FORRESTER®

The Total Economic Impact™ Of Intel vPro® Hardware-Enabled Security Features

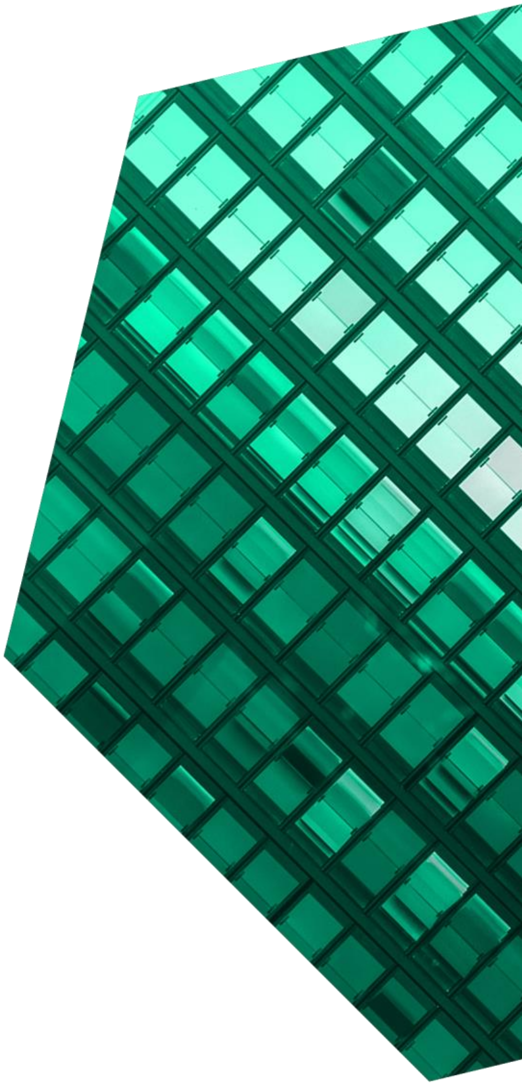
Cost Savings And Business Benefits Enabled By Intel vPro® Hardware-Enabled Security Features

SEPTEMBER 2022

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY INTEL

Table Of Contents

Consulting Team: *Chris Layton*
Tony Lam



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Intel vPro® business laptops and desktops provide hardware-enabled security through integrated technologies focused on foundational security, workload and data protection, and software reliability. Organizations that deploy mostly Intel vPro-based endpoint devices experienced fewer material breaches and were able to recover faster, saving millions of dollars annually. A portion of this benefit was directly attributable to the Intel vPro platform, which provided incremental protection beyond other measures.

The Intel vPro Enterprise platform includes hardware-enabled security features through Intel® Hardware Shield. Hardware Shield provides below-the-OS security from attacks at the firmware and hardware level, application and data protection with hardware-accelerated virtualization and encryption, and advanced threat detection and protection.

Intel Hardware Shield is comprised of security capabilities rooted in hardware to help protect each level of the compute stack. Below-the-OS security capabilities help to identify unauthorized changes to hardware and firmware to prevent malicious code injection with Unified Extensible Firmware Interface (UEFI) protection and visibility. Advanced threat protections powered by Intel Hardware Shield help shut down classes of attacks while detecting threats and reducing false positives using hardware telemetry. In addition, Intel Active Management Technology (Intel AMT) allows IT teams to manage employee endpoint devices securely and remotely, even outside of their corporate firewall.

Intel commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential benefits enterprises may realize in terms of hardware-enabled security features by deploying Intel vPro-based endpoint devices.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of hardware-enabled security features from Intel-based endpoint devices on their organizations.

KEY STATISTICS

BENEFITS PV

$520K

MATERIAL BREACH REDUCTION

28%

To better understand the benefits and risks associated with this investment, Forrester surveyed a total of 786 representatives who used primarily Intel vPro-based endpoint devices, as well as an additional 261 representatives who used non-Intel endpoint devices who were surveyed as a control group. In addition, Forrester had previously interviewed six representatives with experience deploying primarily Intel vPro-based endpoint devices in their organizations and used data from these interviews in this analysis.[2]

Forrester quantified variance in security outcomes explainable by the primary endpoint processor, independent of other hardware and security measures, using regression analysis. The analysis determined that organizations with at least 5,000 employees who used Intel vPro-based endpoint devices saw a statistically significant benefit of hardware-enabled security as compared to organizations that used non-Intel-based endpoint devices.

A statistically significant portion of the variance of this benefit could be explained by whether the organization used Intel vPro-based endpoint devices ("Intel organizations") as opposed to non-Intel-based endpoint devices ("Non-Intel organizations"), and the remaining portion of benefit appeared to be due to other factors and security measures.

For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization with 10,000 employees and billions of dollars in revenue per year.

