Mobile Devices Need Stronger Protections

When it comes to convenience and access in the enterprise, this is a golden age. Users can access corporate resources and data from their smartphones, tablets, or PCs from almost anywhere at any time. Of course, what’s convenient and productive for your users can be a security and management headache for your IT administrators as they strive to take advantage of increased mobility and the bring-your-own-device (BYOD) trend while securing corporate data.

The personal nature and associated usage patterns of mobile devices make them prime targets for attacks. Users are not known for their security awareness. They install all sorts of apps on their mobile devices without regard for the security of those apps. Users allow apps to have all the device permissions the apps ask for even when the permissions are overreaching. Mobile devices are often shared between family members with little oversight over how they’re used or what websites and data they access. The devices also might frequent wireless networks that have dubious levels of security. Users then use these devices to access both personal and corporate data. These usage patterns put mobile devices and their users at higher risk from identity theft, malware, and other stealthy threats that can infiltrate systems at deeper levels to steal data or even take control of a device.

Windows 8.1* now makes mobile management of PCs possible by adding more granularity for control of non-domain-joined mobile devices and support for mobile device management (MDM) products. By supporting the Open Mobile Alliance Device Management (OMA DM) API, Windows 8.1 enables you to manage devices through a low-overhead agent without needing to deploy a full management client on each device. But MDM products don’t offer the same level of control as traditional domain-joined management solutions.

To strengthen endpoint security, you need a solution that builds from the silicon up to better ensure the integrity of the system even before the operating system starts. By using tablets, Ultrabook™ devices, 2 in 1 devices, and laptops powered by 4th generation Intel® Core™ processors and Intel® Atom™ processors running Windows 8.1, you can complement your MDM solution with strong, hardware-assisted security and with more comprehensive management, speed, and efficiency.
Strong Security Starts before the Operating System

Hardware-assisted security adds layers of protection that stay with the device regardless of how it is used or managed. Even before the operating system starts, deeper layers of security are working to help prevent stealth malware, like a rootkit, from injecting itself and taking over a system. For example, during the initial Windows 8.1 boot process, Intel® Platform Protection Technology with BIOS Guard and Boot Guard helps prevent unauthorized software and malware from taking over boot blocks that are critical to a system’s function.1 Unified Extensible Firmware Interface (UEFI) Secure Boot continues early protections by ensuring only a properly signed operating system loader is used during startup.

Windows 8.1 Trusted Boot provides additional startup protections by using the UEFI root of trust to ensure that the rest of the boot components are secure and have integrity. At the same time, Windows 8.1 Measured Boot takes measurements of each component—from firmware up through the boot start drivers and even anti-malware drivers—and securely locks away the measurements in a trusted platform module (TPM), such as Intel® Platform Trust Technology. The measurements collected by Measured Boot can be securely accessed from Intel Platform Trust Technology by third-party security software in order to compare the current state of the system against the known-good state established by Secure Boot. By establishing and verifying a trusted state, you can better ensure the integrity of the system and help identify and block malware before it takes root.

Each time the device is started, these combined technologies help ensure that the deepest levels of the system are not tampered with. But hardware-enhanced security doesn’t end with the boot process. Intel Platform Protection Technology with Intel® OS Guard helps protect the deepest levels of your system, even if an application has been compromised.2 This unique Intel feature helps prevent hackers from remotely taking over a user’s PC by preventing malicious code in compromised application memory from launching low-level, privilege escalation attacks.

Block Stealthy Malware

Once stealthy malware infects the system, it stays invisible to antivirus software. That gives the threat an opportunity to take control of the system, steal confidential information, and spread to other systems. Mobile device users need run-time protections to help block stealthy threats—malware that can infect deeper levels of the system and go undetected by software-only solutions.

The strongest protection from malware comes from solutions that don’t rely on knowledge of existing threats. By pairing built-in protections from Windows 8.1 devices powered by Intel Core processors with McAfee Deep Defender* software, you can detect and block advanced, hidden attacks in real time before they cause damage. McAfee Deep Defender relies on McAfee DeepSAFE* technology, a solution jointly developed by Intel and McAfee that delivers real-time, kernel-level monitoring of memory. This unique connection to hardware with behavioral-based detection makes McAfee Deep Defender more...
Effective than software-based solutions. In fact, in testing against top competitors by AV-TEST labs, McAfee Deep Defender was the only product to detect 100 percent of stealthy rootkits.  

With strong, proactive protections from Intel OS Guard and McAfee Deep Defender, you can stop more kernel-level attacks before they have a chance to propagate and threaten mobile devices based on Intel processors, even when the devices are non-domain-joined or are inaccessible from your corporate network.

**Provide Safer Authentication**

Providing secure access to resources has always been a challenge for organizations. That challenge has grown recently, due to the expanding landscape of mobile devices, applications, and busy employees on the go. To better protect your assets and users, you need to provide something stronger than a simple user name and password scheme for authentication and VPN access. With Intel® Identity Protection Technology (Intel® IPT), Intel provides a hardware root of trust that can be used by multi-factor authentication solutions on devices powered by Intel Core processors and Intel Atom processors.

For example, with Intel IPT with Public Key Infrastructure (PKI), users can log on to a VPN without having to enter a password or fumble with a physical token, while still benefiting from the stronger security offered by two-factor authentication. For devices powered by Intel Atom processors or Intel Core processors with Intel® vPro™ technology, Intel IPT with PKI offers an alternative to physical smart cards that is easier to deploy and less expensive. Intel IPT with PKI has built-in hardware capabilities to store digital certificates in firmware for secure VPN or Secure Sockets Layer (SSL) web site authentication, to authenticate a user and a server to each other, and to encrypt and digitally sign e-mail and documents. Even if you already have a PKI implementation in your organization, Intel IPT with PKI could save you money by eliminating the need to purchase and support traditional smart cards or other token storage options. In addition, on devices powered by Intel Core processors, Intel IPT with PKI can be used with Protected Transaction Display (PTD) technology, which lets you create secure PIN pads to protect passwords and numeric key entries from screen-scraping and key-logging malware.

