A New Approach to Enterprise Security

How to Disrupt the Security Status Quo
Expand Security’s Role and Enable Business

The battle to keep business data and systems compliant and safe from increasingly sophisticated threats is now a decades-long struggle. For much of that struggle, enterprise computer users and even some business leaders have perceived security as a necessary evil—irritating and costly policies and practices that they must endure but which are secondary to the real mission of the business.

This attitude is beginning to change as business leaders recognize that good security practice is good business practice because of the prevalence of threats and the enormous cost of security failures. Today’s business environment is vastly different from the one in which outdated security models and perceptions evolved. For example, businesses are generating value and brand equity online using increasingly interconnected business strategies and processes. Organizations collaborate with each other, exchange sensitive data, and conduct business through many cloud-based services across many different platforms—including mobile devices which are highly susceptible to loss or theft. Because the attack surface is greater today and the risk and costs of breaches are so high, these realities have created an environment in which security practice is—and should be perceived as—an obvious business enabler as well as a mitigator of risk.

Speak Now—They’re Listening

Today’s environment of interconnected processes and increased collaboration creates new opportunities for enterprise security professionals. As organizations come to terms with the rising risk they face, security leaders like you have a chance to show business leaders—now newly receptive because of heightened risk—what has always been true: security does not detract from the bottom line. It is the framework that allows business to live and thrive.

Intel and a rich ecosystem of security partners have a vision for transforming security into a business enabler through a new, unified security framework. While securing enterprise data will always be challenging, this new framework can change the equation in your favor through a three-pronged implementation strategy:

1. Strengthen computing at its silicon roots without hindering the user experience by taking advantage of security features built into great platforms.
2. Deploy innovative software and services that take advantage of those hardware security features.
3. Enable business everywhere with protective capabilities that are consistent across devices from the data center to users’ pockets.

As the leading manufacturer of chips and processors, Intel is actively building toward this business-enabling framework by building security features directly into the silicon. This means that elements of this vision are available to businesses today. In fact, you probably already have platforms in your infrastructure that include hardware-assisted security features.

Disrupt the Security Equation

This new framework enables business by weaving security into the lowest levels of the computing stack. Throughout the history of the security wars, one component has remained relatively stable: the level nature of the battlefield. Software is your attackers’ primary weapon, and software has been your primary means of defense. Intel is working to disrupt that equation by turning platform hardware into a defensive ally.

Intel is building security into the computing foundation—the hardware. This approach strengthens software-based protection through security features encoded directly on the silicon where they are much more difficult to bypass or tamper with. When you deploy Intel platforms with built-in security, software and services can then take advantage of those embedded features, extending and enhancing the traditional protection offered by software alone.

Beyond Protection: A Secure Silicon Foundation Enables Business

Since the PC revolution, enterprise IT organizations, software vendors, and computer manufacturers have approached the problem of computer security through a software-only model. In this model, protection and security are provided by the operating system and the software running on top of it. Antivirus programs, user logon screens, and network access policies are examples of software-based attempts to detect malware and prevent unauthorized access to private information.

The software-only security model has served the enterprise well for the past three decades, but it is beginning to show signs of age. One challenge is that its paradigm is fundamentally reactive. For example, antivirus software scans for known threats or behavior that could indicate malware activity. As a result, IT professionals are left patching holes only after something important has leaked out or something or someone malicious has sneaked in.
Modern computing realities suggest a security approach that strengthens the software-only model by going underneath the operating system and software to the hardware foundation. Here, security features and trust are embedded into the silicon before a device leaves the factory, and then IT professionals can add software and services that take advantage of those embedded features.

In contrast to the reactive stance of the software-only model, a hardware-assisted approach helps you maintain a proactive posture. Because security is anchored in the hardware, stealthy malware and advanced persistent threats (APTs) have nowhere to hide, and encryption keys that protect identities and data are derived from the silicon, not software. This means that keys are never exposed to the operating system and applications, making them much less susceptible to compromise. This hardware-based approach establishes a root of trust anchored in the hardware so that identities, authentication, and access control are verified and trusted from the foundation—protecting users, virtual machines, networks, and data against unknown threats in addition to conventional attacks.

Intel platforms help users and workloads start secure when they are ready to go, run secure while going about their everyday tasks, and stay secure by protecting information wherever users or data roam—all without impeding the user experience or system computing capacity.

Reduce Risk—Start Secure

Though not without vulnerabilities, software has been an effective defense against a variety of threats. However, the software-only model accepts a level battlefield where defensive software struggles against attacking software. A hardware-assisted approach tips the balance in your favor by extending software’s reach with a security-hardened silicon foundation.

