WHITE PAPER

PRESENTED BY intel

How New Computers Raise the Bar for Endpoint Security Protection

Executive Summary

Cybersecurity threats have never been greater, as hackers constantly launch new variations on malware, such as the recently discovered WannaCry and NotPetya. To combat these threats, businesses need to step up their security measures, including both hardware and software tools, from end-to-end encryption to multifactor authentication and beyond.

> "Cybercrime is fast becoming the number one risk for companies, absorbing greater resources and management time. The reputational cost of getting this wrong can be significant, so it's vital businesses commit the appropriate resources."
>
> — Charlie Huggins
> Fund Manager
> Hargreaves Lansdown

Cybersecurity has never been a bigger, more costly issue in IT and business. For hackers, business is booming. Take ransomware, their latest weapon of choice: Attacks leapt from 3.8 million in 2015 to 638 million last year, according to SonicWall,* a leap of more than 16,000%.

In 2017, the threat got even worse. From targeting individual organizations, ransomware went global. The WannaCry attack on May 12 hit 200,000 enterprises across 150 countries, including large sections of Britain's National Health Service* (NHS). WannaCry was luckily stopped in its tracks by a 22-year-old British security researcher, Marcus Hutchins, who discovered a careless "kill switch" in the code. By then, however, the attack had already caused an estimated $10 million in damages.

Just one month later, hackers came back with more resilient ransomware. The NotPetya campaign began June 27 and spread through 60 countries, causing some $850 million in losses to victims including international consumer goods provider Reckitt Benckiser*, shipping giant A.P. Moller-Maersk*, and global advertising agency WPP*. The attack was so severe that it took days—even weeks—for some companies to fully restore their services.

These global attacks have been a wake-up call for businesses.

As Charlie Huggins, fund manager at Hargreaves Lansdown*, told *The Guardian*, "Cybercrime is fast becoming the number one risk for companies, absorbing greater resources and management time. The reputational cost of getting this wrong can be significant, so it's vital businesses commit the appropriate resources."

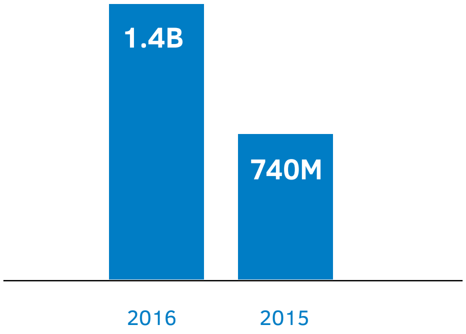
The art of defense: software and hardware in harmony

Other than continue training their staff to be security-savvy and upgrading to the latest security software updates, many organizations will wonder what more they can do. Meanwhile, they hope that they aren't the ones to suffer as the ongoing "arms race" between hackers and defenders continues—where the criminals find new software flaws and suppliers rush to patch them.

Yet while this defense effort is essential, it is endless. It has become increasingly clear that this old way of doing things

+86%

Nearly 1.4 billion data records were lost or stolen in 2016, compared with 740 million in 2015, **an increase of 86%.**



just isn't working. Some 90% of cybercrime incidents in 2016 resulted from software vulnerabilities.

Sticking with software-centric solutions only provides one-dimensional protection. Experts in the information security community have recognized that a multilayered approach is needed to reduce data breaches. Such an approach includes security embedded in both software and hardware, as well as tougher user identity checks, so hackers can no longer break into corporate networks by simply stealing usernames and passwords in the millions.

The latest *Breach Level Index* report from security solutions provider Gemalto* points out that almost 1.4 billion data records were lost or stolen in 2016, compared with 740 million in 2015, an increase of 86%.

"Given this trend that has developed with identify theft as the leading attack model for breaches, it's clear that companies are not doing enough to address this threat," the report states.

