Executive Summary

Data breaches have become so commonplace that many of us no longer flinch when we see another news story on thousands or even millions of records, identities, or credit card numbers stolen. But to security practitioners responsible for ensuring the health of their businesses, every breach is another reminder to check and re-check their companies’ defenses. In a recent U.S. study, the average organizational cost of a data breach for participants exceeded $5.4 million.¹ For some businesses, even a single incident of that magnitude could be crippling.

Despite these high and ever-rising costs, technology hasn’t kept pace with the growing security challenge. For every new firewall or anti-malware deployment, cybercriminals seem to find new vulnerabilities or approaches to infiltrate the new fortifications. In addition, the challenge is exacerbated by an ever-expanding attack surface comprised of mobile devices, laptops, clouds, and ubiquitous wireless connectivity. Without constant vigilance, your workforce, customers, and partners risk theft of sensitive data, and your company risks laborious and costly remediation efforts, in addition to potential damage to its reputation.

Security practitioners have fought back with determination, but many of the software-only solutions they rely upon are insufficient to meet today’s challenges. Simple user name and password schemes, for example, suffer from weak or frequently reused passwords that can’t protect users from modern tactics like spear phishing that use easily-obtainable personal information to target users. Software-based encryption offers another approach to safeguarding data, but encryption keys stored in software might be vulnerable to cybercriminals. Even when solutions are effective, they shouldn’t provide security at the expense of performance or user experience. If users are hindered or frustrated by poor performance on their device, the IT administrators will be the first to hear about it. In fact, many organizations limit or avoid deployment of encryption because the performance impact is unacceptable for widespread use. That tug-of-war between security and performance fights against your intrinsic need to reduce risk and keep your enterprise safe and productive.

Intel and its partners are offering a new approach to data protection that embeds security in the hardware of platforms powered by Intel® architecture: from the data center to users’ pockets. Hardware-enhanced security gives your business an advantage over software-only solutions by strengthening the security of endpoints and better protecting data at rest, in use, or in motion, without dragging down performance. When you reduce risk and complexity, you can decrease remediation costs, improve productivity, and increase confidence in meeting regulatory compliance mandates.
Your Sensitive Data Might Already Be Compromised

Rakesh is the head of engineering for a large aerospace manufacturing company. After arriving at the office one morning, he sits down at the computer with a cup of coffee and reviews new and updated equipment designs from his team. When finished, he goes online to do a weekly scan of his competitors’ designs. He nearly drops his coffee in astonishment when he sees several complex machine parts for sale by a major competitor that are all based on newly developed, unreleased designs by his engineering team! His company had not yet manufactured—or even filed patents—on these particular plans, which were drafted only a few weeks ago. Rakesh can’t figure out how the other company obtained the confidential information.

It takes several weeks of sleuthing, but the IT security team from Rakesh’s company eventually connects the intellectual property theft to an unprotected hard drive on a laptop that was stolen from an employee’s car. As the competitor company reaps enormous sales gains from the theft, Rakesh’s firm now faces potentially crippling financial damages from revenue losses.

Unfortunately, Rakesh’s nightmare isn’t an anomaly. In May 2013, a federal commission estimated that theft of intellectual property from the United States is costing the nation an estimated $300 billion each year. Of course, intellectual property isn’t the only thing cybercriminals are targeting, but whether it’s bank account information, confidential customer data, or other sensitive materials, the organizational costs of stolen data are significant and are increasing. According to a recent PwC global survey of executives, average losses for 2013 were up 18 percent over 2012, with bigger losses increasing faster than smaller ones.
Protect Your Data from Prying Eyes

What are the underlying causes for this growing security challenge? Some of the increase is due to the growing sophistication of cybercriminals, who are employing much more complex and stealthy techniques. But the situation is aggravated by a growing attack surface comprised of mobile devices, laptops, clouds, and ubiquitous wireless connectivity. Without constant attention, your workforce, customers, and partners risk theft of sensitive data, and your company risks time-consuming, costly remediation efforts, in addition to potential damage to its reputation. Diligent security practitioners have faced the onslaught of threats with determination, but it’s not easy to keep up while also responding to changing business needs and new technologies.

66% of data breaches took months or even years to discover.4

When the risks to your business are this high, how can you respond more effectively and proactively without hindering your business? Many existing solutions for protecting data rely on simple user name and password schemes to protect access to devices. But weak or frequently reused passwords are inadequate to protect users from modern tactics such as spear phishing, which uses easily-obtainable personal information to target users. Schemes like this give the bad guys a significant advantage, because they only need one careless or uninformed user to open a targeted e-mail and run a malware-laden attachment to conceivably put your entire enterprise at risk.

Software-based encryption offers one approach to safeguarding data on devices, but also has limitations. For example, encryption keys stored in software might be vulnerable to cybercriminals. In addition, many encryption solutions add processing overhead that negatively impacts performance for users. In fact, many organizations limit their use of encryption to a small subset of drives with sensitive data because the performance hit is unacceptable for widespread use.

Given how pervasive and potentially costly the security risks are, most enterprises would clearly welcome a new, more effective tactic for stronger security and enhanced data protection.

Disrupting the Status Quo

Intel and its partners are upsetting the software-versus-software balance with a new approach to data protection that embeds security in the hardware of platforms powered by Intel architecture: from the data center to users’ pockets. Rooting data protection in the chipset gives your business an increased advantage over software-only solutions by hardening security of endpoints and providing a safer, more seamless experience for users without dragging down performance. This hardware-enhanced approach can also help you reduce risk by allowing you to safeguard data even if a device is lost or stolen, or if access protections are compromised. When you reduce risk and complexity, you decrease remediation costs, improve productivity, and increase confidence in meeting regulatory compliance mandates.