Key results from the investment include avoided downtime from material security breaches, lower regulatory fines and penalties, and retained employee productivity.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Avoided security breach costs (excluding labor).** The composite organization avoids one material breach each year, which would have cost $767,000. Ten percent of this reduction is attributed to Intel vPro and security features enabled by Intel vPro, resulting in $172,000 of avoided costs over three years.
- **Avoided labor to investigate material breaches.** Intel vPro and the security features enabled by it allowed for a faster recovery from material breaches. Fifteen percent of this improvement is attributed to Intel vPro and the security features it enables. This, combined with one fewer breach each year, saves the composite organization $182,000 over three years.
- **Retained employee productivity.** Employees in the composite organization lose less productivity due to fewer breaches and a faster recovery from breaches. Fifteen percent of this improvement is attributed to Intel vPro and security features enabled by Intel vPro. A total of $167,000 of labor is saved over three years due to Intel vPro and the security features it enables.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Retained customers.** The composite organization can retain more customers as it has fewer material breaches; it also benefits from a faster recovery time, helping to protect customer trust.
- **Protected ecosystem trust.** Like customer trust, the composite organization can better protect the trust of ecosystem partners. This provides the composite organization with long-term benefits of better working relationships and security reputation throughout the supply chain and industry.

The financial analysis, which is based on the interviews and survey, found that a composite organization experiences present value benefits of $520,000 over three years.

> **"We're using Intel Active Management Technology to check security with service packs, in antivirus, and the other software. We collect and analyze that information from AMT so we can improve our security risk awareness."**
>
> *IT manager, government*

BENEFITS PV

$520K

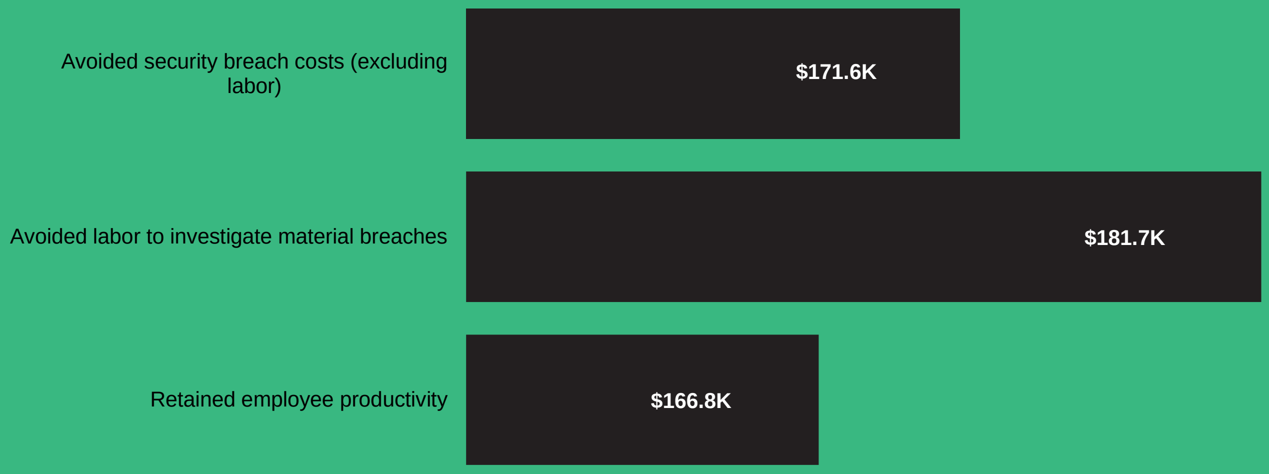
MATERIAL BREACH REDUCTION

28%

MEAN TIME TO RECOVERY REDUCTION

15%

Benefits (Three-Year)



> **“Intel vPro is really the standard. It’s the security of the silicon itself, knowing the manufacturing process, and the assurance of consistency.”**
>
> — Endpoint solutions architect, healthcare

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Intel vPro Hardware-Enabled Security.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Intel vPro Hardware-Enabled Security can have on an organization.

DUE DILIGENCE

Interviewed Intel stakeholders and Forrester analysts to gather data relative to Intel vPro Hardware-Enabled Security.

INTERVIEWS AND SURVEY

Interviewed six representatives and surveyed 786 respondents at organizations using Intel vPro Hardware-Enabled Security to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees and survey respondents.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews and survey using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees and survey respondents.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Intel and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

While Forrester did find benefit in security outcomes for organizations deploying Intel vPro endpoint devices, no product or component can be absolutely secure, and Forrester makes no guarantee of the security outcome of organizations deploying Intel vPro endpoint devices.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Intel Hardware-Enabled Security.

Intel reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Intel provided the customer names for the interviews but did not participate in the interviews.

Forrester fielded the double-blind survey using a third-party survey partner.