Echoing this report, Microsoft*'s Malware Protection Center response team wrote just after NotPetya struck: "The ever-increasing sophistication of ransomware attacks [means] a multi-layer defense stack is needed to protect computers and networks."

And Ryan Wilk, a director at NuData Security*, has said, "There is a definite need for a multilayered approach that includes the need to build systems from the ground up that protect users and data through multifactor authentication."

Silicon strength

So, what could this more robust security approach look like? One way forward is being offered by Intel® and a number of Intel-based PC and device manufacturers, including HP*, Lenovo*, Dell*, and others.

The latest generation Intel® Core™ vPro™ processor-based devices bake identity and data protection into the hardware itself. These security solutions deal with the main weaknesses in current malware protection:

- They strengthen user authentication to curb hackers using stolen credentials—still the main cause of data breaches.
- They protect data, even when it's used by an increasingly mobile workforce, outside the company perimeter and firewalls.
- They make it easier for organizations to recover from attacks by quickly isolating infected devices.

As Tom Garrison, Vice President of the Client Computing Group and General Manager of Connected Home & Commercial Client at Intel Corporation, says, "Our focus is to deliver customers the solutions they need to fight against identity and data breaches. We have a unique approach building these capabilities in the hardware, which reduces exposure to software-level attacks, where the majority of threats happen today."

Stronger user identity checks

Among the new hardware-based solutions, Intel® Authenticate solution targets the biggest security threat for organizations—hackers using stolen or weak passwords to get into the corporate network. This threat was the cause of more than 80% of hacking-related breaches in 2017 according to Verizon*'s *Data Breach Investigations* report.

Cybercriminals know that organizations have a multitude of vulnerable entry points that they can target—every "endpoint" or end-user device connected to their network. Using employee names and stolen or weak passwords is the easiest way to unlock one of these doors, which is why these credentials are so coveted and so commonly used in security breaches.

After all, it's well known that in protecting this mass of entry points, employers

“With the Intel Authenticate solution, we’ve set out to help solve identity breaches in the most aggressive way possible for enterprises.”

— Tom Garrison
Vice President, Client Computing Group
General Manager, Connected Home & Commercial Client
Intel Corporation

must be protected all the time while hackers need to get lucky just once. And when malware gets a foot in the door, it can launch attacks to harvest information or encrypt data and hold the company for ransom. In short, malware then becomes a business nightmare.

To help organizations better guard against identity theft, the Intel Authenticate solution strengthens employee logins below the reach of software attacks. In addition, it offers stronger multifactor user authentication—because more factors equal more security. Instead of using just a name and password, Intel Authenticate solution combines “something you know” (a PIN or password) with “something you are” (biometrics such as fingerprints), “something you have” (a smartphone or badge), and “somewhere you are” (location). This type of solution simultaneously delivers both increased security and the perception of easier log-ons for users.

The range of “factors” supported by the Intel Authenticate solution means companies can customize it to suit their specific business needs. It also takes multifactor authentication a step further by anchoring company security policy, credential keys, and certificates below the software layer in the Intel Core vPro processors—farther from sight and the reach of hackers.

“With the Intel Authenticate solution, we’ve set out to help solve identity breaches in the most aggressive way possible for enterprises,” reveals Garrison.

Recovering from attacks

If a data breach does occur, the Intel® Active Management Technology (AMT) in the latest generation Intel Core vPro processor-based computers helps companies stop the virus from spreading. Using Intel Active Management Technology, IT staff can isolate any infected devices remotely and take them off the network, sometimes even if the operating system is down or a device is powered off, without costly desk-side support.

“Partners like Accenture* estimate that Intel Active Management Technology, built into the Intel vPro platform, results in a 34% cost savings for IT,” explains Garrison.

Assurance at scale

Another feature in today’s PCs powered by the latest generation Intel Core vPro processors helps large enterprises whose task is to deal with hundreds or thousands of endpoint devices. For these companies, managing hardware and software consistency is a major challenge, and the Intel® Stable Image Platform Program (SIPP) brings opportunities for better IT standardization.

