REGION FOCUS: WORLDWIDE

The Business Value of Intel Security for PCs

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC

Table of Contents

Executive Summary

Intel has made security a differentiator in hardware-based computing platforms. Feature offerings initially focused on attributes that live below the operating system (OS). Intel subsequently has invested aggressively in vulnerability management and offensive security research to make the microprocessors themselves more resilient. Finally, Intel is unlocking silicon capabilities to play an active role in threat defense against above the OS attacks. These capabilities are truly differentiated, but … do they matter? If these capabilities enable improved secure outcomes, those outcomes should be able to be objectively measured. The objective of this study is to objectively measure the improved outcomes enabled by Intel's differentiated security capabilities.

IDC spoke with organizations that deploy Intel-based Windows PCs (Intel PCs) and those that also have experience deploying non-Intel Windows PCs (other PCs) to understand the differences in terms of security capabilities, security risk, staff time requirements, and business and operational impact. IDC's analysis shows that Intel PCs offer built-in security functionality that enables organizations to maintain more robust and efficient PC security environments by proactively preventing attacks. As a result, interviewed organizations not only reduce PC-related risks to their business and operations but also have an average total cost, over five years, of buying, running, and securing Intel-based PCs of 14% less than non-Intel PCs due to:

- **Requiring less staff time to secure PCs,** with more frequent automated updates and improved threat mitigation capabilities creating efficiencies

- **Reducing the frequency, impact, and costs of security-related events and performance degradation,** thereby helping employees work productively with fewer interruptions

- **Minimizing the likelihood of major security attacks,** thereby bringing down the business cost and risk associated with a breach that could affect revenue, reputation, and customer goodwill

- **Extending PC replacement cycles and avoiding the need for additional security tools and solutions,** which often offset any additional cost of purchasing an Intel-based PC

Business Value Highlights

Click each highlight below to navigate to related content within this document.

14%
lower five-year cost of operations per PC, saving $934 per PC

26%
lower risk of major PC-related security event

21%
fewer impactful security events

17%
security team efficiency gains

22%
lower cost of lost productivity, PC security, and performance issues

15%
faster to deliver new PCs

Situation Overview

The foundation of today's personal computing systems is the microprocessor; the security and resiliency of the system is built on the top of the processor foundation. Today's processors are highly sophisticated integrated systems on a single chip with multiple classes of architecture — CPU, GPU, FPGA, and artificial intelligence accelerators — to compute the vast array of workloads. These systems on chips additionally have an extended architecture of interconnects including on-chip, chip to chip, cross computer, cross datacenter, cross network, memory hierarchies, and caches all the way to storage. Software in a processor, referred to by names such as firmware, UEFI, or BIOS, drives the system.

As systems become more complex, software vulnerabilities are more probable consequences. A microprocessor vendor can be proactive and look for vulnerabilities or be reactive, waiting for others to find them. Once a vulnerability is known, a vendor can be expeditious in the preparation of a patch or slow to respond. A vendor can facilitate the application of a patch, making the task easy, or allow the user to go it alone. Simply said, the approach to vulnerabilities is not black or white; there is a continuum of quality and speed of response.

However, limiting the processor's role in security to defensive patching of vulnerabilities would be unfortunate. The power of the multiple classes of CPU, GPU, and FPGA architecture and artificial intelligence accelerators can also be brought to bear to improve the security and integrity of the host systems. Hardware accelerators can virtually eliminate the encryption tax, enabling resilient data. Analytics can be applied to workloads to illuminate potentially malicious activity. Trusted execution environments (TEEs) can embed trust in operations and empower security outcomes.

The last phrase is key: empower security outcomes. One of the struggles for the cybersecurity community is the use of too many words and not enough relevant and outcome-centered metrics. Security features are described in prose and the end user is left to intuitively understand the importance. If an activity such as proactively patching a vulnerability before an exploit is available has real value, shouldn't we be able to quantify a secure outcome? If a processor vendor does a superior job of updating BIOS, shouldn't the resulting longer life of the host system be able to be measured? If a processor vendor can leverage the host compute to improve system security, shouldn't those devices be breached less frequently?

This Business Value study looks to use less words and more numbers. Instead of describing in prose the security and resiliency features of Intel microprocessors, IDC looks to measure outcomes through a comprehensive set of metrics.

One of the struggles for the cybersecurity community is the use of too many words and not enough relevant and outcome-centered metrics.

Intel Security for PCs

Intel has looked to make security a differentiator in hardware-based computing platforms. Feature offerings initially focused on attributes that live below the operating system, as the root-of-trust capabilities are typically enabled by computing device platform providers and operating system vendors to improve system integrity. A best practice for IT and security teams is to start with PCs and servers built on the foundation of hardware-based security. Integrated into silicon, root of trust checks the authenticity of the firmware and OS at the boot and during the operation. If alterations are detected from expected measurements, an alert will be generated. Cybersecurity is improved, and the occurrences of disruptive out-of-commission PCs are reduced. It's important to note that security features in silicon can enable additional security features such as trusted enclaves, secure key storage, crypto acceleration, and isolation for apps and virtual machines.

In addition to making the host system increasingly resilient, Intel invests aggressively in vulnerability management and offensive security research to make the microprocessors themselves more resilient. The Intel Bug Bounty program has awarded millions of dollars to external entities to discover vulnerabilities. However, the number of vulnerabilities discovered and reported by Intel itself far outpaces those reported by external entities. Discovery is only the first half of the solution, as creating and enabling easy patching is the other component.

