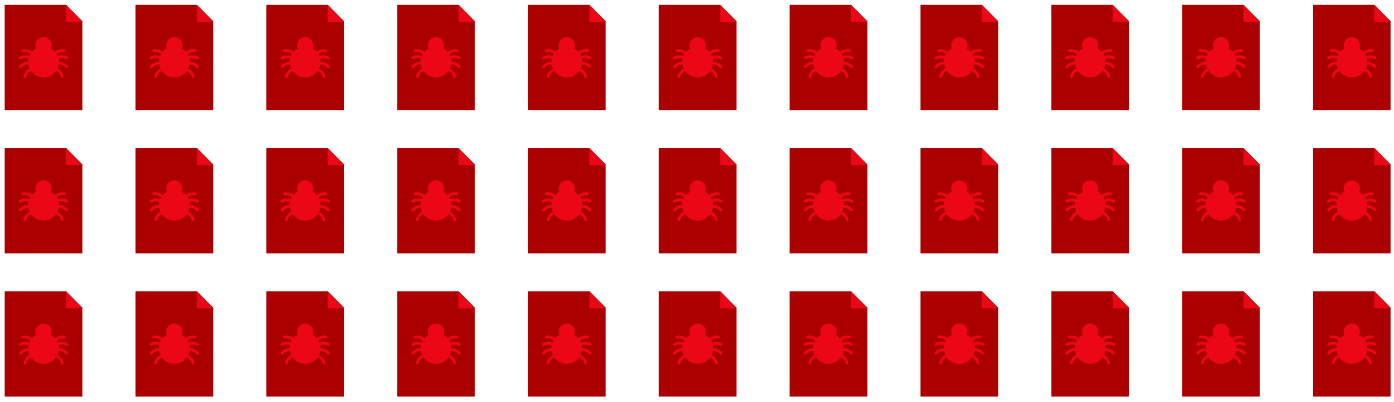
Meeting the Challenges of a Mobile World

Security Solutions for Today's Organizations

The cyberworld we now live in is more dangerous than ever, especially for mobile workers and the devices they rely on to do their jobs. As more people do more work (and conduct more personal business) from their mobile devices, these laptops, tablets, and other mobile devices have become a more attractive target, worthy of a cybercriminal's time and attention.

More than 300,000 new malicious files are created every day and spread through the internet. What's worse, an attacker can go undetected in your environment for 200 days or more.[1] 2015 saw everything from the Android Stagefright exploit to Instagram attacks gathering Personally Identifiable Data (PID)—then Santa Claus malware showed up just in time for Christmas. What about this year? During a recent scan, over 60 Android games hosted on Google Play were discovered to be infected with "Android. Xiny.19.origin," a Trojan that conceals Android executables inside images to avoid being detected.[2]

More than 300,000 new malicious files are created every day.[1]

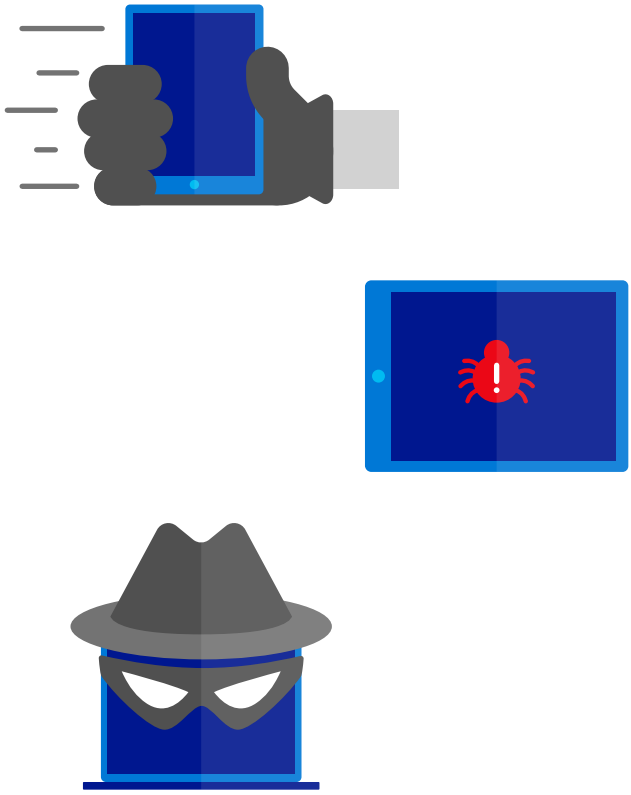


= 10,000 malicious files

Cybersecurity Threats on the Move

Today's mobile threats come in many different forms:

- **Lost or stolen devices.** Devices that go missing represent not only a loss of valuable hardware but also create critical points of vulnerability. A mobile device in the wrong hands can serve as an open door to your network.
- **Malware.** Malware ranges from software that's simply annoying to truly evil apps that rack up charges, demand payments, or install remote access tools that take control of your device. Malware can show up courtesy of drive-by downloads, browser exploits, phishing, SMiSh-ing, infected apps in "trusted" app stores, and other vulnerabilities.
- **Spyware, network spoofing, and Wi-Fi sniffing.** These mechanisms are designed to capture everything from specific user credentials to network traffic en masse—perfect for network infiltration, identity theft, fraud, and other nefarious purposes.



Just how fast are mobile threats growing? New mobile malware threats doubled in less than a year—from Q1 to Q4 in 2015.[2] Every minute, new types of attacks are being conceived and new vulnerabilities are being exploited. New versions of "WannaCry" ransomware, for example, continue to bring both global enterprises and public agencies to their knees.[3] In the meantime, despite IT's best efforts, users continue clicking things they shouldn't.

It's the challenge of IT to prevent these and other cyber-misfortunes, while still making mobile devices easy to use and giving users access to the resources they need to get their jobs done and keep the business running at top efficiency. It's a tough balance for organizations to strike, but this ebook will help you identify the security features that can help you better protect your unique environment, setting your users up for success while giving you peace of mind.

