Hardware-Enhanced Security
Change Your Security Paradigm to Enable Business while Reducing Risks and Costs
In a survey of enterprise users, 71 percent admitted to ignoring security policies meant to protect them, their devices, and corporate data.\(^1\)

This survey result matters for two reasons. First, because some of the most pressing security concerns business leaders like you face—from malware to data theft—pivot around user actions. But perhaps more importantly, the survey result shows one reason why enterprise information security can feel like an uphill struggle. Despite an ever-increasing attack surface, security practices are still sometimes perceived as obstacles to be circumvented. In part, this perception is fed by the fact that for the past three decades, enterprise security practitioners have countered software-based security threats with software-based defenses.

Today, Intel and its partners are working to change the software-versus-software equation to tip the balance in your favor. The new equation enhances software-based protection through a three-pronged security vision anchored in the hardware:

1. Strengthen computing at its silicon roots without impeding the user experience through security features built into great platforms.
2. Deploy innovative software and services that take advantage of those hardware-embedded security features.
3. Enable business everywhere with protective capabilities that are consistent across devices.

Some components of this vision are available to businesses today. In fact, you probably already have platforms in your infrastructure that include security features embedded in the hardware—an approach Intel calls hardware-assisted security. By deploying software and services that use these embedded security features, your organization can benefit from improved prevention and remediation of security vulnerabilities.

Intel is working to strengthen business protection by embedding security features into platform hardware across four fundamental pillars of enterprise security:

- **Anti-malware**: Malware finds nowhere to run or hide
- **Identity**: Simple access with enhanced security
- **Data protection**: Stronger protection keeps data safe in case of theft or loss
- **Resiliency**: Always-updated, robust systems

This paper describes some of the platform-embedded security features that compose these pillars and how these features can help to improve your organization’s security profile.

Security does not detract from the bottom line. Rather, it is the framework that allows businesses to live and thrive.

**The Role of Security Is Expanding**

Since the beginning of the information age, enterprises have treated security measures like fire extinguishers or protective clothing—necessary tools to prevent or limit damage, but secondary to the real mission of the business. Traditionally, even security professionals have taken a relatively narrow view of their role as protectors—a perception which corresponds to a relatively narrow charter. As a result, important security roles and measures are too often tacked on, incrementally and under pressure, to the last ten percent of a project. Perceived merely as a cost, security measures too often do not get the budget dollars or leadership time they need and deserve.

This attitude is beginning to change as business leaders recognize that good security practice is good business practice because of the evolving threat landscape and the enormous cost of security failures. Furthermore, today’s business environment is vastly different from the one in which outdated security models and perceptions evolved. For example, businesses generate value and conduct transactions online through increasingly interconnected business strategies and processes. Organizations collaborate with each other, exchange sensitive data, and conduct business through many cloud-based services...
embedding security features into the hardware across four fundamental pillars of enterprise security: anti-malware, identity, data protection, and resiliency.

The rest of this paper explores how hardware-assisted security enhances protection in these pillars.

**Anti-malware: Reduce Risk and Costs with Enhanced Protection**

The first area where hardware-assisted security can enhance your defenses is in protection from malware. A computing platform must start secure—from the moment the power button is pressed—so that processes occurring after boot can be trusted. Boot and wake from sleep are critical times for devices. During these seconds, computers are in a pre-operating system environment where code is executing but where security capabilities in the operating system and anti-malware software have not yet loaded. Malware developers have learned to insert code that exploits these environments and avoids traditional software-based detection. Even though software might detect some of these activities when it loads, stealthy malware hiding below the operating system can reassert itself upon next boot or wake from sleep. These stealthy attacks, also called advanced persistent threats (APTs), are growing as a source of risk. McAfee Labs reported more than 150,000 new rootkit samples during the fourth quarter of 2012.

Hardware-assisted security features built into computing platforms can help reduce risks and costs by strengthening your protection against APTs and other malware. These features span many different platforms—including mobile devices, which are highly susceptible to loss or theft.

Not only must enterprise security practitioners protect data and identities in this environment, but they must do so without impeding the end user experience, under increased regulatory pressure to protect privacy, and with a verifiable audit trail. These realities have created an environment in which the perceived role of information security practice must change from that of a supplemental protective layer to one of a proactive business enabler.

Information flow is fundamental to everything that enterprises do, and because information technology makes that flow possible, information technology is the enterprise nervous system. A strategy that integrates proven security practices with clear executional plans can keep that nervous system healthy and supports the flow of information on which the business depends.

Today's challenging security environment can also create opportunities for enterprise security professionals. As organizations come to terms with the rising risk they face, security practitioners have a chance to show business leaders—now newly receptive because of heightened risk—that security does not detract from the bottom line; it is the framework that allows businesses to live and thrive. Indeed, as security threats grow ever more sophisticated, security can become a vital differentiator that separates businesses that have evolved from those that have not.

