A Forrester Total Economic Impact™
Study Commissioned By Microsoft
September 2017

The Total Economic Impact™ Of Microsoft Windows 10 Security Features

Cost Savings And Business Benefits Enabled By Windows 10 Security Features

FORRESTER®

Table Of Contents

Project Director:
Steve Odell

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Benefits Snapshot

Avoided costs for third-party security solutions:
$3.2 million

Reduced productivity impact of malware infections:
$1.1 million

Reduced cost of password resets:
$1.0 million

Executive Summary

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Windows 10 security features. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Windows 10 security features on their organizations.

Windows 10 security features provide a security solution that is completely integrated with the Microsoft operating system (OS), which impacts overall security and minimizes use of system resources. Forrester interviewed four customers with experience using Windows 10 security features to better understand the benefits, costs, and risks associated with this investment.

Prior to using Windows 10 security features, the interviewed customers used a myriad of third-party security solutions to handle endpoint detection and response (EDR) and endpoint protection (EPP) including antivirus/antimalware (AV), disk encryption, and data loss prevention (DLP). However, use of third-party security solutions increased the complexity of the overall security architecture and oftentimes resulted in a significant burden on system resources. Due to the significant improvements to security and performance that Microsoft introduced with Windows 10, the interviewed customers looked to reduce their overall reliance on third-party security solutions; in some cases, interviewed customers decided to use Microsoft Windows 10 security features exclusively for their endpoint security solution.

Forrester developed a composite organization based on data gathered from the customer interviews to reflect the total economic impact that Microsoft Windows 10 security features could have on an organization. The composite organization is representative of the organizations that Forrester interviewed and is used to present the aggregate financial analysis in this study. All values are reported in risk-adjusted three-year present value (PV) unless otherwise indicated.

Key Findings

Quantified benefits. The following benefits reflect the financial analysis associated with the composite organization.

- **Avoided costs for third-party security solutions by $3.2 million.** Avoided costs for the composite organization include third-party license costs for EDR, EPP, AV, and disk encryption, in addition to time savings for the security operations team.
- **Reduced productivity impact of malware infections by $1.1 million.** The composite organization experienced overall decreases in: infections requiring manual remediation, severity of infections, and mean-time-to-know (MTTK, a metric for time needed to identify potential infections).
- **Reduced costs of password resets by $1.0 million.** The composite organization realized a significant reduction in password reset requests after implementing Windows Hello (a biometric-based login system).

Unquantified benefits. The interviewed organizations experienced additional benefits that were not quantified for this study but were mentioned as significant benefits by customers:

FORRESTER®

ROI
211%

Benefits PV
$5.23 million

NPV
$3.55 million

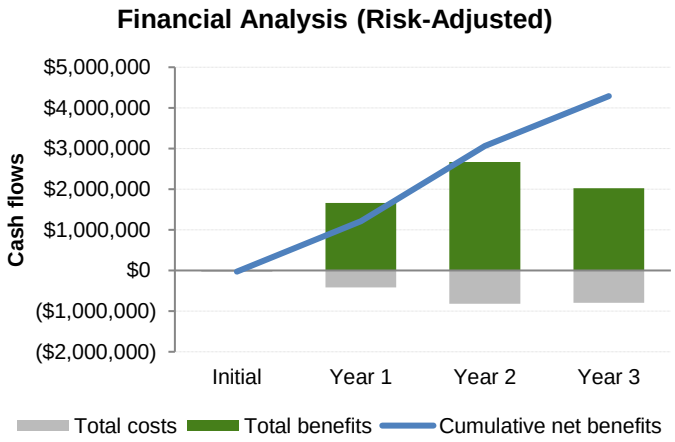
Payback
< 1 year

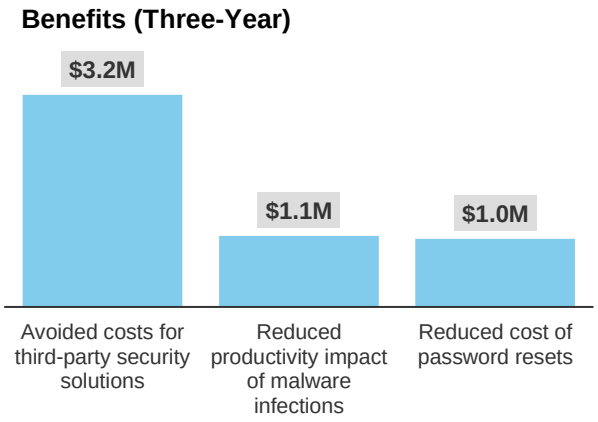
- **Improved device speed and usability, and overall reduced burden on system resources.**
- **Easier to maintain and roll out, as the security solution is integrated as part of the OS.**
- **Better visibility with Windows Defender Advanced Threat Protection (ATP).**
- **Endpoint protection while connected to any internet connection (not just the corporate network), as Windows Defender ATP works via the cloud.**
- **Cloud intelligence via Windows Defender Antivirus and Windows Defender ATP (identified as a differentiator, especially for highly mobile workforces).**
- **Reduced impact of lost devices due to disk encryption and data loss protection on these devices.**
- **Improved disk encryption performance and functionality with BitLocker.**

Costs. The following costs reflect the financial analysis associated with the composite organization.

- **License costs over $1.6 million.** In order to access Windows Defender ATP, an incremental cost per user is paid to step up from the E3 to E5 enterprise license. The composite organization migrated 7,500 users in the first year, and by year two all 15,000 users were migrated.
- **Implementation costs of nearly $66,000.** This includes time needed to evaluate Windows 10 security features, preparation of System Center Configuration Manager (SCCM) for rollback of third-party solutions and rollout of Windows 10 security, and manual update of endpoints where automatic migration failed.

Forrester's interviews with four customers, and subsequent financial analysis, found that a representative composite organization experienced financial benefits of more than $5.2 million versus costs of nearly $1.7 million, adding up to a **net present value (NPV) of $3.55 million and an ROI of 211%.**





FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Microsoft Windows 10 security features.

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 Microsoft Windows 10 security features can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Windows 10 security features.

CUSTOMER INTERVIEWS
Interviewed four organizations using Windows 10 security features to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Microsoft Windows 10 security features' impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide 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 Microsoft and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

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 report to determine the appropriateness of an investment in Microsoft Windows 10 security features.

Microsoft 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.

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

The Windows 10 Security Features Customer Journey

BEFORE AND AFTER THE WINDOWS 10 SECURITY FEATURES INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with Microsoft Windows 10 security customers. Interviewed customers include the following:

INDUSTRY	INTERVIEWEE	ANNUAL REVENUE	EMPLOYEES
Professional sports	Information technology (IT) manager	$200 million	650
Health insurance	Chief technology officer (CTO)	$10 billion	7,000
Consumer food products	Senior manager of information services	$30 billion	80,000
Aviation	Vice president (VP) of cyber security and infrastructure management	$70 billion	85,000

Key Challenges

The interviewed organizations highlighted the following challenges prior to investing in Microsoft Windows 10 security features:

- **Increased burden to maintain third-party security solutions.** Third-party security solutions were becoming increasingly complex and difficult to maintain. In some cases, organizations had to designate a full-time equivalent (FTE) to manage and maintain the multitude of third-party security software and vendors.
- **Increased burden on system resources.** As third-party security solutions do not completely integrate with the underlying OS, there is an increased and often significant demand on system resources to run endpoint security. This is a frustration point for employees, and certain business segments may require purchasing additional computing power to reconcile the difference.
- **Lack of central visibility.** Central visibility suffers due to the fragmented nature of relying on a myriad of third-party solutions for endpoint security. Additionally, the actual visibility and insight offered related to the causes of endpoint infections left much to be desired. This affected how effectively IT professionals could diagnose and remediate malware infections.