The Intel vPro Hardware-Enabled Security Customer Environment

🟩 Drivers leading to the vPro Hardware-Enabled Security investment

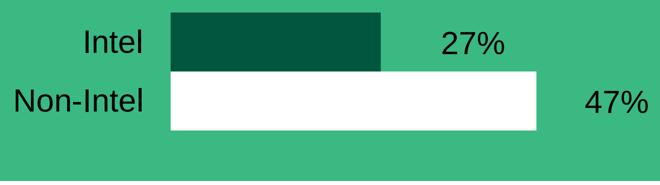
KEY CHALLENGES FOR NON-INTEL ENVIRONMENTS

Forrester surveyed 261 IT decision-makers who used mostly non-Intel-based endpoint devices. These respondents indicated that they experienced pain points in several areas that were less common for IT decision-makers using primarily Intel vPro-based endpoint devices.

This was especially true for organizations of 5,000 or more employees, who identified the following as major areas of difficulty:

- **Maintaining hardware-level upgrades across the PC device fleet.** When asked how challenging it was for their IT department to maintain hardware-level upgrades across their PC device fleet, 47% of those using primarily non-Intel based devices indicated it was “very challenging,” compared to only 27% of those using primarily Intel vPro-based endpoint devices. [3]

“Very challenging” to maintain hardware-level upgrades — grouped by most common endpoint processor

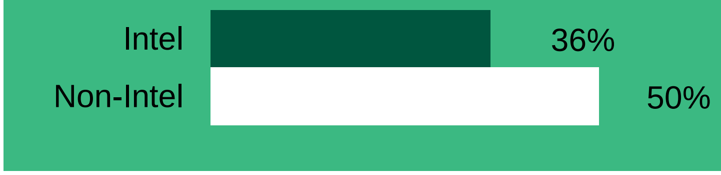


- **Meeting IT compliance standards.** When asked how challenging it was for their IT department to meet IT compliance standards across their endpoint devices, 43% of those using primarily non-Intel based devices indicated it was “very challenging,” compared to only 25% of those using primarily Intel vPro-based endpoint devices. [4]

> **“You start varying from Intel, getting other wireless chipsets … there’s a threat footprint there.”**
>
> *Endpoint solutions architect, healthcare*

- **Addressing the high cost of endpoint security.** When asked how challenging their IT department found the high cost of addressing endpoint security, 50% of those using primarily non-Intel based devices indicated it was “very challenging,” compared to only 36% of those using primarily Intel vPro-based endpoint devices.[5]
- **Providing a poor end-user experience due to security technologies.** When asked to rank their top three IT department-specific challenges, 33% of those using primarily non-Intel-based endpoints listed “poor end-user experience due to security technologies.” Only 24% of those

“Very challenging” to address high cost of endpoint security — grouped by most common endpoint processor



using primarily Intel vPro-based endpoint devices listed this pain point among their top three.[6]

COMPOSITE ORGANIZATION

Based on the interviews and survey, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the 263 survey respondents from organizations with 5,000 employees or more, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global, multibillion-dollar organization has 10,000 employees, the majority of whom have an Intel vPro endpoint device that is a laptop or desktop.

Key Assumptions

- **10,000 employees**
- **Primarily Intel-based endpoint devices**
- **Global operations**
- **Billions of dollars in revenue**

Analysis Of Benefits

🟩 Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Avoided material breach costs (excluding labor)	$68,985	$68,985	$68,985	$206,956	$171,556
Btr	Avoided labor to investigate material breaches	$73,047	$73,047	$73,047	$219,142	$181,658
Ctr	Retained employee productivity	$67,080	$67,080	$67,080	$201,240	$166,818
	Total benefits (risk-adjusted)	$209,113	$209,113	$209,113	$627,338	$520,032

AVOIDED MATERIAL BREACH COSTS (EXCLUDING LABOR)

Evidence and data. Survey respondents from organizations with more than 5,000 employees and primarily Intel vPro-based endpoint devices reported fewer breaches per year, on average, compared to their non-Intel counterparts.

- Non-Intel organizations reported an average of 3.9 material breaches per year, compared to 2.8 annual material breaches for Intel organizations.[7]

- After accounting for other differences between the two groups, including other security measures in place, regression analysis showed that the choice of processor in endpoint devices and improvements enabled by that hardware explained approximately 10% of the total variance in the difference in number of material breaches.[8]

- Intel organizations were also less likely to experience breaches because of external attacks, internal incidents, attacks or incidents involving third-party suppliers, and lost or stolen assets.[9]

- Intel vPro-based endpoint devices were less likely to be associated with hardware-level and operating system-level vulnerabilities.

Material Breaches By Primary Endpoint Processor

IT leaders were asked about the number and types of material breaches they had experienced in the past year, in addition to the level those breaches were enabled in the endpoint device.