A hardware-assisted approach across all platforms can help to support this expanded role for information security. Intel is working to strengthen security as a business enabler by enhancing security software and services, from the hardware up.
Boot and wake from sleep are critical times for devices. Code is executing but security capabilities in the operating system and anti-malware software have not yet loaded.

features start to protect users and information before the platforms are even turned on or awakened from a sleep state—before traditional software-based protections have a chance to load.

By reducing the number of infections, hardware platforms with built-in security can have a direct positive impact on the bottom line because cleanup is costly. 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 end points, a mere one-percent infection rate could cost $30,000 in reimaging time alone. Costs associated with compromise of sensitive data can add significantly to the overall costs—up to $188 per record for an average overall cost of $5.4 million per breach.

Technologies that strengthen software-based malware protection help each platform take advantage of a root of trust that is anchored in the hardware. Software and services can then build upon that foundation to create a more secure environment for workloads and users. If something or someone has tampered with a device’s BIOS, firmware, master boot record, or other low-level components, platforms with hardware-assisted security can identify and prevent the attempted tampering, stopping the attack before it spreads.

Trusted compute pools are an applied example of hardware-assisted security. A trusted compute pool is a collection of computing resources whose trust state has been measured and verified from the lowest levels of the computing stack. Each launch component on each server in the pool is measured against known good states. If a launch component does not match an approved state—for example, the bootblock is different than expected—the system can be excluded from the pool as “untrusted”. This approach allows organizations to deploy workloads to the cloud with greater confidence that the multitenant cloud environment has not compromised security for sensitive data and workloads.

Support Productivity through Stronger Anti-malware Protection

With a secure start provided by hardware-embedded security features, users and administrators can go about their daily business and allow workloads to execute with greater confidence. Software and services that take advantage of security features embedded in the hardware can more effectively protect users and workloads during day-to-day business activities, allowing them to stay productive. That’s because hardware-based security enables use cases that extend protection beyond what is possible through software only. For example, these features can help:

- Root out malware wherever it hides, even rootkits that persist below or within the operating system.
- Limit propagation of malware at the level of the network interface card (NIC).
- Decrease the likelihood that human error will open the door to an attack.
- Create more thorough and efficient detection capabilities.
- Create a trusted compute pool and define policies to ensure that sensitive workloads run only on trusted platforms.

Identity: Reduce Risk through Simpler, Stronger Authentication & Access

While detection and protection against malware are important, they are not enough by themselves. That’s why Intel’s second area of focus for hardware-assisted security is on identities and how users and customers access critical networks.

Today’s enterprise user is hyper-connected—always online using a variety of interconnected apps, services, and devices. This reality invites risk as data and identities are exposed to compromise through an attack surface that is expanding due to misuse, spyware, social engineering, weak passwords, and more. These risks apply to enterprise users and to your business customers who have accounts at any of your online properties. If customers’ accounts are hijacked, they won’t blame themselves for their weak passwords—they’ll blame your business and tell all their friends.

Ninety-three million identities were exposed in 2012 alone, and a simple online search returns dozens of news stories about data breaches. These conditions led security researchers Eric Grosse and Mayank Upadhyay to declare, “We contend that security and usability problems are intractable: it’s time to give up on elaborate password rules and look for something better.”

Safeguard Access to Protected Resources

“So something better” could be hardware-assisted two-factor authentication. Two-factor authentication (2FA) is stronger than traditional username and password authentication because it enhances logon security with another component, such as a one-time password generated by a hardware token. Despite its stronger protection, many organizations do not use 2FA because solutions can be costly and complex. They often require supplementary data center hardware and software that must be configured and managed.

Hardware-assisted security features can greatly simplify 2FA because they can generate one-time passwords traditionally generated by discrete tokens. In other words, the platform itself becomes the token. Software and services can then take advantage of this capability, enabling 2FA solutions that require neither separate fobs nor additional data center investment. Administrators can manage these solutions centrally and eliminate the hassle of configuring and deploying hardware tokens, which are easily lost or stolen, and users can remain productive with a fluid user experience and non-intrusive security measures.

Simplify and Strengthen Authentication for Users and Customers

Intel® Identity Protection Technology (Intel® IPT), which supports hardware-embedded tokens and digital certificates, helps simplify secure authentication without distinct fobs that must be managed separately. By using Intel IPT with Public Key Infrastructure (PKI), you can eliminate the need to purchase and support costly physical smart cards. You can further enhance user logon security with Protected Transaction Display (PTD), a hardware-embedded feature that generates a randomized on-screen keypad that hides user input from screen-scraping malware and proves human presence at the computer, which helps thwart some types of attacks.
In addition to 2FA, these features, along with software and services from Intel partners, enable simpler public key infrastructure (PKI) systems. These systems provide extended security capabilities such as e-mail encryption and document signing—all without additional data center complexity and user burden.

