Research

October 2021

The Payback of Hardware-Enabled Endpoint Security

A J.Gold Associates Research Report
An Independent Study Sponsored by Intel

"This report will discuss the implications of deploying the latest generation of enterprise-class endpoint processors and how they significantly increase the security and privacy of enterprise environments.... The end goal of this report is to provide organizations with a path to being more secure while also reducing cost and potential security threats and liabilities....."

J.Gold Associates

Contents

Introduction

Organizations large and small have transformed to reflect the needs of an increasingly remote workforce. Indeed, digital transformation, once thought to move at a snail's pace, has moved farther in the past year than most thought would happen in 3-4 years. This transformation included an accelerated adoption of cloud-based "as a service" implementations to handle increasingly diverse workforce and access devices. Not only are more employees working remotely, but new tools like video conferencing, broad-based collaboration toolsets, next generation Workspace solutions, and newly emerging wellness apps have all been deployed to better enable remote workers and keep them productive while also making the dispersed workplace more cohesive.

> ***TREND**: Security remains an ongoing battle with companies trying to keep ahead of bad actors. This is especially true as enterprises struggle with implementing a Hybrid Workplace due to pandemic related shutdowns and a need for remote work. While many companies reacted with quick-fix implementations, in the next 2-3 years, enterprises must establish a strategy for fully hybrid work, while also protecting against new threats enabled by the move from centralized worksites to large numbers of remote connections and endpoints. We expect 65% of organizations to offer at least some remote work indefinitely. This requires reevaluating the entire security profile, starting with user endpoints.*
> *J.Gold Associates LLC.*

While many of these tools started out as remote work only products, the ability to morph into full collaboration suites in a relatively short time means they will remain in use even if remote work is reduced or even ceases all together, which we don't expect to happen for the foreseeable future. This means that infrastructure, and especially the user endpoints, must be optimized for this new environment.

But many organizations struggled to move quickly towards the new work reality, often with compromises to security strategies and long held infrastructure standards. This included the use of older computers that did not have the latest generation of security features and enhancements supported in the hardware. Indeed, many companies, out of necessity, even allowed employees to use their own personal PCs in an attempt to make sure everyone was able to stay productive. But this compromise of security best practices, and in some cases the use of outdated equipment, increased the likelihood of hacks and security breaches. This must not remain as a long term solution.

This report will discuss the implications of deploying the latest generation of enterprise-class endpoint processors and how they significantly increase the security and privacy of enterprise environments. The report will identify many of the risks and offer insights into what kinds of threats exist and how they impact organizations. Finally we will show that enterprises can obtain a significant ROI by upgrading to the latest generation of security enhanced PC processors and deploying them within the organization. The end goal of this report is to provide organizations with a path to being more secure while also reducing both cost and potential security threats and liabilities.

Shifting to a Hybrid Workplace

The days of exclusively on-premise workers are likely a thing of the past for most organizations. Workplace transformation into a hybrid model of “work from anywhere” as a result of the pandemic has taken hold. New modes of work require enhanced security and manageability, especially on remotely connected machines. Old best practices need to be updated to the new work realities. We estimate that the workplace shifts caused by the pandemic will continue for the foreseeable future, with some organizations never going back to full time office situations. Indeed, we expect that greater than 65% of organizations will continue some form of Hybrid Workplace capability indefinitely, allowing a significant portion of their workforce to work remotely at least part time. And this style of work will have significant implications for enterprise security.

Hybrid Work versus Security

Not everything goes smoothly when it comes to organizations implementing a remote workplace capability. In the early phases, enterprises often made compromises to get up and running quickly, especially around security of devices connected to the corporate network, as well as diluting many long term security best practices that in many cases were not ready for the new environment. There have recently been a number of studies that show the extent and effect of the new hybrid workplace model on security and data breaches, including:

In IBM’s *Cost of a Data Breach Report, 2020*,

- 76% of respondents said that remote work would increase the time to identify and contain a data breach
- 70% said remote work would increase the cost of a data breach.