Finally, the world above the OS, especially workloads, has historically been largely under-defended by silicon capabilities. This world is governed by software security measures hosted on top of the OS. Intel has been changing this. Under the moniker Intel TDT (Threat Detection Technology), Intel is unlocking capabilities in its system on a chip (SoC) that fundamentally changes the rules of the game. Intel TDT is a capability that is part of the Intel Hardware Shield advanced threat detection portfolio of security capabilities. The other recently released new capability in this category is Intel Control-Flow Enforcement Technology (CET), which closes the door on memory-related control flow hijack attacks.

Intel's strategy leverages silicon-level telemetry and functionality that security independent software vendors (ISVs) and possibly OEMs can leverage to enable the hardware compute platform to play an active role in threat defense against above the OS attacks such as ransomware and cryptomining. The goal of the Intel-security software vendor partnership is to enable and empower the Intel—based systems of today and tomorrow to be fundamentally more secure and have lower malware infection rates than other processor systems.

The capabilities built by Intel are pragmatic and make qualitative sense, but do they matter? Best practice is great, but it relies on faith that the result is a trusted device. If these capabilities result in improved secure outcomes, we should be able to objectively measure these outcomes. This study objectively measures the outcomes enabled by Intel's built-in security capabilities.

The Business Value of Intel Security for PCs

Study Demographics

IDC interviewed individuals who are IT managers or above with PC-related security responsibilities at 15 organizations that use Intel-based Windows PCs and either use or have experience with non-Intel Windows PCs. These in-depth interviews explored the differences between Intel PCs and other PCs in terms of security capabilities and outcomes. As shown in Table 1, participating organizations had an average profile of a large enterprise, with an average of 41,200 employees and $6.81 billion in annual revenue (medians of 5,600 employees and $1.2 billion in annual revenue, respectively). Interviewed organizations had close to a 1:1 employee-to-PC ratio, with Intel-based PCs making up approximately 85% of these PCs. Study participants provided experiences from many different industry verticals, namely, financial services, government, healthcare, manufacturing, entertainment, government contractor, higher education, insurance, pharmaceutical, and technology. For additional information, (see **Table 1,** next page).

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	41,200	5,600
Number of IT staff	1,112	150
Total number of PCs	41,247	6,000
Total number of Intel PCs	35,044	4,900
Countries	United States (13), Australia, United Kingdom	
Industries	Financial services (3), government (2), healthcare (2), manufacturing (2), entertainment, government contractor, higher education, insurance, pharmaceutical, and technology	

n = 15; Source: IDC in-depth interviews, November 2022

Role of Security in Choosing Intel-Based PCs

Study participants described how PC security-related concerns intersect with Intel's security capabilities and how this influences PC buying decisions. They spoke to the importance of having proactive and robust foundational security capabilities for the PCs used on a day-to-day basis by their employees, noting the significant potential business and reputational costs associated with device-related security breaches and incidents. They noted security-related evaluation criteria such as chip-based features, update frequency and capabilities, and encryption functionality. A number of study participants connected their PC buying decisions to their conclusion that Intel PCs provide a higher baseline security standard than other PCs.

Interviewed organizations commented on their PC-related security considerations and how these affect buying decisions:

**Ensure key protection functionality and quality of patching
(healthcare, United States):**
"Being in healthcare, we have to make sure our key protection works. We look at the features chips have, and we are very considerate of firmware updates. Intel always puts out updates to the chips and can hot-patch a chip."

**Minimize systemic risk related to chip functionality
(technology, United States):**
"A lot of threats these days have to do with systemic risk, which arises from how chips are designed by the manufacturer. I see a difference between Intel and other PCs. … We want the ability to have hardware-based encryption on PCs. This is the key component for us."

**Necessity of securing data through encryption for mobile workers
(pharmaceutical, United States):**
"We have a mobile workforce, so it's extremely critical to us that our PCs are secured, and data is not at risk if the PC is stolen, lost, or damaged. We look for encryption and Intel's got more experience with working with it than [other types of PCs], in my opinion, so we have more confidence. It's a corporate strength of Intel that they've been working in the encryption field and the hardware BIOS field for longer."

**Ability to identify threats, functionality in a hybrid work environment
(government contractor, United States):**
"There are always new vulnerabilities, and Intel has researchers and bug hunters that find vulnerabilities constantly. We consider the functionality of tooling in a hybrid environment because we have some users in the office and some remote, and some travel internationally all over the place."

Business Value and Quantified Benefits of Intel Security for PCs

Study participants reported that they value Intel-based PCs for their built-in security capabilities, which allow them to reduce PC-related risk, minimize productivity losses associated with security events and performance issues, and lower the amount of staff time required to secure and support PCs.

Interviewed organizations described such security-related advantages of Intel PCs and how they benefit from a risk, performance, and operational efficiency perspective:

Importance of security updates (healthcare, United States):
"We get more updates from Intel than other PCs. ... For example, encryption on the device, password protection, and protection against theft, and cybersecurity are important, especially for non-desktops."

Speed of updates limits risk (higher education, United States):
"Faster updates with Intel PCs are critical for us because education tends to stand out as a target. Having the ability to quickly deploy critical updates is key."

Strong functionality, efficient management (financial services, Australia):
"We benefit from Intel's threat detection technology and features they have introduced like Total Memory Encryption, which encrypts the D-RAM at the memory level. Things like these are why we have moved over to vPro."

Importance of good firmware updates and ecosystem to execute (healthcare, United States):
"The number 1 benefit for us is that we can fix issues by using good firmware updates on Intel PCs. ... Intel has been continually improving the security on its chips. Sadly, most consumers are never going to understand exactly what they're doing, but they've been doing a really good job of every generation iteratively doing more and more security within chips themselves."