Protection with Performance

The days of locking down data in the data center are long gone. Today’s reality is one of mobile, hyper-connected users on multiple devices, working from any location at almost any hour, connecting to both enterprise-managed data centers and private or public clouds. That means confidential data is always on the move, migrating from device to device and location to location. In order to better protect sensitive information in this fluid environment, you need a way to provide endpoints with the strongest protections possible, without sacrificing the experience and productivity gains users expect. By embedding security technologies into the chipset, Intel enables strong, hardware-enhanced data protection features on fast, efficient platforms powered by Intel® Xeon® processors, Intel® Core™ processors, and Intel® Atom™ processors. Unique hardware-enhanced technologies accelerate cryptographic processes and generate more secure keys for encryption so you can deploy the strongest encryption and authentication methods possible without a noticeable impact to your users.
Accelerate Cryptography

To meet today’s growing threats and achieve regulatory compliance, security practitioners are turning more and more to solutions that engage encryption and stronger authentication in various forms. Solutions such as Secure Sockets Layer (SSL) transactions, RSA encryption, secure hash algorithm (SHA)-based authentication, and many other security protocols rely on cryptographic operations that require complex, processor-intensive mathematics, which can often drag down performance for users. Any time endpoint performance is adversely affected, user experience degrades and administrators grow more reluctant to deploy the security protocol—even when the benefits would be significant.

The latest generation Intel Core processors and Intel Atom processors include a variety of new instructions built directly into the chipset to accelerate the large integer arithmetic required by public key cryptography.

Efficient Encryption and Decryption

To better protect your assets, identities, and reputation, you need a way to deploy strong data encryption across all client devices. Unfortunately, many organizations are hesitant to widely deploy encryption because it can significantly impair performance. Advanced Encryption Standard (AES), for example, has been used worldwide for years as a highly effective solution for protecting data, but the AES encryption and decryption operations can be resource intensive.

To address this challenge, Intel has developed Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI), an instruction set found in Intel Core processors and latest-generation Intel Atom processors, which helps increase encryption and decryption performance and reduce processor load. By implementing some intensive sub-steps of the AES algorithm into the hardware, AES-NI accelerates execution of the AES software application, while also reducing vulnerability to side-channel attacks.

AES-NI helps eliminate barriers to widespread adoption of encryption by contributing to significantly reduced performance bottlenecks. This can boost your ability to protect your data, even in the event of a lost or stolen device. But AES-NI is only one of several hardware-enhanced Intel technologies that help enhance cryptographic performance on devices powered by Intel Core processors and Intel Atom processors. For example:

- ADCX and ADOX instructions help accelerate implementations of the large integer arithmetic used in public key cryptography.
- RORX and MULX can provide performance increases from new instructions, microarchitecture improvements, and innovative software implementations.
- Intel® PCLMULQDQ instruction performs carry-less multiplication of two 64-bit operands, which can help significantly accelerate secure computing. PCLMULQDQ also works in conjunction with AES-NI to help accelerate AES encryption performance.

Simply stated, these and other Intel hardware-enhanced improvements can help accelerate performance for a wide range of security technologies, which frees your organization to implement multiple layers of authentication and encryption with minimal noticeable impact to users.
Protecting Data with Speed, Efficiency, and Usability

Whether they’re after money, secrets, or other sensitive information, data theft is the goal of many cybercriminals. Every month, there are news reports of large-scale credit card thefts, industrial espionage, or loss of confidential customer information. One major breach can be devastating to both finances and reputation. With the stakes this high, data protection has become a critical defensive layer in nearly all enterprise initiatives. As a result, security professionals now find themselves as the driving force in enabling business by mitigating risks, reducing costs, ensuring compliance, and eliminating barriers to efficiency and productivity. Intel helps security practitioners like you fulfill your mission by embedding security features in the platform hardware of devices across the enterprise.

This innovative approach is the key to stronger data protection in the enterprise. Data is vulnerable across all aspects of computing, whether at rest, in motion, or in use. By strengthening and accelerating cryptographic processes, Intel helps you deploy strong, efficient encryption across all your devices. That way, even if the bad guys break through your defenses, they still can’t get your data.

Visit www.intel.com/enterprisesecurity/ to learn more.

Strengthen Encryption with Stronger Keys

Encryption relies on strong cryptographic keys for security. Most encryption products create those keys using software-based random number generators (RNGs). Keys generated with RNG protocols can be more vulnerable to attack because they are frequently based on algorithms that create predictable or poor quality random numbers. Intel encryption takes a different approach for generating stronger cryptographic keys by using Intel® Data Protection Technology with Secure Key: a digital random number generator that creates more secure, truly random numbers directly on the processor chip. The enhanced strength of digital RNGs created with Secure Key can be used by applications to help ensure compliance with industry security standards, such as the Health Insurance Portability and Accountability Act (HIPAA) or Federal Information Processing Standards (FIPS).

<table>
<thead>
<tr>
<th>Intel Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Data Protection Technology with AES-NI®</td>
<td>Helps accelerate performance of industry-standard AES encryption, which can help remove performance barriers for widespread deployment of full disk encryption.</td>
</tr>
<tr>
<td>Intel® Data Protection Technology with Secure Key</td>
<td>True digital random number generator with keys created more securely in the hardware.</td>
</tr>
</tbody>
</table>

Table 1: Intel hardware-enhanced technologies help protect data with strong security and efficiency

Protecting Data from Prying Eyes

Security practitioners exist “to enable business—to help deliver IT capabilities that provide competitive differentiation.”

- Malcolm Harkins, Intel Chief Security and Privacy Officer

![Figure 2: Intel® Data Protection Technology with Secure Key helps harden security by generating strong, digital random numbers](image)
Protect Your Data from Prying Eyes