And In Microsoft’s *Digital Defense Report, September 2020*, the top five security-related concerns expressed by both the CISO and C-suite executives regarding remote work were:

- Remote workers making choices that reduce security (58% CISO, 60% C-Suite)
- Securing personal devices for remote work (42% CISO, 45% C-Suite)
- Increase in Phishing campaigns and identity fraud (45% CISO, 44% C-Suite)
- Making compromises in security to accommodate remote work (39% CISO, 34% C-Suite)
- Attackers shifting focus to network/VPN infrastructure (31% CISO, 34% C-Suite)
- Interestingly, very few thought there would be a decrease in productivity owing to negative impacts of extra security measures (8% CISO, 12% C-Suite)

Clearly the impact of remote working and hybrid workplaces requires companies to look at the security of remote connectivity as well as the security of their endpoints much more closely than if everything was operating in a controlled on-premises workplace. Keeping the workplace technology up to date is mission critical, yet many enterprises compromise on this creating significant potential risks.

Keeping Tech Refreshed

In the early days of the pandemic, many organizations had to improvise in order to deal with the new realities brought on by lockdowns and remote work. Indeed, many relied on existing technology meant for traditional work styles to implement their new requirements for any worker, any location, and any device. But keeping the old technology in play can result in a significant security exposure.

According to the *Cisco 2021 Security Outcomes Study*:

> *"A proactive tech refresh strategy increases the chance of reporting a successful security program by roughly 11% to 15%".*

While this is a modest improvement and doesn't sound like very much, as we will see later, the cost of a data breach is very high, and even such a modest improvement can offer a large payback.

Old Tech was Required to Keep the Business Running

We estimate that at least 35% of enterprise endpoints deployed at the start of the pandemic were "old tech" that were at least 3 generations behind the current offerings, and therefore much more likely to be a security risk. This increased security risk is a function both of the deficits in older hardware-based security implementations, as well as the lack of some operating system security features fully supported only in newer equipment. Indeed, with many organizations allowing end users to work from their own personal machines, often based on a necessity to get something for their employees to work on, the ability to make sure each machine is up to date and secure was significantly compromised. Over time, this was mitigated by many enterprises replacing personal devices with corporate obtained and managed machines. But there are still a significant number of companies that rely on older devices to empower their workers, and this is problematic. And while the rate of newer machines being deployed to end users has increased, we estimate that at least 25% of currently deployed enterprise machines are 3 or more generations behind the current generation of hardware.

Implications for Security

While the endpoint device is not the only exposure companies face from bad actors attempting to hack the organization, it is a major path of entry for data breaches to occur. In *Verizon's 2020 Data Breach Investigation Report*, they found;

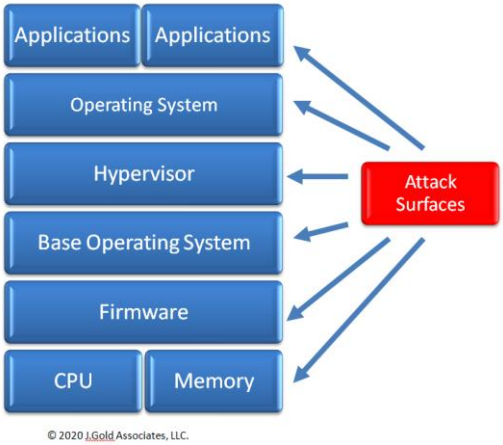
- Approximately 30% of all data breaches they investigated were due to desktop/laptop vulnerabilities.

This is especially problematic when you consider that many companies refresh their endpoints on a 4-5 year cycle, or even worse – replacing the device only when a machine breaks. Such old technology, even if it includes necessary updates of the Operating System, still contains many vulnerabilities that newer processor technology mitigates. Aside from the major performance improvements available from deploying newer technology, the security implications of keeping older machines in use are troubling.

Security Starts with a Security-Enhanced Processor Platform

The most important first line of defense is in the capabilities inherent in the processor platform powering the device. Modern systems offer multiple potential attack surfaces.