Study participants linked the security advantages of Intel PCs to two important outcomes. First, they reported decreasing the risk associated with major security events that could result in large-scale costs in terms of lost revenue, regulatory compliance fines, or even reputational damage. Second, this reduction in costs associated with security risk, alongside security-related efficiencies and improved PC performance, has allowed them to deploy, run, secure, and support PCs at an average lower total cost of 14%, which brings down the cost of operations per PC by an average of $934 over a five-year PC life span.

Security Team Efficiencies

Study participants reported that they can secure and support Intel-based PCs more efficiently and proactively. They cited more robust security functionality, including more frequent and impactful updates, built-in encryption functionality, and better leverage of other security tools — as driving efficiencies. Taken together, this means that organizations can ensure the security of their PCs and respond to security-related issues more efficiently for Intel PCs than for other PCs.

Study participants spoke to how they have enabled device security, incident response, security patching, and help desk teams to spend less time on day-to-day responsibilities on a per-device basis with Intel PCs:

Would require more staff time without Intel (technology, United States):
"If we had all [other PCs] for these devices, it would require twice as much staff time because managing, maintaining, upgrading, and supporting other PCs is a lot more difficult than with Intel. Even third-party software is usually more compatible with Intel, which affects how long it takes to support things."

Efficiencies in patching and updating keep staff time requirements lower (technology, United States):
"If we used other PCs for those we currently have that are Intel based, we'd probably need at least 50% more people. … For patching and updates, it takes more time with other PCs; for Intel-based PCs, it takes an average of an hour, and almost double that for other PCs."

Ease of onboarding requires less staff time to support (healthcare, United States):
"It takes more time to onboard other PCs than an Intel PC because there are better tools to roll out an Intel PC. I'd say it takes about 30% longer because someone's got to babysit those. With Intel PCs, you literally plug it in, turn it around and log in because the tooling is so well established."

Interviewed organizations reported that they require less time with Intel PCs for the following security- and performance-related activities:

- **PC security teams:**
  Teams responsible for ensuring device security benefit from built-in functionality such as encryption and overall hardened security, resulting in average efficiencies of 17% for these teams.

- **PC incident management teams:**
  Intel PCs experience relatively fewer security- and performance-related issues than other PCs, thus reducing the time required per PC for these activities by an average of 8%.

- **PC security patching teams:**
  Intel PCs have automated and robust patching functionality that generates efficiencies for staff and teams responsible for PC patching, with average time savings of 20% compared with other PCs.

- **PC help desk teams:**
  Users require less frequent support for security- and performance-related issues with Intel PCs, with average efficiencies for help desk support teams of 24%, including 17% fewer tickets and 7% faster resolution of tickets.

Combined, these security team–related efficiencies mean that study participants save an average of 1.6 hours per PC per year or 16% efficiencies compared with other PCs. **Figure 1** shows these efficiencies on a per-PC basis, which IDC calculates equates to $86 savings per PC on an annual basis in terms of security staff time savings.

FIGURE 1

PC Security- and Performance-Related IT Staff Efficiencies
(Hours per PC per year)
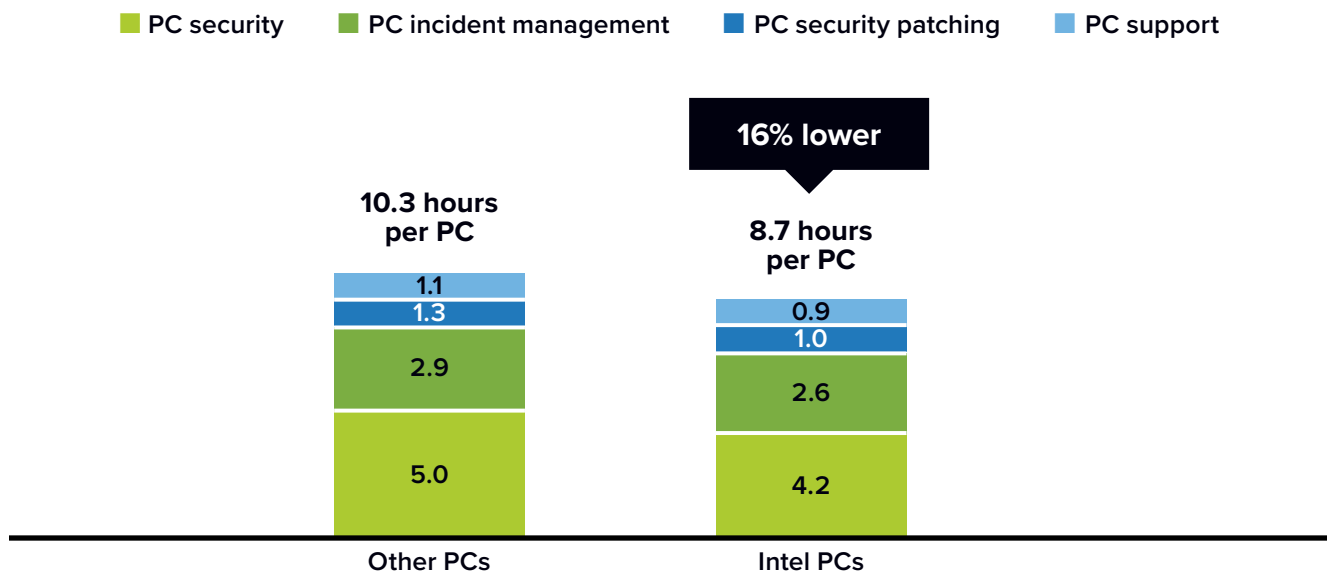
n = 15; Source: IDC in-depth interviews, November 2022

For an accessible version of the data in this figure, see Figure 1 Data in the Appendix.

Improved PC Security and Performance

Study participants reported that they can more readily ensure the security and performance of Intel PCs than other PCs. As a result, they face fewer security breaches and other performance-impacting issues and ensure consistent access to business-critical applications and systems for employees.