> "One of the things I'm driving for in my security role is reducing operational complexity. A lot of the issues we're seeing is due to integrations of all the third-party security. Whether it's reduced performance on laptops or integration into the management console, it's getting more and more painful in the security environment, especially for big enterprises."
>
> *VP of cyber security and infrastructure management, aviation industry*

Key Results

The interviews revealed that key quantifiable benefits from the Windows 10 security features investment include:

- **Avoided costs for third-party security solutions.**
- **Reduced productivity impact of malware infections.**
- **Reduced costs associated with password reset requests.**

These quantifiable benefits are discussed in more detail starting on page 6. The interviews also revealed several significant but unquantified results, which are detailed on page 11.

> "Our number one reason for deploying Windows 10 was for the security features."
>
> *CTO, health insurance industry*

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas of the business financially impacted. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. The composite organization is a large enterprise with 15,000 employees. It migrated from a prior state of Windows 8 using leading third-party solutions for EDR, EPP, AV, and disk encryption, to a current state using Windows 10 security features exclusively for endpoint security. The composite organization specifically deployed: Windows Defender; Windows Defender ATP; Windows Hello; and BitLocker.

Deployment characteristics. Prior to the migration, the composite organization spent four months evaluating Windows 10 security features and developing the plan to roll back the third-party security solutions and roll out Windows 10 security features. Over the next eight months, 7,500 employees were migrated to Windows 10 security features; the remaining 7,500 employees were migrated within the following year.

Key assumptions

15,000 employees

Windows Defender
Windows Defender ATP
Windows Hello
BitLocker

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Avoided costs for third-party security solutions	$1,141,125	$1,646,280	$1,010,356	$3,797,761	$3,157,044
Btr	Reduced productivity impact of malware infections	$266,870	$522,265	$511,036	$1,300,172	$1,058,183
Ctr	Reduced cost of password resets	$250,128	$500,256	$500,256	$1,250,640	$1,016,674
	Total benefits (risk-adjusted)	**$1,658,123**	**$2,668,801**	**$2,021,648**	**$6,348,573**	**$5,231,900**

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to have a PV greater than $5.2 million.

Benefit 1: Avoided Costs For Third-Party Security Solutions

Interviewed organizations described the following benefits related to reduced costs for third-party security solutions:

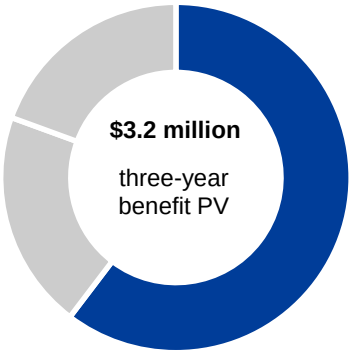
- License costs for third-party security solutions for EDR, AV, and disk encryption resulted in either a total bottom-line cost savings or a reinvestment in other high-value technology solutions when moving to Windows 10 security features for endpoint security.
- Consolidation of several third-party security solutions into a single security solution via Windows 10 resulted in a significant time savings for the security operations team, as there was no longer a need to manage and maintain third-party security solution software or vendors.

For the composite organization, Forrester assumes that:

- Based on information from the customer interviews and average list price for third-party services, third-party EDR and AV annual licenses for the composite organization cost a total of $75 per endpoint, and third-party disk encryption is a one-time cost of $100 per endpoint.
  - *Note, while these were the third-party costs for the composite organization, readers should use their own organization's costs to calculate this benefit; this will ensure any pre-existing corporate contracts or discounts are accounted for.*
- One half of an FTE is required to manage and maintain third-party security solution software and vendors.
- The annual fully burdened salary for IT security professionals starts at $120,000 and increases by 3% each year.

Avoided costs for third-party security solutions can vary with:

- License costs for third-party security solutions, depending on pre-existing corporate contracts or discounts.
- The effort associated with managing and maintaining third-party security solution software and vendors, depending on the existing overall security architecture.



Avoided costs for third-party security solutions: **60%** of total benefits

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

FORRESTER®

› Differences in annual fully burdened salaries for IT security professionals.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of nearly $3.2 million.