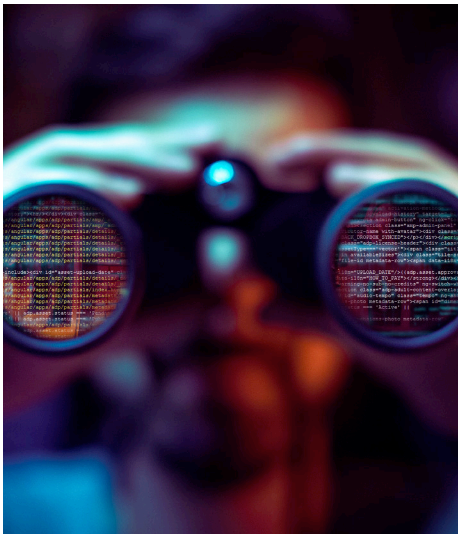
Through SIPP, all devices running the latest Intel Core vPro processors maintain the same software image across a network of drivers, the operating system, and applications. This configuration helps avoid incompatibilities between hardware and software, and reduces the costs of validation tests and platform configurations—while also minimizing disruption for IT teams.

The SIPP program also limits any major changes to key platform components and drivers for up to 15 months while Intel announces plans for new chip generations in advance. This program helps IT departments minimize the changes they need to make and the variables they need to deal with.

Reasons to change

This range of multilevel security and authentication built into the Intel vPro platform gives companies a way forward just as the impact of data breaches is becoming increasingly clear—both short and long-term.

Businesses obviously face immediate costs and consequences when they are breached. The NotPetya attack, for example, gave Nurofen maker Reckitt Benckiser a huge headache: disrupted production,



delays in product deliveries, and some permanent loss of revenue, estimated by *The Guardian* at around 100 million British pounds. Likewise, the *Financial Times* reported that shipping giant Maersk* was forced by NotPetya to reroute ships, could not dock or unload containers at some of its 76 ports, and had to suspend its main order-taking platforms for six days.

We are now also beginning to understand a permanent impact from data breaches. The April 2017 *Cyber Value-Connection* report from IT consulting firm CGI* and Oxford Economics* was the first to gauge the full share price cost. It found that valuations fall by an average 1.8% on a permanent basis following a severe breach. In some cases, breaches have wiped as much as 15% off affected companies' valuations.

Future prospects are also bleak. Following the latest global ransomware campaigns, a July 2017 report by Lloyd's of London* and security firm Cyence* for the first time calculated the economic impact of other likely large-scale cyberattacks. The estimated cost of one plausible scenario, hacktivists causing a mass outage at a global cloud service provider, was a staggering $53 billion—roughly equal to the cost of damage caused by Hurricane Sandy in 2012. That puts cybersecurity risk on a par with natural disasters.

Closing the door on hackers

In the face of these risks, Intel has secured widespread industry support for its strategy to build hardware-based security enhancements into enterprise PCs with the latest Intel Core vPro processors.

These new Intel-powered devices add strong security at the level of firmware and silicon to help organizations secure their endpoints and lock down their front lines. Just as burglars often walk through the front door of homes, every endpoint device across an organization is a door that gives hackers an opportunity to break in.

When companies simply update the security software on their devices, they essentially change the locks on the doors. That helps, but it doesn't address the real problem: It's easier to pick or bypass a lock than it is to break down a reinforced steel door. In the case of endpoints, silicon is the steel, and upgrading to new devices with Intel Authenticate and Intel Data Guard reinforces corporate doors.

Upgrading to new devices powered by latest generation Intel Core vPro processors doesn't only improve performance, it offers businesses an entire platform of hardware-enhanced security solutions.

Learn more at **Intel.com/EndPointSecurity**

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 Intel.com/endpointsecurity.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps www.intel.com/EndPointSecurity.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.