Interviewed organizations spoke to the security advantages of Intel PCs:

Strength of multilayered security (technology, United States):
"The basic security benefit of Intel PCs is encryption at the chipset level. A lot of systematic risks occur when we don't have that level of multilayered security enforcements. When we were doing research, we noticed that Intel has a hardware shield component, which basically sits below the operating system and application security. This helps with advanced detection of threats and blocking them."

Inherent security (manufacturing, United States):
"We have seen specific malware variants target non-Intel chipset devices. We believe this happens because instruction sets are built into [other] chips that are not on the Intel equivalent. Therefore, as a result, we believe that the Intel chipsets provide an inherently greater security profile."

Study participants frequently referenced the volume and quality of security updates and patches provided on Intel-based PCs in explaining improved security. They noted that these updates, while more frequent, are also seamless in nature, enabling uninterrupted access to PCs.

Interviewed organizations provided specific examples of the value of proactive Intel-driven security updates:

Strength of updates and ability to hot-patch (healthcare, United States):
"We can get updates that cover so much with Intel PCs, which has been incredibly good. Also, the ability to hot-patch chips has been good for us in terms of being able to digitally sign the EFI and allowing for verification by TPM on the motherboard."

Quality of firmware updates based on real-world experience (government contractor, United States):
"Firmware updates are of better quality with Intel PCs. We had a painful experience with other PCs where, even though we tested a BIOS update and we didn't discover any issues, we had issues when several groups received the update and we had to roll it back."

As **Figure 2** demonstrates, study participants reported that Intel PCs receive 26% more security-related updates per PC than other PCs, which hardens PCs against new and evolving security threats. This more proactive approach toward security updates helps ensure that organizations close off potential attack vectors through PCs before they materialize and positively affects results in terms of security incidents incurred as discussed (see **Figure 3** next page).
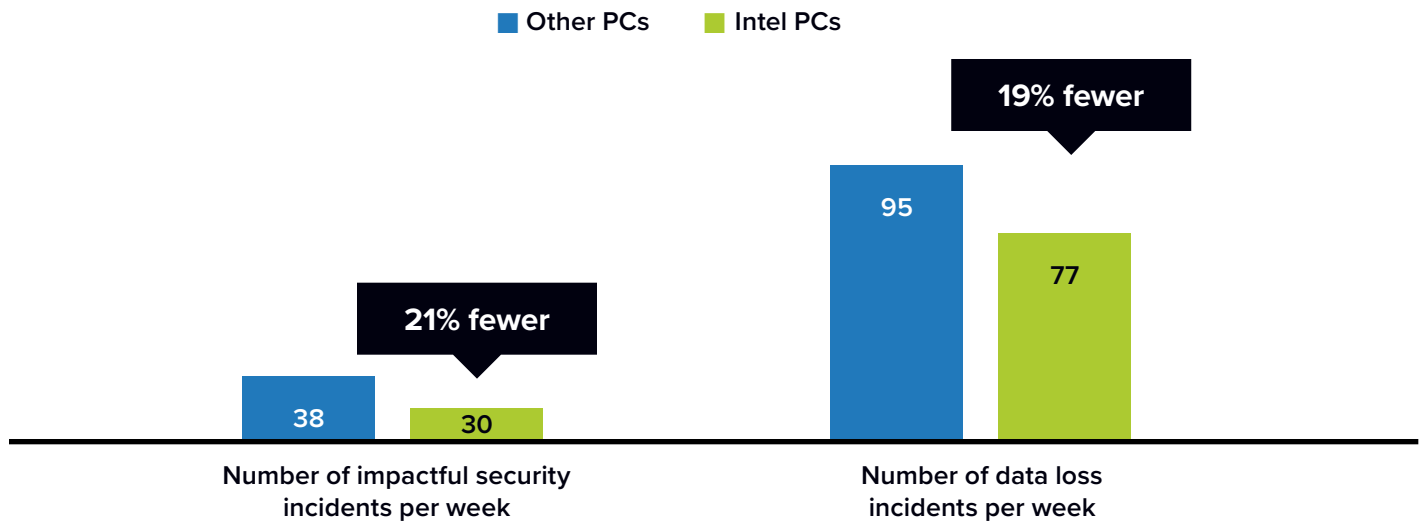
FIGURE 2

Number of Security Updates per Year per PC
(Number per PC per year)

26% more

Other PCs **3.5**

Intel PCs **4.7**
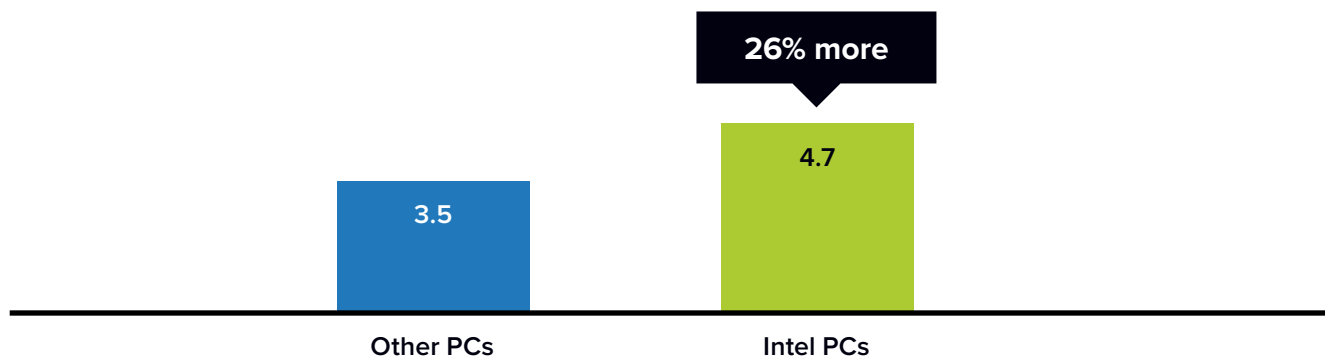
n = 15; Source: IDC in-depth interviews, November 2022