Organizations with at least 5,000 employees using mostly Intel-based endpoint devices reported fewer breaches and were less likely to have experienced each type of breach source and type of vulnerability.

	Intel vPro	Non-Intel
Average number of breaches	2.8	3.9
Breach source		
External attack	66%	77%
Internal incident	56%	83%
Business partners/third-party suppliers	59%	77%
Lost/stolen asset (e.g., smartphone, tablet, laptop, USB flash drive, etc.)	65%	80%
Level of endpoint vulnerability		
Hardware-level vulnerability	50%	57%
OS-level vulnerability	41%	47%

- Intel organizations were more likely to prioritize hardware security in general. These security measures correlated with additional reduction in material breaches.
- Forrester has measured both the internal and external costs of a material breach. For organizations of 10,000 employees, the total cost of a material breach was $767,000.[10]

> **“We’re more than getting a return on investment [from Intel] and the number of security tools that we have that goes with it.”**
>
> *Senior IT architect, insurance*

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite organization avoids an average of one material breach per year, in part due deploying Intel vPro-based endpoint devices.
- A total of 10% of the benefit of the avoided material breach is attributed to Intel vPro hardware security and better security policies enabled by Intel vPro.
- The benefit of an avoided material breach is $767,000 in avoided internal and external costs.

Risks. The actual financial benefit will vary among organizations depending on the following factors:

- **Maturity and use of security systems and policies.** Some of the benefit of avoided material breach was from security priorities that were enabled by Intel vPro, such as higher patch rates and pre-OS boot protection. If organizations do not use Intel vPro’s hardware security features to support their security policy, they may not receive as high a benefit.
- **Other characteristics of the organization.** Much of the variance in the number of material breaches was explainable by factors other than the endpoint processor choice, such as industry, size, and IT and security budget. There may be more inherent risk for some types of organizations, and hardware security may not completely mitigate this risk.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $172,000.

Avoided Material Breach Costs (Excluding Labor)

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of material breaches for organizations using non-Intel endpoint devices	Survey	4	4	4
A2	Number of material breaches for organizations using Intel endpoint devices	Survey	3	3	3
A3	Cost of a material breach	Forrester research	$766,502	$766,502	$766,502
A4	Cost of material breaches for organizations using non-Intel endpoint devices	A1*A3	$3,066,008	$3,066,008	$3,066,008
A5	Cost of material breaches for organizations using Intel endpoint devices	A2*A3	$2,299,506	$2,299,506	$2,299,506
A6	Subtotal: avoided cost of material breaches for organizations using Intel devices	A4-A5	$766,502	$766,502	$766,502
A7	Variation in number of material breaches attributable to Intel	Survey	10%	10%	10%
At	Avoided material breach costs (excluding labor)	A6*A7	$76,650	$76,650	$76,650
	Risk adjustment	↓10%			
Atr	Avoided material breach costs (excluding labor) (risk-adjusted)		$68,985	$68,985	$68,985

Three-year total: $206,956 **Three-year present value: $171,556**

AVOIDED LABOR TO INVESTIGATE MATERIAL BREACHES

Evidence and data. Forrester research shows that significant labor is required across IT teams to correct and remediate after a material security breach occurs. Intel organizations avoided some of this labor by reducing the number of breaches that occur.

Material breach recovery for organizations using mostly Intel vPro-based endpoints:

15% faster

- Non-Intel organizations reported an average of 3.9 material breaches per year, compared to 2.8 material breaches for Intel organizations.[7]
- Intel organizations were able to recover from material breaches 15% faster than non-Intel organizations.[11]
- After accounting for other differences between the two groups, 15% of the total, weighted benefit of reducing the number of material breaches and recovering faster from breaches is attributable to Intel vPro hardware-enabled security.
- Organizations with more than 5,000 employees reported that, on average, a total of 9,600 labor hours were required to correct and remediate a material breach.[10]
- Security operations, IT/network, and development operations were required to spend more than 2,000 labor hours per material breach. Additional time was required from external resources.[10]

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite organization avoids an average of one material breach per year, in part due deploying Intel vPro-based endpoint devices.
- Of the three material breaches that do occur, the composite organization is able to recover 15% faster with Intel vPro than without it.
- A total of 15% of the benefit of the avoided material breach and the faster time to recovery when material breaches do occur is attributed to Intel vPro hardware security and better security policies enabled by Intel vPro.
- A total of 9,600 hours is required to correct and remediate after a material breach without Intel vPro and hardware security enabled by Intel vPro. This is reduced by 15% with Intel vPro.