**Secure Your Company’s Data**

Data is your company’s most valuable asset. From customer information to employee identities to your intellectual property—if a device is lost or stolen, you need to keep those assets out of the wrong hands. With mobile devices off the company network and outside of domain control, this can be a challenging proposition; but several Intel hardware-assisted technologies can help you keep your data away from prying eyes.

Encryption is one of the best ways to keep your data safe, but organizations are often reluctant to widely deploy encryption because of the overhead it entails. Intel helps you remove the barriers to deployment with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), a cryptographic instruction set that accelerates AES data encryption and decryption on devices powered by Intel Core processors and Intel Atom processors. Because of the enhanced cryptographic performance of Intel AES-NI, IT can reap the benefits of encryption for stronger security without imposing any significant performance hit on users.

**Figure 1:** Unified Extensible Firmware Interface (UEFI) Secure Boot and Measured Boot technologies in Windows 8.1* help verify and secure the system at startup.

**Intel Silicon Root of Trust**

- **Secure Boot**
  - Only signed, verified OS loaders are allowed to start.
  - OS loader enforces signature verification of Windows® components.

- **Measured Boot**
  - Boot components are measured at startup and stored in Intel® Platform Trust Technology (Intel® PTT).
  - Remote attestation, if available, can validate client state.

---

17,317,184 Identities exposed in 447 reported breaches in 2012.
**Stronger Endpoint Security Starts with a Hardware-Based Foundation**

<table>
<thead>
<tr>
<th>TECHNOLOGY</th>
<th>BENEFIT</th>
<th>INTEL® CORE™ PROCESSORS</th>
<th>INTEL® ATOM™ PROCESSORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEFI Secure Boot</td>
<td>Provides a secure root of trust and prevents execution of an unverified bootloader</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Intel® Platform Protection Technology with BIOS Guard¹</td>
<td>Protects the BIOS flash from modification without platform manufacturer authorization</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Intel® Platform Protection Technology with Boot Guard¹</td>
<td>Helps maintain boot integrity by preventing execution of unauthorized software and malware in the boot blocks</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Intel® Platform Trust Technology</td>
<td>Provides a standards-based TPM solution for securely storing measurements used to verify integrity of the system</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Intel® OS Guard²</td>
<td>Helps prevent privilege-escalation attacks that allow attackers to take control of the OS</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Intel® Secure Key⁹</td>
<td>True digital random number generator with keys created more securely in the hardware</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Intel® Virtualization Technology (Intel® VT-x)¹²</td>
<td>Provides hardware-assisted foundation for McAfee DeepSAFE* and McAfee Deep Defender* security</td>
<td>X</td>
<td>X¹¹</td>
</tr>
<tr>
<td>Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)⁸</td>
<td>More efficient encryption; used with McAfee Complete Data Protection Suites* to help keep data safer without any noticeable impact on performance</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI)⁵</td>
<td>Provides strong two-factor authentication without the need for physical tokens</td>
<td>X</td>
<td>X¹²</td>
</tr>
<tr>
<td>Intel IPT with Protected Transaction Display (PTD)⁵</td>
<td>Helps verify human presence at PC and prevent screen-scraping and key-logging of passwords</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Intel AES-NI also accelerates the encryption used by McAfee Complete Data Protection Suites*, which include protection from stealth attacks, real-time memory and CPU monitoring and, of course, strong, efficient encryption of data.

Encryption is even simpler when you deploy client devices built with the Intel® Solid-State Drive (SSD) Pro 1500 Series. These advanced SSDs include an integrated hardware-based 256-bit AES engine that can seamlessly encrypt and decrypt data without compromising performance. When coupled with systems powered by Intel® Core™ vPro™ processors, the Intel SSD Pro 1500 Series also gives you extensive remote management capabilities, including remote password reset. If a user forgets the password to their SSD, IT can reset the password quickly and remotely so the user can get back to work more quickly.

**Strengthen Encryption with True Random Numbers**

Typically, encryption keys are generated from software-based, pseudo-random number generators. Pseudo-random numbers offer complexity that seems secure, but in reality can be replicated by sophisticated hackers who determine the procedure used to generate the numbers. Intel® Secure Key responds to this...
Meet the Mobile Device Security Challenge

Today’s modern workforce expects full access to resources from a wide range of devices tailored to their needs. To better protect your devices, data, and users, complement your management solutions with strong, hardware-assisted protections available on devices powered by Intel Core processors and Intel Atom processors and running Windows 8.1. With enhanced security rooted in hardware, Intel integrated technologies help keep your systems safer with the speed and efficiency to meet the requirements of modern devices running Windows 8.1 and to satisfy the needs of your demanding workers.

For more information on Intel hardware-assisted security features, visit:

www.intel.com/technology/security

For more information on tablets and Ultrabook devices powered by Intel Core processors and Intel Atom processors, visit:

www.intel.com/tabletforbusiness
www.intel.com/ultrabookforbusiness

No system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and an enabled operating system. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Identity Protection Technology-enabled system, including a 2nd gen or higher Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://intel.com.


No system can provide absolute security under all conditions. Requires an Intel Secure Key enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.


No computer system can provide absolute security under all conditions. Requires an Intel Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.