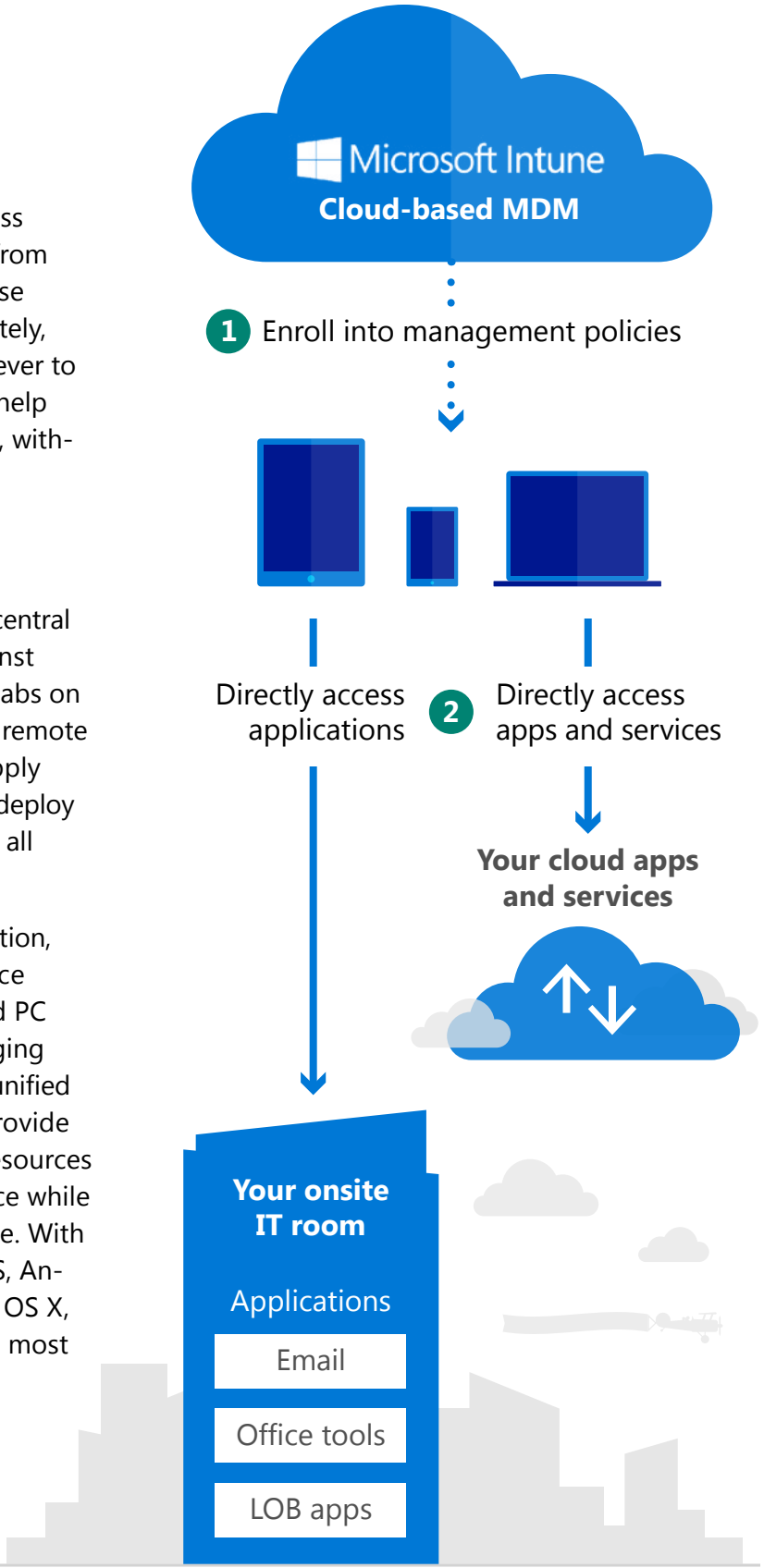
Mobile Security Must-Haves

Your job is to provide users with secure access to apps, data, and other network resources from whatever device they're using—whether those resources are onsite or in the cloud. Fortunately, today's technology is better equipped than ever to meet the challenge, providing features that help users work where, how, and when they want, without compromising on security.

Mobile Device Management

Mobile Device Management (MDM), is your central command for managing your defense against threats and malware. MDM helps you keep tabs on roving devices, providing visibility as well as remote control of those devices, allowing you to apply security updates and settings en masse, and deploy new features quickly and consistently across all mobile devices.

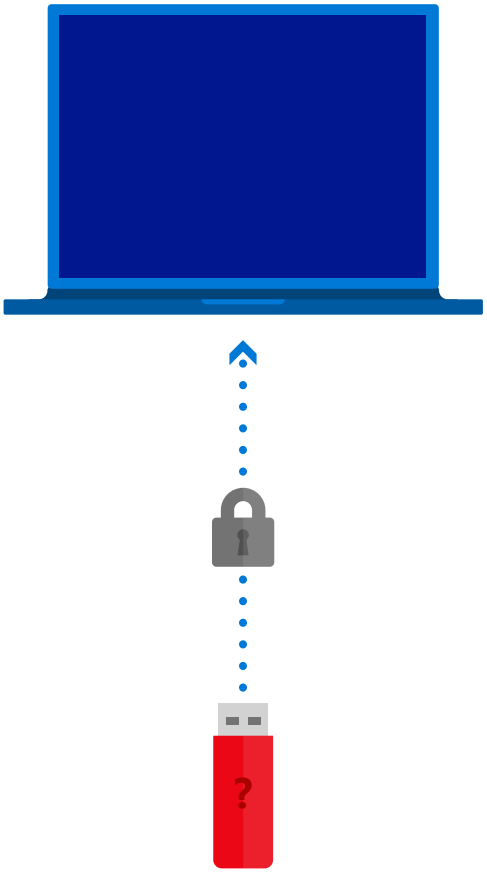
For example, Microsoft Intune, an MDM solution, provides comprehensive cloud-based device management, application management, and PC management capabilities—as well as managing on-premises and static devices—in a single unified solution. Using Intune, organizations can provide employees with access to apps, data, and resources from virtually anywhere on almost any device while helping to keep company information secure. With support for operating systems including iOS, Android, Windows, Windows Mobile, and Mac OS X, Intune allows IT teams to easily manage the most diverse environments.