> **"We use AMT first to check security in service packs, antivirus, and the other software in the PCs. We started to work with information that AMT gives us from every desktop so we can be aware of the risks we have."**
>
> *IT manager, government*

Risks. The actual financial benefit will vary among organizations depending on the following factors:

- **Maturity and use of security systems and policies.** Some of the benefit of avoided material breach was from security priorities that were enabled by Intel vPro, such as higher patch rates and pre-OS boot protection. If organizations do not use Intel vPro's hardware security features to support their security policy, they may not receive as high a benefit.

- **Other characteristics of the organization.** Most of the variance in the number of material breaches can be explained by factors other than the endpoint processor choice, such as industry, size, and IT and security budget. There is more inherent risk for some types of organizations, and hardware security may not completely mitigate this risk.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $182,000.

Avoided Labor To Investigate Material Breaches

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of material breaches for organizations using non-Intel endpoint devices	Survey	4	4	4
B2	Number of material breaches for organizations using Intel endpoint devices	Survey	3	3	3
B3	Total labor hours to investigate a material breach	Forrester research	7,317	7,317	7,317
B4	Weighted average hourly wage (fully burdened)	TEI standard	$51	$51	$51
B5	Total labor cost to investigate material breaches for organizations using non-Intel endpoint devices	B1*B3*B4	$1,492,668	$1,492,668	$1,492,668
B6	Reduction in mean time to investigate material breaches for organizations using Intel endpoint devices	Survey	15%	15%	15%
B7	Total labor cost to investigate material breaches for organizations using Intel endpoints	B2*B3*B4*(1-B6)	$951,576	$951,576	$951,576
B8	Subtotal: voided labor to investigate material breaches for organizations using Intel devices	B5-B7	$541,092	$541,092	$541,092
B9	Improvement in mean time to recover attributable to Intel	Survey	15%	15%	15%
Bt	Avoided labor to investigate material breaches	B8*B9	$81,164	$81,164	$81,164
	Risk adjustment	↓10%			
Btr	Avoided labor to investigate material breaches (risk-adjusted)		$73,047	$73,047	$73,047
	Three-year total: $219,142		**Three-year present value: $181,658**		

RETAINED EMPLOYEE PRODUCTIVITY

Evidence and data. Material security breaches impact affected employees' ability to perform their jobs. Organizations deploying Intel vPro-based endpoint devices reported fewer material breaches and faster recovery from material breaches, reducing the impact on affected employees.

- Non-Intel organizations reported an average of 3.9 material breaches per year, compared to 2.8 material breaches for Intel organizations. [7]
- Intel organizations were able to recover from material breaches 15% faster than non-Intel organizations.[11]
- After accounting for other differences between the two groups, 15% of the total, weighted benefit of reducing the number of material breaches and recovering faster from material breaches is explainable by Intel vPro hardware-enabled security.
- Forrester research has found that employees affected by material security breaches lose an average of 3.6 hours of productivity. [12]

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite organization avoids an average of one material breach per year, in part due deploying Intel vPro-based endpoint devices.
- Of the three material breaches that do occur, the composite organization is able to recover 15% faster.
- A total of 15% of the benefit of the avoided material breach and the faster time to recovery when material breaches do occur is attributed to Intel vPro hardware security and better security policies enabled by Intel vPro.
- The weighted average hourly salary (fully burdened) of an employee in the composite organization is $43.

Risks. The actual financial benefit will vary between organizations depending on the following factors:

- The hourly salary of employees and the opportunity cost of them not being able to perform their work during a material breach.
- The number of affected employees and the impact of a material breach on their part(s) of the organization.
- The organization's maturity and use of security systems and policies. Some of the benefit of avoided material breach was from security priorities that were enabled by Intel vPro, such as higher patch rates and pre-OS boot protection. If organizations do not use Intel vPro's hardware security features to support their security policy, they may not receive as high of a benefit.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $167,000.

Retained Employee Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of material breaches for organizations using non-Intel endpoint devices	Survey	4	4	4
C2	Number of material breaches for organizations using Intel endpoint devices	Survey	3	3	3
C3	Hours of lost productivity per employee during a material breach for organizations using non-Intel endpoint devices	Forrester research	4.0	4.0	4.0
C4	Hours of lost productivity per employee during a material breach for organizations using non-Intel endpoint devices	Forrester research	3.6	3.6	3.6
C5	Number of employees	Composite	10,000	10,000	10,000
C6	Percentage of employees impacted by material breach	Composite	20%	20%	20%
C7	Hourly salary per employee (fully burdened)	TEI standard	$43	$43	$43
C8	Lost productivity due to material breaches for organizations using non-Intel devices	C1*C3*C5*C6*C7	1,376,000	1,376,000	1,376,000
C9	Lost productivity due to material breaches for organizations using Intel devices	C2*C4*C5*C6*C7	928,800	928,800	928,800
C10	Subtotal: avoided lost productivity for organizations using Intel endpoint devices	C8-C9	$447,200	$447,200	$447,200
C11	Improvement in mean time to recover attributable to Intel	Survey	15%	15%	15%
Ct	Retained employee productivity		$67,080	$67,080	$67,080
	Risk adjustment	0%			
Ctr	Retained employee productivity (risk-adjusted)		$67,080	$67,080	$67,080