Built-in security features combined with more frequent and robust security updates bring positive real-world results to study participants. While they generally cannot eliminate PC-related security issues entirely, they strive to minimize the frequency, duration, and impact of such events. Overall, study participants reported that their Intel PCs hold up better against malware, viruses, and bad actors that can cause security issues. One interviewed financial services organization in the United States spoke to why Intel PCs reduce its security exposure: *"Intel is a lot better designed, so Intel PCs can fend off these kinds of threats quite easily. … In terms of updates, I also believe that they can get security mitigation measures to us in a timely manner."* Results from the sample on the whole back up this sentiment: On average, IDC calculates that interviewed organizations experience 21% fewer impactful security incidents and 19% less frequent data loss events with Intel PCs compared with other PCs (see **Figure 3,** next page).

FIGURE 3

Impact on Core Security KPIs

(Number per week)

Legend: ■ Other PCs ■ Intel PCs

- Number of impactful security incidents per week: Other PCs = 38, Intel PCs = 30 (21% fewer)
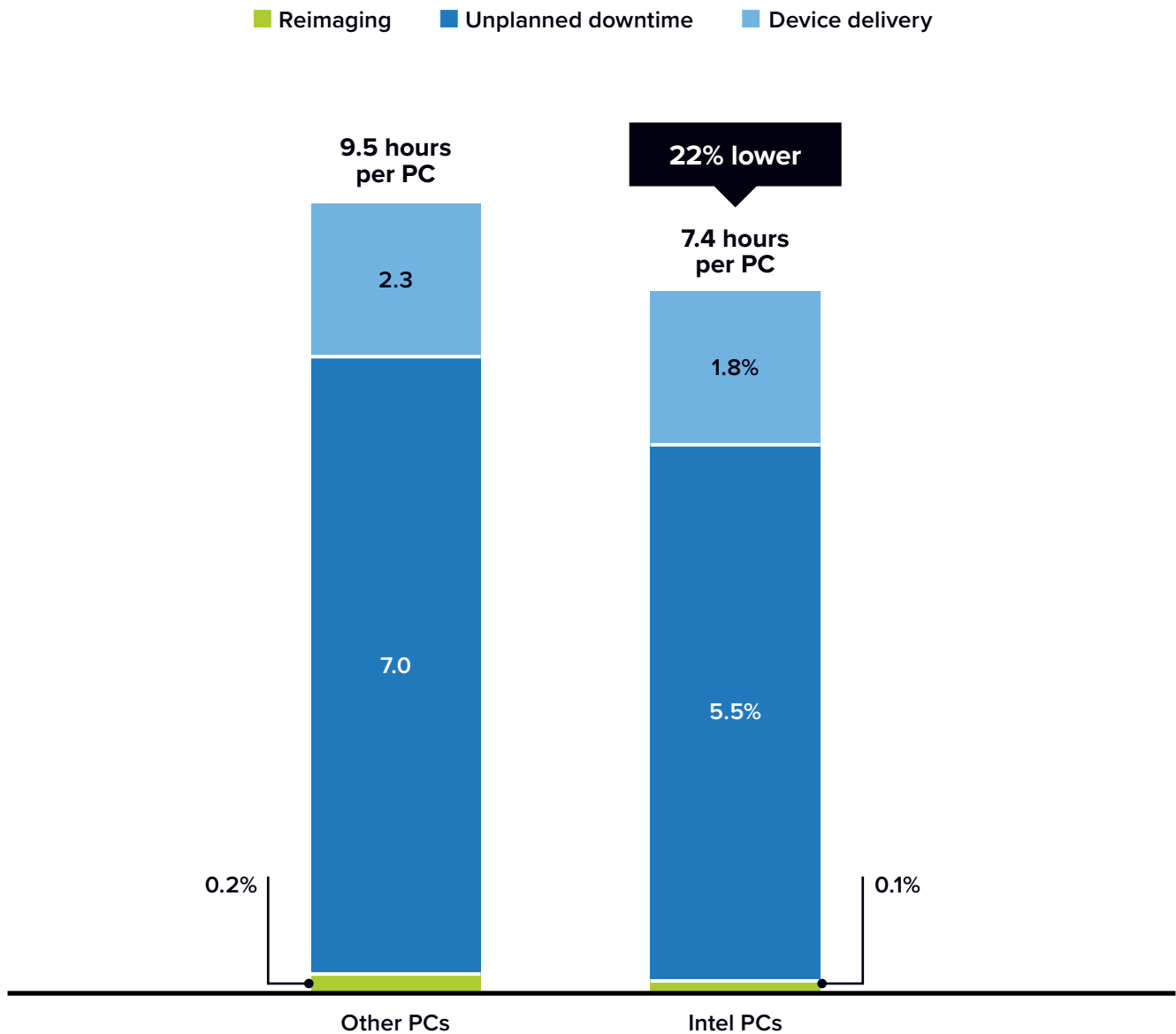- Number of data loss incidents per week: Other PCs = 95, Intel PCs = 77 (19% fewer)

n = 15; Source: IDC in-depth interviews, November 2022

For an accessible version of the data in this figure, see Figure 3 Data in the Appendix.