Hardware-Based Security

Today's devices allow IT to take advantage of the Unified Extensible Firmware Interface (UEFI) to enhance security at the hardware level. UEFI firmware works in conjunction with a Trusted Platform Module (TPM) chip. The TPM creates a secure hash value based on the computer's hardware signature. This signature hash can be used by a number of technologies, like BitLocker Drive Encrypton, to secure a computer against threats. With BitLocker, you can lock the encrypted contents of your system's storage—including the system drive—preventing boot up even if the storage is moved to another device or the computer's hardware signature changes.

Advanced UEFI features found on premium devices like Microsoft Surface provide many other security options, such as allowing IT to prevent booting from the USB port with a portable drive. Disabling this feature allows full use of the USB port for everything but booting. You can also shut off the SurfaceConnect USB connection, disabling support for Surface Dock and its USB ports and Ethernet. The same goes for the microSD reader. You can also control ports, cameras, Wi-Fi, and Bluetooth settings.

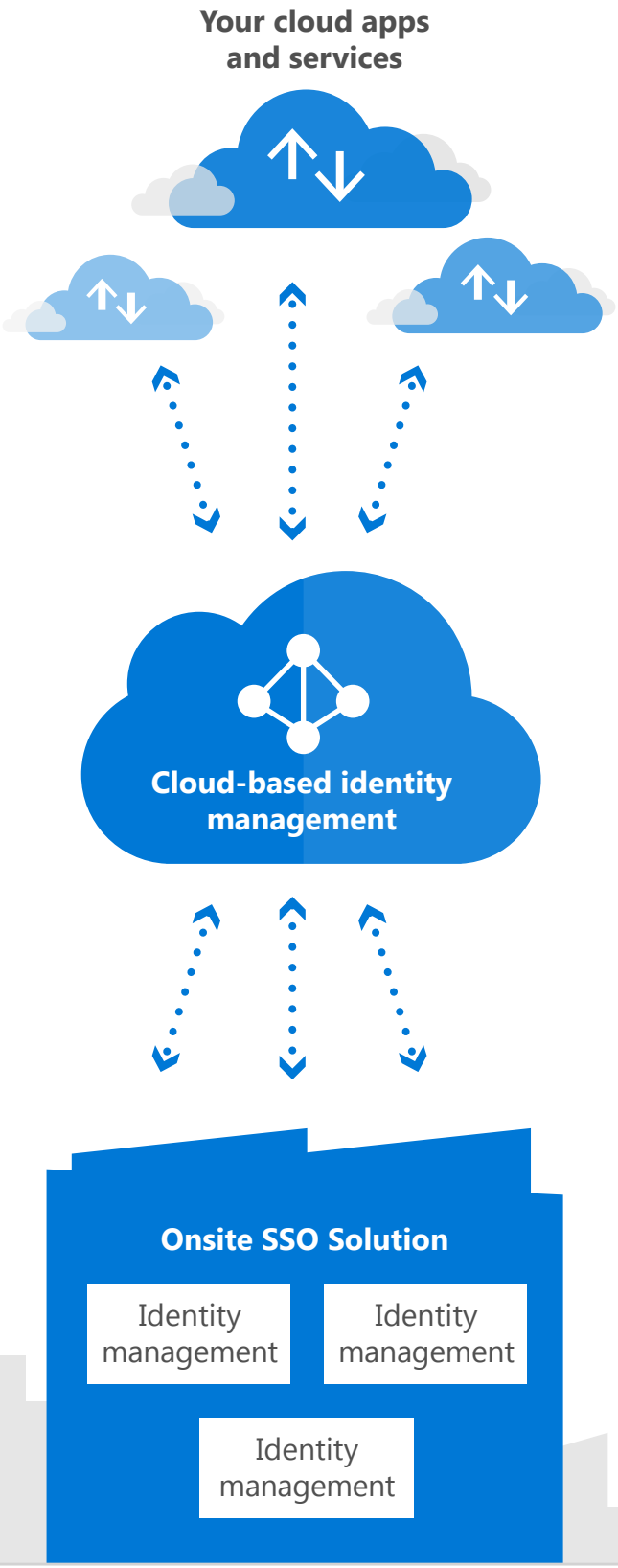


OS-Based Security

When it comes to OS-based security, Windows 10 is setting the new standard, providing a suite of features that protect devices, data, intellectual property, and other network resources against all manner of threats:

- **Device Guard and AppLocker** completely locks down the device so only trusted applications and scripts can be run
- **Trusted Boot** helps ensure that only a genuine version of Windows starts up on the device, preventing attackers from evading detection
- **Dynamic Lock** can be configured to automatically lock your PC when your Bluetooth phone goes out of range
- **Windows Hello for Business** replaces passwords with strong two-factor authentication on PCs as well as mobile devices—authentication that requires both a device-specific biometric and PIN
- **File-level data protection** helps ensure that company data isn't accidentally or intentionally leaked to unauthorized users or locations
- **Single sign-on** (SSO) can be used to help boost security and prevent password problems for Azure Active Directory-connected applications, Integrated Windows Authentication apps and services, and AD Federation Services applications in Windows Server 2016

Windows 10 users also benefit from ongoing Microsoft OS security updates. For example, Microsoft patched the WannaCry vulnerability in March of 2017, two months before the malware was released. Thanks to this protection, up-to-date Windows 10 systems were immune to the worm.



Software-Based Threat Protection

Microsoft enables a strong security baseline by including anti-malware capabilities out of the box, reducing the footprint available for malicious activity in the ecosystem. For example, Windows 10 provides Windows Defender Security Center, a comprehensive anti-virus and anti-malware program. Defender is designed to send security data back to a monitored Microsoft Security Operations Center, creating what may be one of the largest networks of malware sensors in the world. This approach ensures that any necessary updates can be pushed out quickly to everyone protected by Defender.

Built-in solutions such as Absolute Data and Device Security (DDS) provide yet another layer of data and device security. DDS is an optional solution that uses location-based services to help IT track and recover lost or stolen devices. If the DDS app is removed, it will automatically reinstall itself, enabling continuous location monitoring.

Microsoft Surface: Setting Users Up for Success and Security

Microsoft Surface devices help IT teams set up employees for success while empowering the organization to face today's tough security challenges head on. Packed with native hardware, Windows 10 OS, and software-based security features, Surface devices allow end users to enjoy the performance, flexibility, and ease of use of the latest mobile devices without putting the organization's valuable network resources at risk.

Staying on top of security threats can be challenging, but Surface makes it easy for IT teams to take advantage of its suite of security features. For example, once you've identified the advanced UEFI features you want to implement, you can automate the configuration of those security settings by using Surface Pro Firmware Tools available from the Microsoft Download Center.

Surface devices also offer an onscreen keyboard as part of the boot-up process—a feature that can be used in conjunction with PIN-based authentication to keep the device locked until the proper PIN or password is entered, easily adding a second layer of authentication beyond the traditional user name and password combination. Research shows that 75% of users reuse the same three or four passwords across all their business and personal accounts.[1] Even if your organization isn't ready for biometric authentication, Surface can help you strengthen access controls across mobile devices in ways that won't disrupt user productivity.

Surface Pro

Surface Hub

Surface Book

Surface Studio

A Surface for Every Occasion

The Microsoft Surface portfolio provides a wide range of options to meet your users' unique business needs:

- The **Surface Pro** is a fully functioning laptop in a lightweight tablet form factor
- The **Surface Book** laptop features high performance and a detachable screen that can be used as a tablet or canvas
- The **Surface Studio** converts from a desktop experience to the huge canvas of a drafting table
- The **Surface Hub** provides a giant touchscreen and high-quality video and audio to enable powerful collaboration

To learn more about the Microsoft Surface family of products, visit our **website**, or **send us a note** and one of our Surface specialists will contact you. Our experts can answer any questions you may have about Surface and can help you identify the perfect Surface devices for your organization.

Microsoft

Sources:

1 "Outsmart Them with Windows 10," *Microsoft*. http://wincom.blob.core.windows.net/documents/Win10Security.pdf

2 "Mobile Threat Report," *Intel Security*. https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

3 "WannaCry Ransomware Situation Gets Worse As Copycats And Fake Decryptors Appear," *Forbes*, May 15, 2017. https://www.forbes.com/sites/leemathews/2017/05/15/wannacry-ransomware-copycats-fake-decryptor/#5931fdfe3429