Benefit 1: Avoided Costs For Third-Party Security Solutions Calculation Table

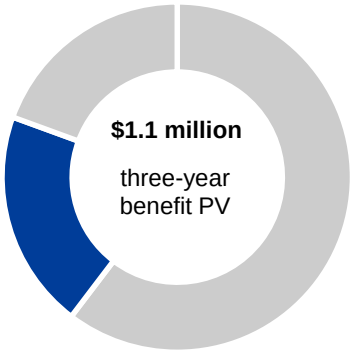
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Number of endpoints that have migrated from third-party security solutions to Windows 10 security features	Composite organization	7,500	15,000	15,000
A2	Third-party EDR annual cost per endpoint	Composite organization	$50	$50	$50
A3	Third-party antivirus annual cost per endpoint	Composite organization	$25	$25	$25
A4	Third-party disk encryption one-time cost per endpoint	Composite organization	$100	$100	$100
A5	Number of endpoints requiring disk encryption	Number of users migrated	7,500	7,500	0
A6	*Subtotal: EDR, AV, and disk encryption costs*	*A1*(A2+A3) + A4*A5*	*$1,312,500*	*$1,875,000*	*$1,125,000*
A7	FTEs no longer assigned to manage third-party software and vendors	Composite organization	0.25	0.5	0.5
A8	Annual fully burdened salary of IT security professional	Composite organization	$120,000	$123,600	$127,308
At	Avoided costs for third-party security solutions	A6 + A7*A8	$1,342,500	$1,936,800	$1,188,654
	Risk adjustment	↓15%			
Atr	**Avoided costs for third-party security solutions (risk-adjusted)**		**$1,141,125**	**$1,646,280**	**$1,010,356**

Benefit 2: Reduced Productivity Impact Of Malware Infections

Interviewed organizations described the following benefits related to reduced productivity impact of malware infections:

› When coming from Windows 7 or 8 and using third-party security solutions, interviewed organizations observed an overall decrease in total infections requiring manual remediation when using Windows 10 security features exclusively for endpoint security. The automatic identification and remediation features within Windows 10 security helped in this regard.

› Additionally, Windows 10 security features significantly reduced the rate of infections requiring a complete refresh for the endpoint (i.e., wipe-and-reload).



Reduced productivity impact of malware infections: **20%** of total benefits

- Interviewed customers effectively had zero infections with an MTTK of one day or greater when using Windows 10 security features. MTTK for most cases was seconds.

For the composite organization, Forrester assumes that:

- The annual rate of total infections on endpoints was 14.8% with the prior solution, compared to 5.3% with Windows 10 security features.
- Total infections are reduced by 5% each year given improved employee training to combat malware infections via social engineering.
- Fifty percent of infections with the prior security solution required wipe-and-reload remediation, compared to 35% of infections with Windows 10 security features.
- Wipe-and-reload remediation requires 4 hours of time (for both the IT professional and the end user), and the remainder of infections requiring manual remediation average 1 hour of time.
- Ninety percent of wipe-and-reload infections had an MTTK of one day or greater with the previous solution. While no infections with an MTTK of one day or greater were observed with Windows 10 security features, a 1% value is used for the composite organization.
- For infections with an MTTK of one day or greater, the impact to the end user could potentially be one day or more of rework due to data corruption and / or the infected endpoint being rolled back to a pre-infected version. However, as employees are likely to have backup copies of work saved on the cloud or corporate network, a four-hour exposure for rework is assumed.
- The hourly fully burdened salaries are $60 for IT professionals and $50 for the average composite organization employee; these increase by 3% each year.

The reduction in productivity impact of malware infections can vary with:

- The rate of malware infections and the resulting impact of implementing Windows 10 security features.
- The mean time for remediation, both pre- and post-Windows 10 security features.
- Fully burdened salaries for IT professionals and average employees.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of nearly $1.1 million.