By minimizing the frequency of security events and issues that lead to PC outages and performance problems and hamper agility, study participants reduce productivity losses for PC users. Overall, IDC calculates that interviewed organizations will reduce productivity losses by an average of 22%, equal to 2.1 hours per PC user per year, with Intel PCs by:

- **Reducing the frequency of PC outages and performance degradation,** which creates user frustration and costs productive time. On average, IDC calculates that users gain back 22% of productivity losses with Intel PCs, including 7% fewer outages and 16% faster resolution when issues occur.

- **Requiring less reimaging of PCs,** which can take PCs away from users for extended periods of time due to security events, bugs, and performance issues. IDC puts productivity savings related to reimaging at an average of 39% with Intel PCs compared with other PCs.

- **Providing new Intel PCs faster to users** because interviewed organizations must do less to prepare Intel PCs for use. On average, IDC calculates that study participants deliver new Intel PCs 15% faster than other PCs (7.0 days vs 8.2 days on average), which leads to earlier use of higher-performing devices and cuts productivity losses associated with PC deployment by an average of 23%.

Figure 4 shows the overall average productivity losses per PC per year associated with these security- and performance-related issues. As shown, IDC calculates that study participants reduce productivity losses by 22% per PC with Intel PCs, saving an average of 2.1 hours per PC per year.

FIGURE 4

PC Security- and Performance-Related User Productivity Losses
(Hours per PC per year)

n = 15; Source: IDC in-depth interviews, November 2022

For an accessible version of the data in this figure, see Figure 4 Data in the Appendix.

Reduced Risk of Major Security Events and Enhanced Business Confidence

Study participants also linked substantial reductions of risk related to major security events that affect business results, reputation, and customer goodwill to their use of Intel PCs. They cited overall hardened devices with Intel PCs as better ensuring security, as well as enhanced features and functionality that minimize the likelihood of major security events occurring.

Several interviewed organizations spoke in detail to the advantages of Intel PCs:

Importance of security verification (government, United Kingdom):
"We can do more security verification directly with Intel PCs, which saves time and cost and reduces risk of unauthorized access. I'd say that the risk with Intel is lower by about 20–25%."

Importance to business activities (financial services, United States):
"We get questionnaires and assessments from some of the customers we provide service to in our industry who ask us how we protect our devices. They ask whether we are using Intel or [other PCs] in proposals and whether we offer remote management. We have more confidence in addressing these opportunities with Intel PCs."

Interviewed organizations linked major security events to very large business costs in terms of potential lost revenue, remediation costs, and regulatory fines. On average, they reported that such events had a potential cost per instance of $11.43 million. Importantly, they also put the risk of such a major security event's occurring through an Intel PC at an average of 26% lower than other PCs, which reduces the imputed cost of risk related to such significant security events for Intel PCs compared with other PCs (see **Table 2,** next page).

TABLE 2

Cost of Risk Analysis

	Other PCs	Intel PCs	Difference	Benefit
Potential cost of major security incident	$11.43M			
Less likely with Intel PCs	26%			
Likelihood of major security event, assuming baseline of 1 event in 5 years	20%	15%	5%	26%
Cost of major security incident per PC per year	$55	$41	$14	26%
Cost of major security incident per PC, 5 years	$277	$206	$71	26%
Cost of major security incident per organization per year	$2.29M	$1.70M	$585,500	26%
Cost of major security incident per organization, 5 years	$11.43M	$8.50M	$2.93M	26%
Total revenue lost per year	$2.53M	$0.82M	$1.70M	67%
Total net revenue lost per year	$379,200	$124,200	$255,100	67%

n = 15; Source: IDC in-depth interviews, November 2022

PC-Related Cost Savings

Study participants reported that they typically pay more initially for Intel Windows PCs than other Windows PCs, with a cost premium for Intel PCs of 11%, or $157 per PC. However, they noted that they make up this cost difference through longer PC longevity, reduced requirements for additional software and tools, and more efficient IT team support. For example, one study participant noted: *"We would spend more for software if we had more non-Intel PCs, probably another 20% more; I'll say about another $500,000–600,000/year, plus at least another four FTEs to manage that software."* Longer average PC life spans of 12% for Intel PCs mean that over a five-year period, study participants must replace 35% fewer PCs, allowing them to avoid the cost associated with providing many new PCs to employees. Thus IDC calculates that in total over five years, study participants spend 2% less on Intel PCs than other PCs when taking these factors into account, as laid out in **Table 3**.

PC-Related Cost Savings

Study participants reported that they typically pay more initially for Intel Windows PCs than other Windows PCs, with a cost premium for Intel PCs of 11%, or $157 per PC. However, they noted that they make up this cost difference through longer PC longevity, reduced requirements for additional software and tools, and more efficient IT team support. For example, one study participant noted: *"We would spend more for software if we had more non-Intel PCs, probably another 20% more; I'll say about another $500,000–600,000/year, plus at least another four FTEs to manage that software."* Longer average PC life spans of 12% for Intel PCs mean that over a five-year period, study participants must replace 35% fewer PCs, allowing them to avoid the cost associated with providing many new PCs to employees. Thus IDC calculates that in total over five years, study participants spend 2% less on Intel PCs than other PCs when taking these factors into account, as laid out in **Table 3.**

TABLE 3

PC Cost Analysis Over Five Years

	Other PCs	Intel PCs	Difference	Benefit
Cost per PC, initial	$1,432	$1,589	−$157	−11%
Cost per PC, additional devices required, replacement cycle	$614	$443	$170	28%
Cost per PC, additional security solutions required	$28	$0	$28	100%
Total five-year cost per PC	$2,074	$2,033	$41	2%
Total five-year PC cost per organization	$85.54M	$83.84M	$1.71M	2%

n = 15; Source: IDC in-depth interviews, November 2022

Cost of Operations Analysis

The security- and performance-related benefits of using Intel PCs generate a compelling overall value proposition for study participants. Perhaps, most importantly, they linked lower risk to Intel PCs, which is critical given that major security incidents can exert costs measuring into the many millions of dollars. Further, IDC analysis shows that considering cost efficiencies related to risk, IT staff time requirements, employee productivity, and PC costs, Intel PCs cost markedly less to buy and operate over five years than other PCs. As shown in **Figure 5,** IDC calculates that interviewed organizations incur costs that are 14% lower with Intel PCs, worth $934 per PC over five years. While significant even on a per-PC basis, these cost efficiencies are especially meaningful when viewed through the prism of deploying hundreds, thousands, or even tens of thousands of PCs. For example, even a deployment of 1,000 PCs would yield cost savings, staff efficiencies, and productivity gains worth $934,000 over five years according to IDC's analysis.