**Data Protection: Improve Compliance and Reduce Risk with Stronger, Faster Encryption**

Data protection is the third area of focus for hardware-assisted security. In addition to protecting IT assets against malware and hackers, information security practitioners must also protect data and the devices running applications that touch the data. This is no small task, given the rapid proliferation of devices and the services they access.

- Of the 93 million identity exposures in 2012, most were a result of theft or loss of the device on which sensitive data were stored.²
- Mobile users who access phishing websites are three times more likely to submit their logon info than desktop users.⁷
- The number of password-stealing Trojans grew by 74 percent in the fourth quarter of 2012.²

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

These data points emphasize what security practitioners face every day: sophisticated, targeted attempts to steal sensitive information. In addition, attacks on trust—in the underlying, invisible systems on which secure exchange relies, such as certificate authorities and Secure Shell (SSH)—are a growing threat. A Ponemon analysis estimates that “failed key and certificate management threatens every global enterprise with potential cost exposure of almost U.S. $400M.”⁸

“A few kilobytes of cryptographic data is all that stands in the way of millions lost in sales, grounded airplanes, and closed borders.”

—Ponemon Institute, “2013 Annual Cost of Failed Trust Report: Threats and Attacks.”⁸

Data encryption is a necessary step in mitigating risks while protecting data. Embedded security features and instructions on Intel platforms can strengthen data protection by accelerating software-based encryption in important ways:

- They accelerate data encryption so that greater security does not impact performance.
- They provide a more robust digital random number generation (DRNG) to make encryption more difficult to crack.
- They store cryptographic keys in a secure chip so that keys are never exposed to malware that might be running on a system.
Resiliency: Return Users to Productivity Faster

Experience has shown that no matter how careful you are or how many security layers you have in place, security incidents are still going to occur. User carelessness could lead to an infection; devices get stolen; people work around security practices to do their jobs.

However, a security incident does not have to become a threat to the bottom line. The fourth area of focus for hardware-assisted security is resiliency. Intel embeds features in platform hardware that help you stop a breach or infection, limit the damage, and allow users to quickly return to productivity.

When something gets through, the impact on IT organizations and enterprise bottom lines is fast and considerable. Security incidents such as malware infections often require a desk-side visit by a support technician, which contributes to high help desk costs. In fact, while relatively few help desk requests (including security events) require a desk-side visit, those instances consume a disproportionately large percentage of help desk budget because desk-side visits are costly.

You need a reliable way to remediate security incidents from the data center before they spin out of control. Your organization can reduce costs and risks associated with security incidents through remote manageable powered by hardware-embedded features on Intel platforms. These embedded features can help administrators:

- Identify infections, including advanced malware, in near-real time
- Quickly block threats and isolate infected devices
- Dramatically accelerate remediation through remote manageability and repair, including remote boot from network, remote keyboard, video, and mouse capability, and more

The Intel IT department estimates that in certain scenarios, hardware-assisted resiliency features will enable a 10 times faster response time for the help desk and a 10 times faster return to productivity for users.³

Unite Security and the Bottom Line

Revolutions in business computing during the past two decades mean that risk is pervasive and growing, touching every facet of the enterprise infrastructure. Despite this sobering reality, enterprise security professionals can re-invigorate security practice by explicitly realigning their mission with business goals. As Malcolm Harkins, Intel Chief Security and Privacy Officer, states in his book Protect to Enable, security practitioners exist “to enable business—to help deliver IT capabilities that provide competitive differentiation.”⁴ Sound information security strategy enables business because it helps to mitigate risk and ensure compliance, while opening doors to new initiatives that can engage customers and increase productivity and efficiency.

Intel is working to empower security practitioners to fulfill their mission as business enablers by embedding security features in the platform hardware of devices across the enterprise. You can then deploy innovative software and services that take advantage of those features to extend protection beyond that offered by software alone. This approach can help unite security practices and business interests by shifting the conversation from one of technical protections needed to one of business benefits gained.

For this strategy to be effective, security can’t be treated as an after-thought or “fix” that is bolted onto a solution during deployment. Instead, security considerations need to be an integrated part of the planning phases for all IT and line of business (LOB) projects. When security is included in the planning and budgeting for new initiatives, protections can be designed into solutions in a way that lets you control the balance between comprehensive security, cost-effectiveness, and a rich user experience. That approach helps you manage risk more effectively while freeing your business to pursue new opportunities.
To learn more about the four critical areas where features embedded in the silicon can strengthen protection, visit Intel online at www.intel.com/enterprisesecurity.