> "Our number one reason for deploying Windows 10 was for the security features. We are now convinced as an organization that Windows 10 Defender AV is ready to replace our current third-party antivirus software."
>
> *CTO, Health insurance industry*

Benefit 2: Reduced Productivity Impact Of Malware Infections Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
B1	Number of endpoints that have migrated from third-party security solutions to Windows 10 security features	A1	7,500	15,000	15,000
B2	Annual rate of infections with third-party security solutions	Composite organization	14.76%	14.02%	13.32%
B3	Percent of infections requiring wipe-and-reload with third-party security solutions	Composite organization	50%	50%	50%
B4	Hours needed to remediate wipe-and-reload infections	Composite organization	4	4	4
B5	Hours needed to remediate infections not requiring wipe-and-reload	Composite organization	1	1	1
B6	Percent of infections with a MTTK of one day or greater with third-party security solutions	Composite organization	45%	45%	45%
B7	Hours of rework required for end users	Composite organization	4	4	4
B8	Hourly fully burdened salary of IT professional	Composite organization	$60.00	$61.80	$63.65
B9	Hourly fully burdened salary of average employee	Composite organization	$50.00	$51.50	$53.05
B10	*Subtotal: IT security professionals' productivity impact of malware infections with third-party security solutions*	*B8*B1*B2*(B3*B4 + [1-B3]*B5)*	*$166,050*	*$324,960*	*$317,973*
B11	*Subtotal: End users' productivity impact of malware infections with third-party security solutions*	*B9*B1*B2*(B3*B4 + [1-B3]*B5 + B6*B7)*	*$238,005*	*$465,776*	*$455,762*
B12	Annual rate of infections with Windows 10 security features	Composite organization	5.28%	5.02%	4.77%
B13	Percent of infections requiring wipe-and-reload with Windows 10 security features	Composite organization	35%	35%	35%
B14	Percent of infections with an MTTK of one or more days with Windows 10 security features	Composite organization	1%	1%	1%
B15	*Subtotal: IT security professionals' productivity impact of malware infections with Windows 10 security features*	*B8*B1*B12*(B13* B4 + [1-B13]*B5)*	*$48,708*	*$95,322*	*$93,272*
B16	*Subtotal: End users' productivity impact of malware infections with Windows 10 security features*	*B9*B1*B12*(B13* B4 + [1-B13]*B5 + B14*B7)*	*$41,382*	*$80,985*	*$79,243*
Bt	Reduced productivity impact of malware infections	(B10-B15) + (B11-B16)	$313,965	$614,430	$601,219
	Risk adjustment	↓15%			
Btr	**Reduced productivity impact of malware infections (risk-adjusted)**		**$266,870**	**$522,265**	**$511,036**

Benefit 3: Reduced Costs Of Password Resets

Interviewed organizations described that implementation of Windows Hello had the effect of reducing overall costs associated with password resets due to the reduced number of password reset requests per endpoint per year; as Windows Hello is a multifactor login system, end users no longer had to remember complex and phishable passwords since they could use a PIN or biometrics on capable devices.

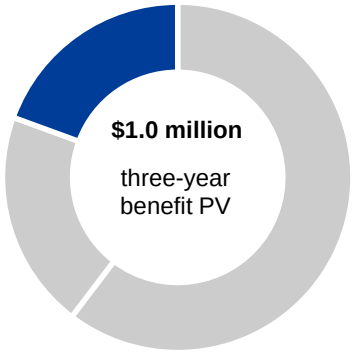
For the composite organization, Forrester assumes that:

- Each endpoint averages 1.5 password reset requests per year.
- While implementation of Windows Hello should result in nearly a 100% reduction in password reset requests, Forrester conservatively assumes an 80% reduction in identity-related reset requests since PINs may still be forgotten (albeit likely not as often, as PINs don't require the frequent periodic changes typical for phishable passwords). This also accounts for the potentially higher complexity of reset requests related to Windows Hello.
- The average cost to reset a user password is $30.88.