FIGURE 5

Five-Year Cost of Operations per PC
($ per PC, five years)
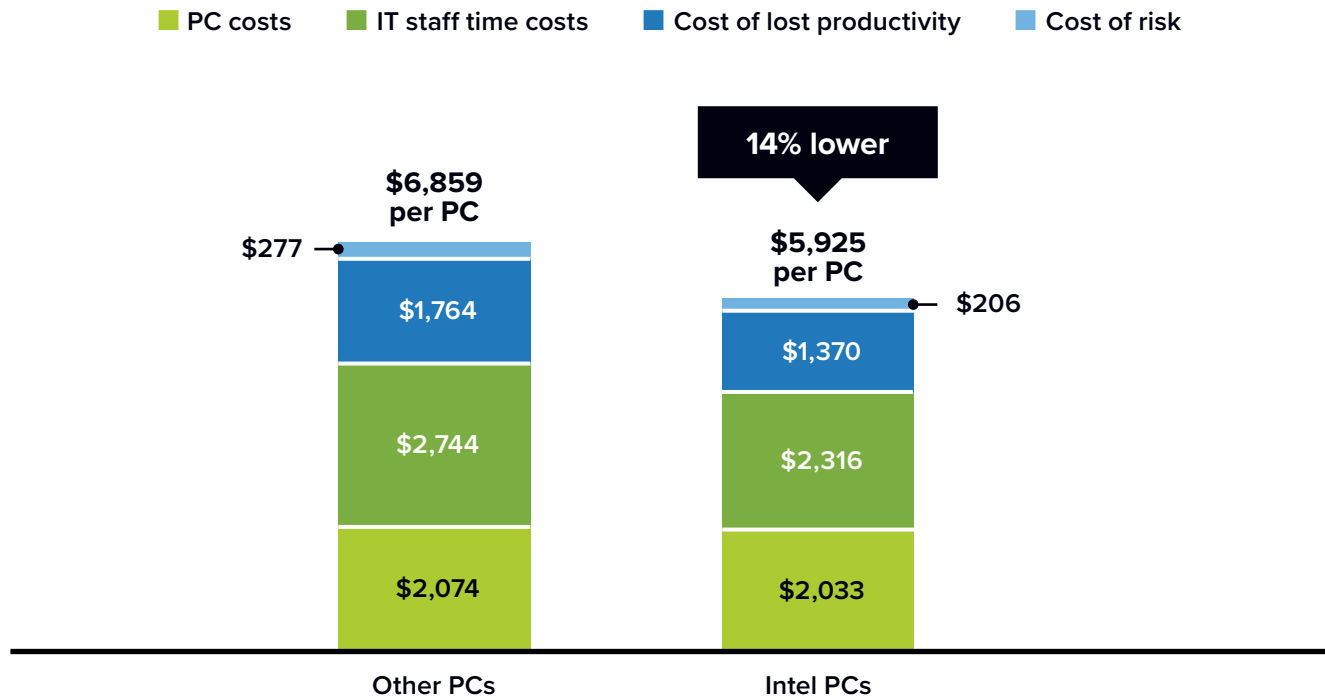
Legend: ■ PC costs ■ IT staff time costs ■ Cost of lost productivity ■ Cost of risk

Other PCs: $6,859 per PC — $277 (Cost of risk), $1,764 (Cost of lost productivity), $2,744 (IT staff time costs), $2,074 (PC costs)

Intel PCs: $5,925 per PC (14% lower) — $206 (Cost of risk), $1,370 (Cost of lost productivity), $2,316 (IT staff time costs), $2,033 (PC costs)

n = 15; Source: IDC in-depth interviews, November 2022

For an accessible version of the data in this figure, see Figure 5 Data in the Appendix.

Challenges/Opportunities

The features provided by Intel enable a demonstrable improvement to security. The operative word is *enable*. Intel cannot create the outcomes alone. It is reliant on OEMs designing these security capabilities, partners in the security ecosystem enabling these capabilities, and end users activating these capabilities to create improved security outcomes.

Certainly, Intel can drive the discovery of vulnerabilities and proactively create patches, but it must rely on system providers for the distribution of patches and the system operator to apply the patches. It is the reality of the System Integrity Responsibility Model. It sounds simple, but the best patch is ineffective if not applied.

A best practice for IT and security teams is to start with PCs and servers built on the foundation of hardware-based security. Root of trust checks the authenticity of the firmware and OS at the boot and during the operation. Just like in the distribution of patches, the root-of-trust capabilities are typically enabled by computing device platform providers and operating system vendors to improve system integrity.

Finally, above-the-OS protections, such as Intel TDT, are innovations in the battle against malware. However, the key to the strategy is security software vendor utilization.