Figure 1: Mulitple Potential Computer Attack Surfaces



The good news is many of these attack surfaces can be better protected by deploying the latest generation of processors. Newer generation platforms have added a significant number of hardware features and accelerators to fight attacks from bad actors and help secure the data being processed. Among the critical capabilities inherent in the processor platform are the features/functions indicated in Table 1 below. This is meant to be an overview of features and not an exhaustive list, but it represents a guideline of what organizations should require when deploying machines to their workforce.

Table 1: Processor Platform Security Optimization Functions

Features/Functions
Pre-Boot – full health check before startup, including root of trust, verification of boot, verified boot loader
Platform Update Support - secure firmware/BIOS updates, integrity checking, remote management
Trusted Execution Environment - virtualization instructions, protected memory execution/isolation, secured access
Provisioning/Policy Enforcement Tools - configurations, encryption, device components enabled (camera, etc.), enrollment, network access, VPN, remote operation and updating
Advanced Threat Protection - HW supported advanced threat protection against threats like Ransomware and Cryptomining, secure GPU offloads for protected processes
Cryptographic Extensions/Services - HW accelerated Encryption/Decryption, Secure Key Storage, random key generation, public/private keys

While some of these features may be available in older processors, the majority, and certainly the highest functionality and most critical of them are only available on very recent processor platforms. Its important to note that the amount of security available when all of these components are in place is significantly greater than if only that individual feature was available on the device. Indeed, overall security is greater than the sum of the parts. As added layers of protection are included the overall security improvement multiplies in a non linear fashion. As a result, machines that are even 2-3 generations behind have significant exposures that are mitigated by current processor platforms, and which enable a much more stringent data protection capability to be implemented. The increased components of modern processors that affect security are often what enables a PC to withstand and defeat attacks that earlier generations would be susceptible to. It's the deployment of older generation machines that makes malware and viruses so long lasting in their ability to cause damage.

The High Cost of Data Breaches

Every data breach is unique and has its own costs associated with finding and remediating the breach, including paying the potential increasingly burdensome penalties enacted by regulators in local and larger geographic areas, some of which may actually include criminal penalties. While costs vary, studies have found some compelling statistics about their cost. The *IBM Cost of a Data Breach Report 2020* found the average worldwide and US data breach costs as shown in Table 2.

Table 2: The Average Cost of a Data Breach: US and Worldwide

	USA	Worldwide
Average Cost of Data Breach	$8.64M	$3.86M

Also highlighted in the above report are four primary attack types, listed in Table 3. Each attack type has a different average cost, based on the characteristics of the damage they inflict. Malicious attacks that destroy data and ransomware attacks are more expensive than average malicious attacks or data breaches. Therefore, new technology aimed at protecting against ransomware and malicious data destruction attacks, now becoming available in newer generation processors, have a higher potential return on investment than the average data breach cost data mitigation would suggest.

Table 3: The Average Cost of Breach by Attack Type

Type of Attack	Avg $
Destroyed Data in Destructive/Wiper-Style	$4.52M
Ransomware	$4.44M
Average Malicious Breach	$4.27M
Average Data Breach	$3.86M

The Time Needed to Identify a Data Breach is Costly and Growing

Even with all of the security tools available to organizations like Security Information and Event Management (SIEM) that provides real time analysis of security alerts from networks and applications, the time to identify a data breach is growing. The *IBM Cost of Data Breach Report 2020* indicated that the average time to identify and contain a data breach was 280 days in 2020. Further;

- The potential savings of containing a data breach in less than 200 days was $1M, compared to containment in more than 200 days.
- And the report found that 39% of the total cost of the data breach was spent more than a 1 year after the breach occurred.

It's clear that deploying technology that can defeat threats provides a long term payback.

Determining ROI for Upgrading to More Secure PCs

It's difficult to come up with an average number that can be applied to all companies, as the number and scope of data breaches may vary widely. However, it's clear that a large percentage of companies have experienced data breaches, sometimes unrecognized, and that many more will do so in the future. And the costs are high.

Verizon did a study in 2015 (*Verizon 2015 Data Breach Investigations Report*) that showed a company with 1K employees losing 100K records in a data breach would have a cost of $475K to address each breach. While we think that's low by today's standards, it does provide a lower end estimate.