Three-year total: $201,240 **Three-year present value: $166,818**

UNQUANTIFIED BENEFITS

Interviewees and survey respondents mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Retained customers.** Business and IT leaders using mostly Intel vPro-based endpoint devices reported that their organizations were less likely to lose customers compared to leaders of organizations using mostly non-Intel-based endpoint devices. When asked about the effects of material breaches over the past year, only 29% of organizations using mostly Intel vPro-based reported a loss of customers compared to 40% of organizations using mostly non-Intel-based endpoints.[13]
- **Protected ecosystem trust.** In addition to protecting customer trust, leaders of organizations using primarily Intel vPro-based devices were less likely to report that they had lost trust of ecosystem partners (35% reported that this was true) than their counterparts at organizations using mostly non-Intel-based organizations (43% reported that this was true).[14]

> **"AMT and EMA give us security enhancements. There are some capabilities and things that are available now that weren't five years ago."**
>
> *Endpoint solutions architect, healthcare*

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Intel vPro Hardware-Enabled Security and later realize additional uses and business opportunities, including:

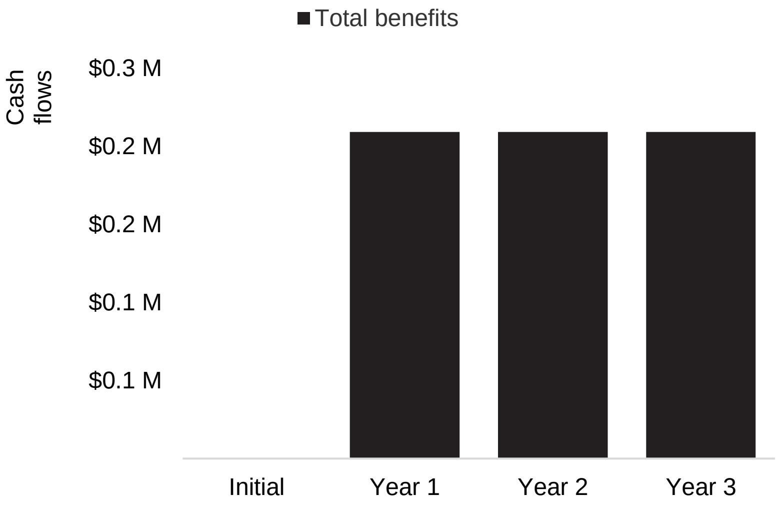
- **Continued improvements to hardware-enabled security.** Interviewees described how Intel vPro had improved its security offerings over time and that these improvements allowed IT teams to strengthen their own security position. Forrester has previously discussed how future-proofing endpoint management and security strategies can be accomplished with natively embedded technologies.[15]
- **Ongoing employee experience and flexibility.** Only 24% of surveyed leaders at organizations using mostly Intel vPro-based endpoint devices reported that poor end-user experience due to security technologies was an issue for their organization, compared to 33% of leaders from organizations using mostly non-Intel-based endpoints who noted the same.[16]

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



Forrester assumes a yearly discount rate of 10% for this analysis.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total benefits	$0	$209,113	$209,113	$209,113	$627,338	$520,032

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV Sources are calculated for each total cost and benefit estimate. NPV Sources in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value Sources of the Total Benefits and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

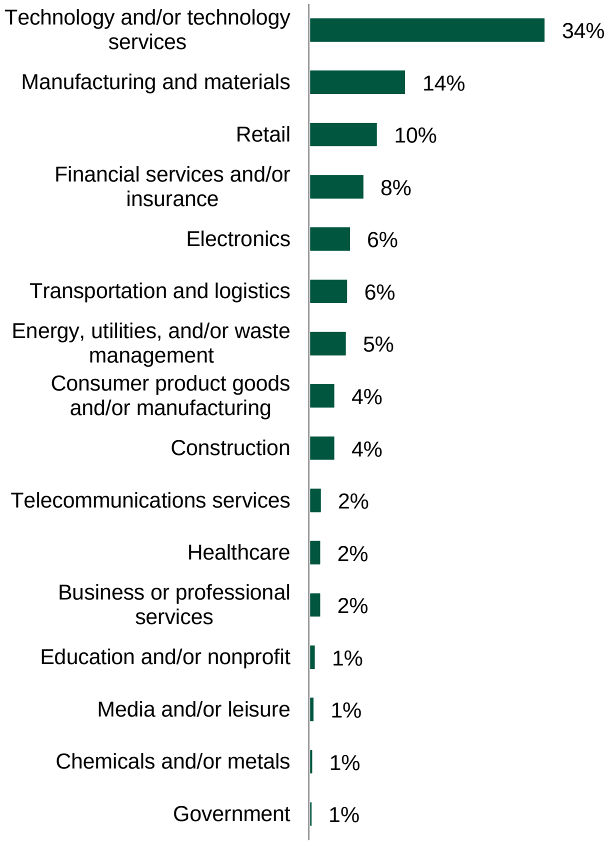
The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Interview And Survey Demographics