The reduction in costs related to password resets can vary by:

- Number of employees and average number of password reset requests.
- The average cost to reset a user password.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of over $1.0 million.



Reduced costs of password resets: **20%** of total benefits

Benefit 3: Reduced Costs Of Password Resets Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Number of endpoints that have migrated from third-party security solutions to Windows 10 security features	A1	7,500	15,000	15,000
C2	Average number of password reset requests per endpoint per year without Windows Hello	Composite organization	1.5	1.5	1.5
C3	Reduction of password reset requests due to Windows Hello	Composite organization	80%	80%	80%
C4	Average cost to reset a user password	Composite organization	$30.88	$30.88	$30.88
Ct	Reduced costs of password resets	C1*C2*C4 - C1*C2*(1-C3)*C4	$277,920	$555,840	$555,840
	Risk adjustment	↓10%			
Ctr	**Reduced costs of password resets (risk-adjusted)**		**$250,128**	**$500,256**	**$500,256**

FORRESTER®

Unquantified Benefits

While there were strong and quantifiable benefits the interviewed organizations observed by using Windows 10 security features, there were significant other benefits experienced that were not quantified for this study due to lack of available data and metrics.

Of these, the **improved device speed and usability, and overall reduced burden on system resources** experienced by using Windows 10 security features compared to third-party security solutions was a significant if intangible benefit. While the bottom-line impact to an organization of this benefit can be calculated with availability of the appropriate metrics (e.g., avoided cost of additional cloud computing, improved productivity, improved employee engagement, etc.), the overall tangible and intangible improvements associated with improved device usability was strongly echoed as a significant benefit by each of the interviewees.

> "A key consideration for endpoint security solutions is the footprint on the device itself; how big is it, how much overhead is it going to take as far as CPU and memory utilization, how well does it perform. And this is where Windows 10 security really differentiates itself."
>
> *IT manager, professional sports*

In addition to improved device speed and usability, and overall reduced burden on system resources, other unquantified benefits in this study for Windows 10 security features include:

- **Easier to maintain and roll out, as the security solution is integrated as part of the OS.** This benefit could be quantified by identifying the time spent by the IT department on testing third-party software compatibility prior to rollout of updates, and reviewing any applicable vendor management costs not already included in the analysis. Additionally, in rolling out newer, more secure updates to the Windows OS, the IT department does not have to wait for third-party vendors to update their software for compatibility with the new version of Windows.
- **Better visibility with Windows Defender ATP.** When implementing an EDR solution such as Windows Defender ATP, there is a much better "cookie trail" to see what activities occurred around the infection. For example: what the user clicked on, what resulted, and where in the process chain the infection was blocked. This results in a perpetually improving ability to diagnose and remediate infections with greater accuracy and in shortened time windows.
- **Endpoint protection while connected to any internet connection (not just the corporate network), as Windows Defender ATP works via the cloud.** The impact of this benefit could be quantified in a similar manner to benefit two (reduced impact of malware infections), by comparing end user activities being performed while on the corporate network and while off the corporate network.
- **Cloud intelligence via Windows Defender Antivirus and Windows Defender ATP (identified as a differentiator, especially for highly mobile workforces).** This provides system visibility into items such as backup update failures and information protection, while leveraging insights and information from other Windows 10 security customers; the business impact of this benefit could be quantified accordingly.

> "As a fully-integrated part of the OS, Windows 10 security is so much easier for me to maintain."
>
> *CTO, health insurance industry*

- **Reduced impact of lost devices due to disk encryption and data loss protection on these devices.** This benefit could be quantified by analyzing the value of data on lost devices, the impact on the business due to potential loss of that data to a competitor, the amount of time needed to adjust user permissions given the lost device, and potential fees or fines associated with regulatory compliance related to information privacy.
- **Improved disk encryption performance and functionality with BitLocker.** A general industry guideline is that 3% to 5% of hard drives fail disk encryption using third-party solutions, whereas with BitLocker that number is substantially less due to the lower encryption time. This lower encryption time is due to the fact that BitLocker only encrypts used space at the time of initial encryption, whereas third-party solutions always encrypt the entire drive; third-party solutions require on average an additional eight hours for disk encryption. Furthermore, BitLocker has a network unlock feature which allows system administrators to manually unlock an endpoint to apply a patch without requiring action from the end user. The business impact of this benefit could be evaluated and quantified accordingly.