According to the *IBM Cost of Data Breach Study 2020*, the average cost for each lost or stolen record containing confidential information is $146. Therefore, if we use this metric, a company that loses 100K records would incur a cost of $14.6M. Assuming that organization has 1K employees, that's a cost of $14,600 per employee per data breach.

Using the above information, it's easy to see that better security is a good investment. Indeed, having one such breach of 100K records in a 1K employee organization will cost the organization $475 per employee according to Verizon estimates on the low side, or $15,400 per employee according to IBM estimates on the higher side. An average amount between the two estimates is $7,538 and we believe this is a more realistic estimate of the cost for most organizations. Applying an equivalent amount towards obtaining an upgraded PC with latest generation processor and security enhancements will offer a substantial Return on Investment. Assuming an average cost of $1K for a new enterprise-class PC with hardware enhanced security, plus an estimated $1200 in IT and end user costs to configure, install and replace the devices, eliminating just one data breach will produce a per user ROI of 243% for each machine deployed, as shown in Table 4.

Table 4: The average per employee cost of a data breach per incident, and ROI of new device upgrade

Cost of Data Breach	Low Estimate	High Estimate	Average Amount	Cost of New Client	Potential ROI
Cost per user	$475	$14,600	$7,538	$2,200	243%

The total cost of data breaches is not only in mitigating lost records or customer data. Costs are also associated with addressing suspected breaches where companies must change internal systems through Active Directory updates, user credential resets, etc. This is no small task, nor inexpensive. Our research has shown that over a three year lifespan of a typical corporate PC, the total cost due to continual password change per employee is $1011 to $1272 per user (*see J.Gold Associates Research report, "Your PC has an Identity Crisis: Saving the Cost of a Hack and Other Benefits of Enhanced Identity"*).

Most studies of data breaches have focused on the cost of lost records. However we estimate that for every actual data breach, many more suspected breaches cause companies that feel they may have been compromised to take remedial steps to mitigate the potential harm. "Suspected" credential compromise is a major problem that is under reported. And the loss of end user productivity due to "false positive" security alerts that trigger immediate end user action is a major headache for many organizations, not to mention the aggravation it causes employees. A more secure PC can alleviate many of these efforts and costs.

A Need for Enhanced Device Management

While we have focused above on the internal security features inherent in the newer generation of processors, there is also a significant security advantage that comes from having a higher level of manageability in newer generation machines, as well as having an increased level of manageability functions available when selecting "Pro" level processors over standard processors. Indeed, automated systems and capabilities that can remotely and rapidly keep machines updated with the latest BIOS, firmware, OS, and apps can add a significant amount of protection over less well managed devices. Further, especially with the increase in remote workers and distributed locations, the ability to do remote and "out of band" manageability to maintain and update systems is a critical requirement for new generation platforms.

In the *IBM Cost of a Data Breach Report 2020*, they found that security automation significantly reduces the time to find and mitigate a breach. In looking at the data breach lifecycle, IBM found that:

- *When automation was fully deployed the time to identify averaged 175 days and the time to contain averaged 59 days.*
- *Without automation, the time significantly increased to an average of 228 days to identify a breach and 80 days to contain, for a total of 308 days*.

And IBM found that for the 21% of companies that had fully deployed automation;

- *The average total cost of data breach was $2.45 million for organizations that fully deployed security automation, which was $3.58 million less than the average cost for organizations without security automation deployed*.

In the cases studied by IBM, they focused on cost reduction available to companies with a fully implemented security stack/infrastructure. Simply managing the endpoints, while important, would not produce the same level of savings. Yet without the inclusion of security management for endpoints and their central role in so many breaches, we estimate that the overall cost savings for the automated organization would diminish by at least 25%-35% and that the time to discover and mitigate a breach would increase dramatically.