Stealthy malicious software, such as rootkits and other APTs, can entrench itself within or below the operating system where it is undetectable to most anti-malware software. It then reasserts itself each time a device reboots or wakes from a sleep state. Security features embedded in the hardware can protect pre-boot, boot, and wake processes before the operating system and protection software have loaded, strengthening your defenses against these types of attacks.

Enlist Hardware-Embedded Security to Reduce Risk and Cost

Reduce costs and complexity and enhance protection without impeding performance or user experience.

Safeguard compliance and productivity with hardware-embedded features during run-time.

Reduce risk with secure boot processes.

Figure 1: Intel platforms can help users and workloads start secure when they are ready to work, run secure while going about their everyday tasks or normal execution, and stay secure by protecting users and information across platforms.
Strengthen Compliance across the Continuum—Run Secure

When you start with a secure and trusted foundation, you can extend that protection up through the computing stack as workloads and day-to-day computing tasks take advantage of additional hardware-embedded features.

The proliferation of devices, connectivity, and services expands the potential attack surface and complicates the defense of enterprise assets when they are protected by software only. And when something gets through, the impact on IT organizations and enterprise bottom lines is considerable. Reimaging after an infection can take up to five hours per machine, derailing both the IT technician and the end user for a total of 10 hours in lost productivity and an estimated cost per reimaged endpoint of $585. If your organization has 5,000 endpoints, a mere one-percent infection rate could cost $30,000 in reimaging time alone.² Costs associated with compromise of sensitive data are much higher—$188 per record for an average overall cost of $5.4 million per breach.³

“Although the volume of [stealthy] threats is unlikely to approach that of simpler attacks on Windows* and applications, the impact of these complex attacks can be far more devastating. We expect to see more threats in this area during 2013.”

—McAfee Labs, “2013 Threats Predictions”¹

Intel platforms help users and workloads start, run, and stay secure wherever users and data roam—all without impeding the user experience or system computing capacity.

Intel platforms with hardware-embedded security features add crucial protection to data center workloads and the daily digital experience of users—whether they are inside the enterprise firewall or conducting personal business on mobile devices that they also use for work. These platforms provide a secure and verified foundation that strengthens security software and actively monitors hardware and firmware for unexpected behavior that might indicate a compromised system. Then, if something goes wrong, features embedded in the hardware can help isolate infected devices, which dramatically accelerates remediation, and helps limit risk and losses associated with infection and breaches. Because these features are embedded in the hardware, IT administrators can use them to strengthen security across the infrastructure with no discernible impact on user experience or workload performance.
Mitigate Risk by Securing Data and Users—Stay Secure

Improved security for workloads and day-to-day computing tasks is necessary but not sufficient. Organizations must also protect physical devices, corporate networks, and the information those devices and networks store or transmit.

Embedded security technologies inside Intel platforms harden protection for information and identities so that a stolen laptop doesn’t have to mean data breaches, compliance violations, and potential brand damage. These technologies can support and enhance strong multifactor authentication, which helps to prevent unauthorized access to corporate resources even if a username and password are compromised. They strengthen encryption, making it practically impossible for unauthorized people to view data on lost or stolen devices. They also accelerate encryption, making it less disruptive to the end user so that encryption can be used more widely. By accelerating some security tasks to the hardware, embedded security features on Intel platforms can help decrease software-based pressure on computing cores, which means that stronger security does not decrease user experience or system performance.

Time to Change the Rules of Engagement

Intel and its partners are working to transform enterprise computing’s security role from that of protector to indispensable business enabler. Toward that end, Intel is building security into the hardware foundation across all platforms that touch enterprise computing. Intel platforms include security features that are embedded into the silicon, which become anchors for hardened software and services that help your workloads and users start, run, and stay secure. This approach makes platform hardware a defensive ally rather than a neutral thoroughfare, extending the protective reach of the software-only approach.

Intel has identified four critical areas where security features embedded in the silicon can strengthen software-only protection:
- Threat mitigation
- Identity protection
- Data protection
- Resiliency

Amid all the uncertainty surrounding information security, two things are certain: security threats will continue to evolve and grow in sophistication, and no silver bullet will ever offer total infallible protection. However, a new security framework anchored in the silicon and extending upward through software and services can help tip the balance in your favor.

Visit us online to learn how embedded technologies can strengthen protection for business computing.

www.intel.com/enterprisesecurity/