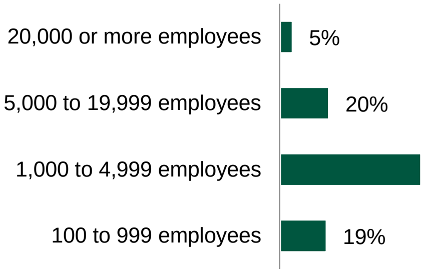
Interviews

Interviewee	Industry	Region	Employees	Intel vPro desktops And Laptops
Senior manager, endpoint planning/ engineering	Telecommunications	US with global reach	135,000	25,000
Endpoint solutions architect	Healthcare	US and UK	275,000	250,000
Senior IT architect	Insurance	US	100,000	90,000
IT infrastructure architect	Higher education	Mexico	20,000	11,500
IT manager	Government	South America	3,000	1,500
Client devices manager	Automotive	China	12,000	2,400

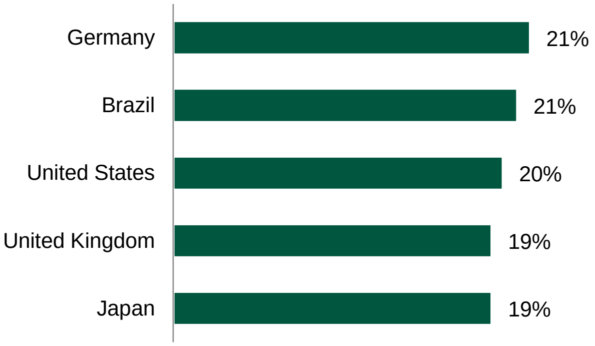
"Which of the following best describes the industry to which your company belongs?"



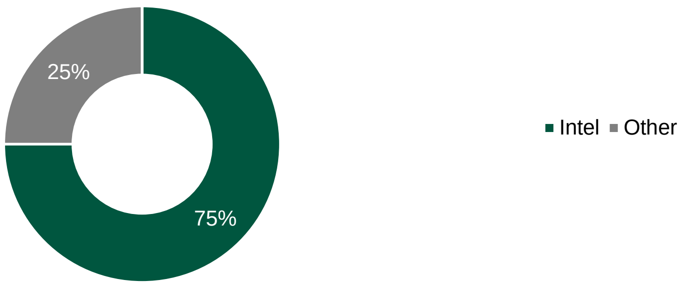
"Using your best estimate, how many employees work for your firm/organization worldwide?"



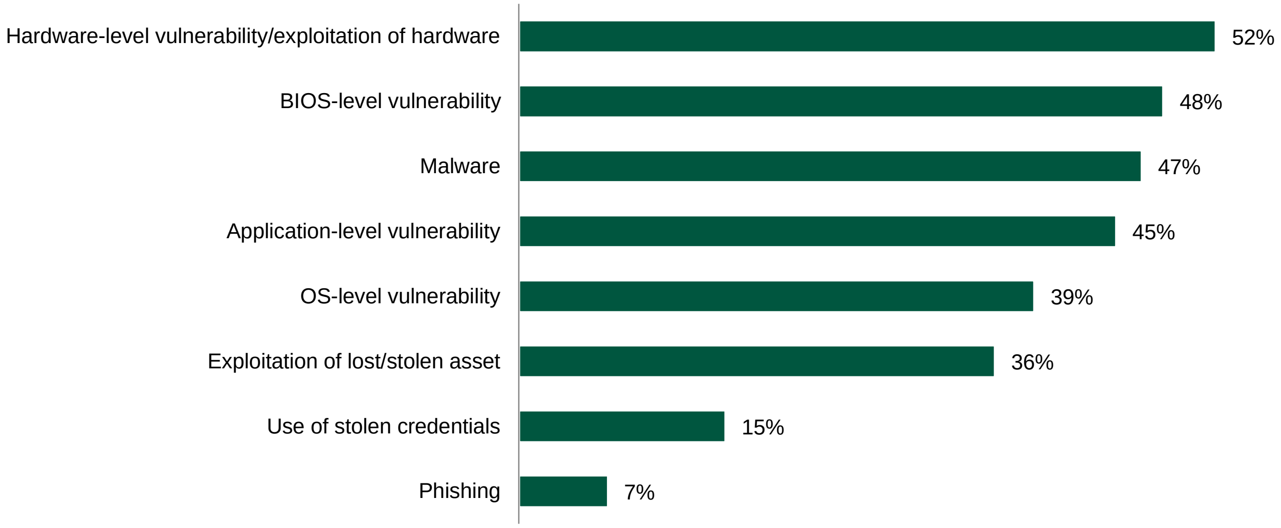
"In which country or region are you located?"