Recommendations

We recommend organizations take the following actions:

- Enterprises must explore the upgrading of their user endpoints so that the latest security features can be deployed to limit the expanding attack surface that most companies face.
- Organizations must ensure that each endpoint is capable of being managed for security updates and other enhancements in an automated fashion no matter where the machine is located.
- Enterprises should ideally require that any remote worker's computer used for corporate business and accessing corporate resources be no more than 1-2 generations behind in processors so as to maintain the highest level of security and privacy capability.
- Companies must determine a rapid replacement cycle for all non-compliant computers, while making sure each is a fully managed device on the corporate infrastructure.
- Organizations should implement Enterprise-grade processors and compatible management tools whenever possible. The small additional cost will be outweighed by the increased security and privacy capabilities, as well as enhanced manageability.
- Those organizations that fail to adopt a strategy for deploying security enhanced computing systems will be at significantly increased risk of having a security breach that can easily cost the company millions of dollars as well as being highly disruptive to its operations, or even cause a business failure.

Conclusions

We recommend that enterprises explore the use of enhanced, current generation processor-based computers in the next 6-12 months, and eliminate as quickly as possible any machines that are more than 1-2 generations behind in processor technology. Further, all organizations must include automated security management functions that can “touch” each machine and keep each up to date as needed to stay ahead of increased security threats. Finally, while many companies believe there may be no real payback to quickly updating endpoints, the ROI on avoiding potential data breaches and hacks can easily justify the cost of upgrading equipment, without waiting for the typical 3-5 year refresh cycle.

While there is no 100% sure thing when it comes to security, requiring current generation enhanced processor-based machines is a major step forward and should be implemented whenever possible to maximize security and privacy and consequently reduce the overall exposure to expensive and business disrupting hacks and data breaches.

Appendix: Intel vPro® Platform

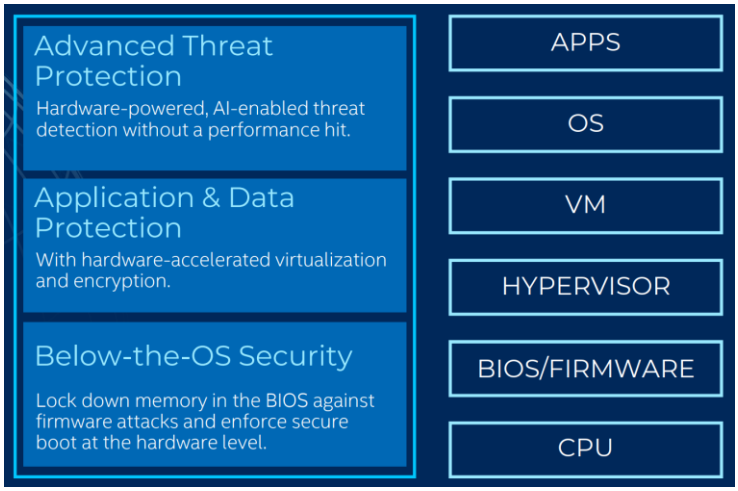
The Intel vPro® Platform family of processors provides enterprise-class features that extend security capabilities to benefit both end users and IT departments and to help maximize security and privacy. The enhanced capabilities of the Intel vPro Platform include:

Intel vPro Platform Features:

Professional Grade Performance – Tuned for needs of enterprise users while helping minimize any impact due to security components
Multilayer Security - securing fleets of business machines with comprehensive security features that complement and enhance existing IT infrastructure
Complete Management – lifecycle management and proven IT tools for modern cloud-enabled environment enables maintaining all machines at peak performance and up to date firmware/OS status
More Reliable Security – rigorous internal testing and deep partnerships with researchers, OEMS, and industry experts to verify and fix issues before they have an impact on users

Also included in each vPro Platform product is:

Intel® Hardware Shield Technology



Copyright Intel Corp.

The result is that Intel vPro Platform uniquely enables organizations to help secure their data, manage their devices, enhance user productivity and fully maximize the value from their technology investments.

Intel, the Intel Logo, and other Intel marks are trademarks of Intel Corporations or its subsidiaries.

About J.Gold Associates

J.Gold Associates provides insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.

J.Gold Associates, LLC
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com