaches has increased by 29%. There is a 27% probability that organizations will have a material data breach within the next 24 months.[4]

+133%
increase in malvertising

Worse yet, reports show that malvertising (using malicious codes in online ads to spread malware) increased by 133% from 2015 to 2016.[5] An attack by a malicious insider or criminal is 22% costlier than system glitches or human error.[4]

In the U.S., there are three root causes of data breaches:[4]



41% Malicious criminal attacks

33% System glitches

26% Human error

Here are a few security risks that can threaten your organization:

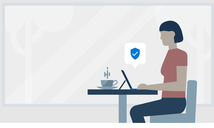
PHYSICAL ACCESS
A lost or stolen device in the wrong hands is very dangerous. Typical passwords and basic security features are not enough to prevent hackers from accessing your data.

DEVICE ATTACKS
Attacks on devices, such as malvertising, can come through web browsers, email attachments, and ad clicks. These can be used to gain access to device data or control the device's functions from afar.

COMMUNICATION INTERCEPTION
Devices connected to Wi-Fi are susceptible to man-in-the-middle (MITM) attacks, where a hacker gains access to a public Wi-Fi portal and intercepts communication between the device and the cloud.

INSIDER THREATS
Employees can misuse their devices to transfer corporate data to external locations, share information over unsecured email, or install risky, unapproved apps for personal use.

Despite these threats, there are premium security solutions built for your business. Remove the barriers for a more mobile and productive team with the right hardware.



Create balance through trusted hardware

How can a smart business strike a balance between trusting employees and trusting their devices? The answer is in the very building blocks of a device's security—the hardware.

When choosing a device for your mobile workers, look for a premium solution that includes the latest in security protection.

DUAL-FACTOR IDENTIFICATION
Passwords can be cracked, but dual-factor identification provides an extra layer of protection. Even better, biometric logins minimize the use of alphanumeric passwords.

HARDWARE ENCRYPTION
This allows the storage of your device to be encrypted with a native solution and protected against attempts to access device storage from boot disks, disk cloning, or physical access to the device's storage components.

SECURITY COMPLIANCE
Ensure that the device you select meets the highest standards for security compliance as rated by third-party boards.

VIRTUALIZATION-BASED SECURITY (VBS)
VBS combines software with hardware to create a heavily restricted, specialized subsystem for storing and transferring critical data—keeping it protected should a device be compromised.

CENTRAL MANAGEMENT
Simplify deployment and key recovery, provide centralized compliance monitoring and reporting, and reduce costs associated with supporting encrypted drives by centrally managing hardware behavior at the firmware layer.

Surface is your secure mobile solution

Learn more about the Surface portfolio of products and how it can drive your company forward.

Read How to Roll Out Tech Like a Pro
or see The Innovator's Guide to Modern Note Taking

Sources:
1. "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation," 2015, Juniper Research
2. "Cybersecurity at the Speed of Digital Business," 2016, Gartner
3. "Latest Telecommuting Statistics," 2016, Global Workplace Analytics
4. "Cost of a Data Breach Study," 2016, IBM
5. "Annual Malvertising Report," 2016, RiskIQ

Microsoft Surface