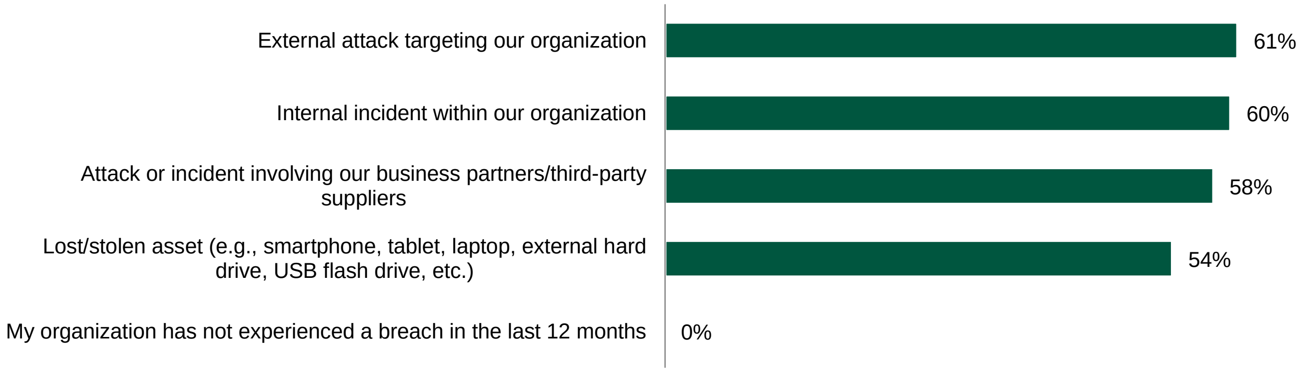
“To the best of your knowledge, what is the most common processor vendor inside your company’s Windows laptops and desktops?”



“You indicated earlier that your organization has faced a breach within the last 12 months. How was a breach enabled in your organization?" *(Select all that apply.)*



“Has your organization faced any of the following types of breaches in the last 12 months?” *(Select all that apply.)*



Appendix C: Supplemental Information

Related Forrester Research

"The Future Of Endpoint Management And Security Is Now," Forrester Research, Inc., September 1, 2022.

"Our 2022 Top Recommendations For Your Security Program: CISOs Get An Offer They Can't Refuse," Forrester Research, Inc., April 6, 2022.

Online Resources

More information about endpoint security is available on Forrester's blogs.

Appendix D: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[2] The six interviewed IT decision-makers referenced in this research were interviewed as a part of "The TEI Of The Intel vPro Platform," published in 2021. While these interviewees discussed many benefits of the Intel vPro platform, only the data on security has been included in this research.

[3] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "How much of a challenge does your IT department find the following endpoint security activities: Maintaining hardware-level upgrades across our PC fleet." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[4] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "How much of a challenge does your IT department find the following endpoint security activities: Meeting IT compliance standards." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[5] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "How much of a challenge does your IT department find the following endpoint security activities: High cost of addressing endpoint security." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[6] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "What are the top IT-department specific challenges your organization faces with its current approaches to endpoint security? (Ranked first, second, and third): Poor end-user experience due to security technologies." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[7] The percentages referenced in this paragraph are based on 719 worldwide IT decision-makers with endpoint management responsibility responding to the question "How many security breaches have happened to [device]

with [processor] at your organization in the past year?" Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, 2021.

[8] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "Has your organization faced any of the following types of breaches in the past 12 months?" Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[9] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "You indicated earlier that your organization has faced a breach within the last 12 months. How was a breach enabled in your organization?" Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[10] Survey data represented is based on a data subset base of organizations with at least 5,000 employees, taken from "Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021."

[11] The percentages referenced in this paragraph are based on 238 worldwide IT decision-makers with endpoint management responsibility responding to the question "Thinking of your most recent breach, how long did it take your organization to recover from the breach?" Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[12] Survey data represented is taken from "Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021."

[13] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "What has the impact of a breach been on your organization: Loss of customers." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[14] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "What has the impact of a breach been on your organization: Less trust from the partner ecosystem." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

[15] "The Future Of Endpoint Management And Security Is Now," Forrester Research, Inc., September 1, 2022.

[16] The percentages referenced in this paragraph are based on 239 worldwide IT decision-makers with endpoint management responsibility responding to the question "What are the top IT-department specific challenges your organization faces with its current approaches to endpoint security? (Ranked first, second, and third): Poor end-user experience due to security technologies." Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, September 2022.

FORRESTER®