Conclusion

Organizations must minimize security vulnerabilities in the face of increasing scale and complexity. The ubiquity of PCs puts microprocessors at the center of security efforts, and today's processors are highly sophisticated and integrated across IT environments. This increases the importance of microprocessor security approaches and capabilities, especially whether the processor takes a more or less proactive approach to patching, updates, and other security-related capabilities. This study evaluates the quantitative difference in terms of security between Intel-based chips and non-Intel chips running Windows PCs.

Study participants reported perceiving differences in Intel-based and other PCs in important areas related to security functionality, costs, and results. They cited Intel's more proactive approach and in-built security functionalities in reducing risk related to PC security breaches, which not only minimizes the potential for business losses but also helps lower the overall cost of operating PCs. Further, they cited efficiencies in security and supporting their Intel PCs and cost advantages from needing to replace Intel devices less frequently. Taken together, these advantages of Intel-based PCs combine to create a compelling value proposition in terms of lower total cost of operations (14% lower on average) as well as minimizing the potential for major security disruption through PCs.

Appendix 1: Methodology

IDC's standard Business Value/ROI methodology was utilized for this project. This methodology is based on gathering data from organizations currently using Intel-based PCs that also have experience with non-Intel PCs as the foundation for the model. Based on interviews with organizations using Intel PCs, IDC performed a two-step process to calculate the ROI and payback period:

Use subheadings to introduce bulleted lists/content:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment** of the impact of using Intel-based PCs. Benefits included security team efficiencies, reduced risk associated with security incidents, higher user productivity, and PC-related costs savings.

2. **Created a complete investment (five-year total cost analysis) profile based on the interviews** comparing overall costs of buying, deploying, and running Intel-based PCs compared with non-Intel PCs.

IDC bases the payback period and ROI calculations on a number of assumptions, including time values multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

Appendix 2:
Select Additional Quotes

Appendix 2 provides additional selected quotes from interviews with organizations using Intel-based PCs that were not otherwise used in the study.

Preferred choice for handling sensitive data, meeting regulatory requirements (financial services, United States):

"We consciously chose to have Intel PCs for a couple of reasons. It has to do with us being in the financial services vertical, so Intel is the preferred choice because of the sensitivity of data that is accessed. Intel PCs have a rigor in terms of components. Also, we have to navigate regulations and want to be sure to keep regulators happy."

Importance of security verification (government, United Kingdom):

"We can do more security verification directly with Intel PCs, which saves time and cost and reduces risk of unauthorized access. I'd say that the risk with Intel is lower by about 20–25%."

Staff efficiencies from ability to use software and tool solutions (Government, United Kingdom):

"Intel PCs are easier to update and patch, and the Intel chips allow them to run some native software more easily. There is some software that we cannot run on non-Intel PCs, and we would probably have to add people and tools. … I'd say add another person, in addition to the time savings we already talked about. In terms of tools, we'd have to spend another $50,000 per year."

Efficiencies in patching and updating keep staff time requirements lower (technology, United States):

"If we used other PCs for the 4,800 PCs that we currently have that are Intel-based, we'd probably need more people to keep the same level of security. I'd say that we'd need at least 50% more people. … For patching and updates, it does take more time with other PCs; for Intel-based PCs, it takes an average of about an hour, and almost double that for other PCs."

Ease of onboarding requires less staff time to support (healthcare, United States):

"We have a team that onboards new PCs. It takes more time to onboard other PCs than an Intel PC because there are better tools to roll out an Intel PC. I'd say it takes about 30% longer because someone's got to babysit those. Otherwise, with Intel PCs, you literally plug in, turn it around,z and log in because the tooling is so well established."

Appendix 3: Supplemental Data

The tables in this appendix provide an accessible version of the data for the complex figures in this document. Click "Return to original figure" below each table to get back to the original data figure.

FIGURE 1 SUPPLEMENTAL DATA

PC Security- and Performance-Related IT Staff Efficiencies

	PC Security	PC Incident Management	PC Security Patching	PC Support	Total
Other PCs	5.0	2.9	1.3	1.1	10.3 hours per PC
Intel PCs	4.2	2.6	1.0	0.9	10.3 hours per PC

n = 15; Source: IDC in-depth interviews, November 2022

Return to original figure

FIGURE 3 SUPPLEMENTAL DATA

Impact on Core Security KPIs

	Other PCs	Intel PCs
Number of impactful security incidents per week	38.0	30.0
Number of data loss incidents per week	95.0	77.0

n = 15; Source: IDC in-depth interviews, November 2022

Return to original figure

Appendix 3: Supplemental Data (continued)

FIGURE 4 SUPPLEMENTAL DATA

PC Security- and Performance-Related User Productivity Losses

	Reimaging	Unplanned Downtime	Device Delivery
Other PCs	0.2	7.0	2.3
Intel PCs	0.1	5.5	1.8

n = 15; Source: IDC in-depth interviews, November 2022

Return to original figure

FIGURE 5 SUPPLEMENTAL DATA

Five-Year Cost of Operations per PC

	PC costs	IT Staff Time Costs	Cost of Lost Productivity	Cost of Risk	Total
Other PCs	$2,074	$2,744	$1,764	$277	$6,859 per PC
Intel PCs	$2,033	$2,316	$1,370	$206	$5,925 per PC

n = 15; Source: IDC in-depth interviews, November 2022

Return to original figure

About the IDC Analysts

Frank Dickson
Program Vice President, Cybersecurity Products, IDC

Frank leads the team that delivers compelling research in the areas of network security; endpoint security; cybersecurity analytics, intelligence, response, and orchestration (AIRO); identity and digital trust; legal, risk and compliance; data security; IoT security; and cloud security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson

Matthew Marden
Research Vice President, Business Value Strategy Practice, IDC

Matthew is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas with a focus on determining the return on investment (ROI) of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

@idc | @idc | idc.com