Windows 8

Addressing the Security Challenges of Today and Tomorrow

Anyone who has followed the enterprise security landscape for the past few years knows it has reached a turning point. Today's cyberattacks have become more targeted, persistent, clandestine and damaging than the attacks of a few years ago. Yesterday's hackers were often after fun and notoriety.

Today they are more likely to be seeking valuable proprietary information, intellectual property and state secrets. If that isn't scary enough, security has been complicated by the proliferation of personal mobile devices, such as smartphones and tablets, and the "bring your own device" (BYOD) trend.

A February, 2013 Ponemon Institute study ("The Post Breach Boom," Ponemon Institute LLC, sponsored by Solera Networks) revealed that breaches have not just become common, they've become much more difficult to detect and financially damaging. Malicious data breaches cost organizations an average of $840,000 per breach, according to the study, and the average malicious breach today takes about 80 days to detect and more than 123 days to resolve.

That's why IT strategy has shifted from simply preventing security breaches to also containing and mitigating the damage of the ones that slip past today's defenses. In this environment, state-of-the-art security technologies are more important than ever before.

An OS with a Defense-in-Depth Approach

Aside from its mobility and productivity advances, Windows 8 represents the most significant step forward yet in client security. The innovations are vital for preventing and containing emerging threats, including viruses, Trojans, boot/rootkits, BIOS attacks and even advanced persistent threats.

Windows 8 moves beyond making it difficult to attack the operating system, applications and data: It includes a reengineered architecture that, in many cases, can eliminate the possibility for successful attacks. It's an essential tool for a defense-in-depth strategy that contains and eliminates the impact of the most challenging intrusions and malicious code. It's not just an incremental upgrade; it's a game changer for the Windows platform that can equip even the most security sensitive organizations with the tools they need to address the security challenges of today and tomorrow.

"The security advancements from Windows XP to Windows 7 are leaps and bounds, and the advancements from [Windows] 7 to [Windows] 8 are just as great," says Chris Valasek, director of security intelligence at IOActive.

Groundbreaking Malware Resistance

Past versions of Windows provide robust protection from a variety of security issues, but Windows 8 is the first Windows release to have a hardened boot process and the ability to protect antimalware solutions from tampering.

Windows 8 offers full support for the Unified Extensible Firmware Interface (UEFI), a standards-based replacement for the legacy system BIOS. UEFI's Secure Boot feature ensures that the very first software to start on the system consists of authorized, trusted and tamper-free UEFI drivers, applications and operating systems, not malware.

From there, Trusted Boot protects the remainder of the boot process and loads an Early Launch Antimalware (ELAM) driver. This ensures that all of Windows' defenses and an antimalware solution are running before any other third-party drivers and software. If any tampering is detected, Trusted Boot can automatically repair the Windows boot components and the antimalware driver and return it to a secure state.

The comprehensive boot protection that Windows 8 includes is unprecedented, and it will help prevent sophisticated types of malware from compromising devices.

Reduce the Chances of an Exploit

Windows 8 also has two enhanced features that make the system less likely to be exploited even in the event that a vulnerability is discovered. With address space layout randomization (ASLR) and Data Execution Prevention (DEP), the likelihood that an exploit will be successful is drastically reduced, if not eliminated. In fact, all known exploit techniques used to attack previous versions of Windows have been reviewed and rendered useless on Windows 8. "I wouldn't want to be tasked with creating a heap exploit for Windows 8," says Valasek.

Windows Defender has been updated in Windows 8 to provide comprehensive antimalware capabilities, protecting against a full range of malicious software, including viruses and spyware. IT managers can now be assured that all Windows 8 devices, including those used under a BYOD policy, have the fundamental protection that organizations need.

With the Windows Store, IT can rest assured that users now have a trustworthy place to download applications that have been prescreened for security flaws and malware and will run in a sandbox. For applications that are acquired from the Internet, Windows 8 SmartScreen performs a reputation check and can block execution when malicious software is detected.

Using AppLocker, IT administrators can also control the applications users can install on their Windows 8 devices.

Modern Authenticators

User passwords are increasingly challenging when it comes to preventing unauthorized access to sensitive information. Users often create weak, easily hacked or guessed passwords and can be tricked into revealing them via social engineering tactics. Studies show that about 60 percent of users maintain the same password for multiple accounts. Hackers regularly steal the login information of thousands of users from organizations and then use them to steal identities and hack into other organizations. Multifactor authentication using smart cards, biometrics and other advanced techniques are vastly more effective than passwords, but until now they've been expensive and difficult to manage.

Windows 8 addresses the challenges of multifactor authentication with virtual smart cards, which enable IT to easily provision a solution that doesn't burden users and IT with cumbersome and easy-to-lose smart cards and tokens. Windows 8 also offers picture passwords, a powerful enhancement to the traditional text password that provides an intuitive, easy-to-use sign-in option for touch devices.

Pervasive Data Protection

Robust data encryption is an essential way to prevent hackers from stealing sensitive data. While encryption is notoriously difficult to deploy, regardless of the technology and vendor, Windows 8 addresses these challenges by providing a high-performance, easy-to-provision-and-manage encryption solution with BitLocker and BitLocker To Go.

Windows 8's BitLocker has vastly improved the process of provisioning hard disk encryption. BitLocker also speeds encryption up to 20 times by allowing encryption of used disk space only. If the device is equipped with an encrypting hard drive, BitLocker can secure the entire drive in about a second.

BitLocker can even be used to protect Windows To Go devices. Windows To Go allows the creation of an entire secure Windows 8 environment on a USB drive that mobile users can plug into compatible computers. The Windows To Go environment completely separates itself from the system to which it connects, making it secure for accessing sensitive data and applications.

When it comes to IT priorities, improving security tops the list. IT departments should take a close look at how deploying Windows 8 can improve their organization's entire security posture. It is the best version of Windows for securing the system, apps and data — addressing the emerging security challenges of today, and the evolving challenges of pervasive mobility.

To learn more about how Windows 8 Enterprise works to increase security, please visit: http://www.microsoft.com/windows/securedevices.

Photo: Microsoft