IS SOFTWARE-ONLY SECURITY TOO SOFT?

By deploying hardware-enhanced security solutions, enterprises can create much stronger security than with software alone and enjoy fast recovery cycles.

All it takes is a quick look at the latest headlines to see that cyberattacks are more pervasive and sophisticated than ever before. That can spell bad news for businesses—and even worse news for their customers. Experts estimate that a new malware specimen is created every 4.2 seconds, often growing, mutating, and remaining undetected for months[1].

Why this sudden uptick in cybercrime? One word: money. Hacking isn't the amateur hobby it used to be—it's now a highly lucrative field, with some hackers earning up to $80,000 a month from their illegal exploits[2].

So how can businesses help lock down the security of their enterprise and their customers' data in the face of relentless threats? And, perhaps more important, how can they do it in a way that doesn't compromise productivity?

> "SOFTWARE IS SO EASY TO ATTACK TODAY. THE HARDWARE IS IN A TOTALLY DIFFERENT LEVEL—IT'S BELOW, CLOSED IN NATURE, A LOT HARDER TO ACCESS."
>
> —Yasser Rasheed
>
> Director of Business Client Security, Intel

It's time to look beyond software

The short answer is this: Businesses today need to consider hardware-enhanced security solutions. A software-alone approach is no longer viable, as all software—no matter how sophisticated—is inherently hackable. And once the attacker gets past the software, if hardware protections are not in place, there's nothing to stop him from corrupting the network or stealing credentials or data.

"Software is so easy to attack today," said Yasser Rasheed, director of business client security at Intel. "Software is by design open for innovation and creativity and people writing apps. But that also means bad actors have similar access. So it's a race between the good and the bad."

According to Rasheed, even the best antivirus software is no substitute for a hardware-enhanced solution. "The new type of attacks, they call them polymorphic attacks, which means they change in memory," he said. "So even if you scan the disk, you're out of luck because it's in memory and it's changing its code in memory."

When security is built into the silicon itself, authentication abilities become more powerful, data is protected by default, software can better reach its full potential, and devices can be scanned for malware before the machine even activates or boots the OS.

"The hardware is in a totally different level," said Rasheed. "It's beyond the reach of a traditional software attack—below the layer of software that sits on the surface, closed in nature, and a lot harder to access."

A NEW MALWARE SPECIMEN IS CREATED EVERY 4.2 SECONDS[1]

Passwords no longer pass the test

Hardware-enhanced security provides substantial improvements in user authentication. Today's hackers are experts at breaking through password protections or using phishing attacks to trick users into giving passwords away.

"We all know that password-only authentication doesn't work, right?" said Rasheed. "People write it down on a piece of paper at the end of the day if it's too complicated."

Thankfully, new technologies have arisen that can help protect the enterprise from the inside out.

One such technology, the Intel® Authenticate solution, replaces traditional passwords with hardened, multifactor authentication, including biometrics and other factors. More important, the authentication policy is managed by IT and enforced by hardware, making it exponentially harder for an attacker to get in. This creates an unprecedented improvement in security and a significant reduction in IT tickets, and when these keys are anchored in the silicon of the device itself, they're less susceptible to tampering.

Biometrics that actually work

As you're probably well aware, older biometric technology came with a host of problems. Fingerprint scanners were fussy and unreliable, facial recognition software could be influenced by background activity or personal movement—the list goes on. In some cases, these security measures barely even worked, and did little to protect the enterprise.

The Intel Authenticate solution is designed to work with the latest biometric sensors, which have developed a number of revolutionary, proven advancements that diminish the shortcomings of older biometric technology. Fingerprint fidelity can now be captured more accurately with built-in sensors with higher dot-per-inch density to match every ridge that makes the fingerprint unique.

Precise infrared webcams are now designed to better distinguish the personal peaks and valleys of users more accurately—no more holding still and trying not to blink like you're posing for a photograph in the 1800s. They also work in a variety of background lighting situations. For instance, if the user is working on an airplane where all the lights are turned off or dimmed, her face can still be recognized.

Making the most of Windows* 10

The latest 7th Gen Intel® Core™ vPro™ processors further harden the built-in protections of Windows 10, working to stop malicious code from getting through in the first place. They help ensure only good code can run, and block malicious access to the business's most valuable asset: user credentials.

Protecting the power-on process

Hardware-enhanced security can even protect data before devices are booted up. At the vulnerable moment of boot, before any security software is able to turn on, Intel® BIOS Guard and Intel® Boot Guard help Unified Extensible Firmware Interface (UEFI) for Secure Boot* ensure the coast is clear before handing control over to the operating system.

Recovery re-energized

Unfortunately, nothing is truly unhackable. While biometrics, pre-boot protection, and other hardware-based security solutions can greatly reduce the number of breaches, they can't eradicate cyberattacks completely.

When an attack does happen, that's where recovery comes into play. And, again, the best solutions are ones that involve hardware-enhanced recovery and aren't relying solely on software to get the job done.

"Today's attacks are generally very hard to detect, and when you detect them, it's too late because they've already caused certain damage," said Rasheed. "And even if you detect them on the disk, they change in memory and they evade that detection."

Intel® Active Management Technology enables IT to remotely remediate compromised devices and remove them from the network if needed, limiting the fallout quickly and conveniently. Even in the case of operating system failure, the out-of-band capabilities of Intel Active Management Technology keep IT in control with minimal effort.

Hardware-hardened for a more protected enterprise

With hardware-enhanced security features like the Intel Authenticate solution and Intel Active Management Technology, IT security becomes more robust, powerful, and convenient. Out-of-the-box, easy-to-use security features harden the front lines of data protection in ways software alone can't, and do it in ways that don't hinder user productivity.

[1] https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017
[2] http://www.businessinsider.com/we-found-out-how-much-money-hackers-actually-make-2015-7

© Intel Corporation. Intel, the Intel logo, Intel Core, Intel vPro are trademarks of Intel Corporation in the U.S. and/or other countries.
Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.
No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com/windows10migration.
*Other names and brands may be claimed as the property of others.