"I believe the No. 1 thing we can do as an organization to improve our security stance is to have a better run desktop environment. And Windows 10 is clearly the platform for that."

CTO, health insurance industry

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Windows 10 security features and later realize additional uses and business opportunities. Flexibility factors to consider include the following:

- Windows-as-a-Service means that newer, more secure versions of Windows 10 can be deployed faster without waiting for third-party solution compatibility testing.
- Improvements, enhancements, and updates to Windows 10 security features continue to be a priority for Microsoft.
- Much of the Windows 10 security feature set is configurable based on what's most important for an organization's risk profile and can be deployed on an as-needed basis.

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

"Not only are we getting value from the security features we're using in the native OS vs. third-party now, but we have future plans to implement some of the Windows 10 security features where we have no current equivalent."

CTO, health insurance industry

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	License costs	$0	$397,500	$795,000	$795,000	$1,987,500	$1,615,684
Etr	Implementation costs	$28,080	$21,450	$22,094	$0	$71,624	$65,839
	Total costs (risk-adjusted)	**$28,080**	**$418,950**	**$817,094**	**$795,000**	**$2,059,124**	**$1,681,523**

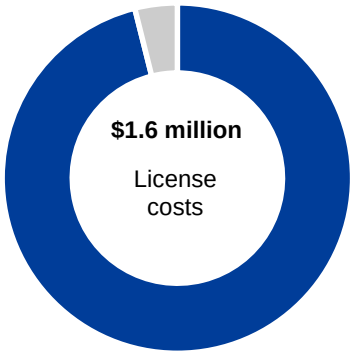
Cost 1: License Costs

For the composite organization, Forrester assumes that an incremental cost per user to step up from the E3 to E5 license is paid to access Windows Defender ATP. By Year 2, all 15,000 endpoints have upgraded to the E5 license. This yields a three-year risk-adjusted total PV of over $1.6 million.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to have a PV of nearly $1.7 million.

Cost 1: License Costs Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Windows 10 E3 to E5 license cost	Composite organization		$397,500	$795,000	$795,000
Dt	License Costs	D1	$0	$397,500	$795,000	$795,000
	Risk adjustment	0%				
Dtr	**License Costs (risk-adjusted)**		**$0**	**$397,500**	**$795,000**	**$795,000**



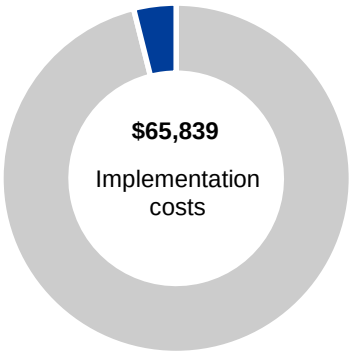
Cost 2: Implementation Costs

Interviewed organizations discussed the following costs associated with implementation of Windows 10 security features:

- Evaluation of Windows 10 security features and planning and preparation for uninstalling third-party security solutions.
- SCCM preparation and setup of automated migration.

For the composite organization, Forrester assumes:

- Evaluation of Windows 10 security features and planning and preparation for uninstalling third-party security solutions required three weeks of effort for an IT security professional.
- SCCM preparation required one IT professional devoted half the time for three months.
- Two percent of automated migrations failed, requiring a manual update to be initiated during normal working hours.



FORRESTER

Implementation costs can vary by:

- Planning time required for third-party solution rollback and Windows 10 security features rollout.
- Percent of failed automated migrations and amount of time required for a manual update.
- IT professional and average employee fully burdened salaries.

To account for these risks, Forrester adjusted this cost upward by 30%, yielding a three-year risk-adjusted total PV of nearly $66,000.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

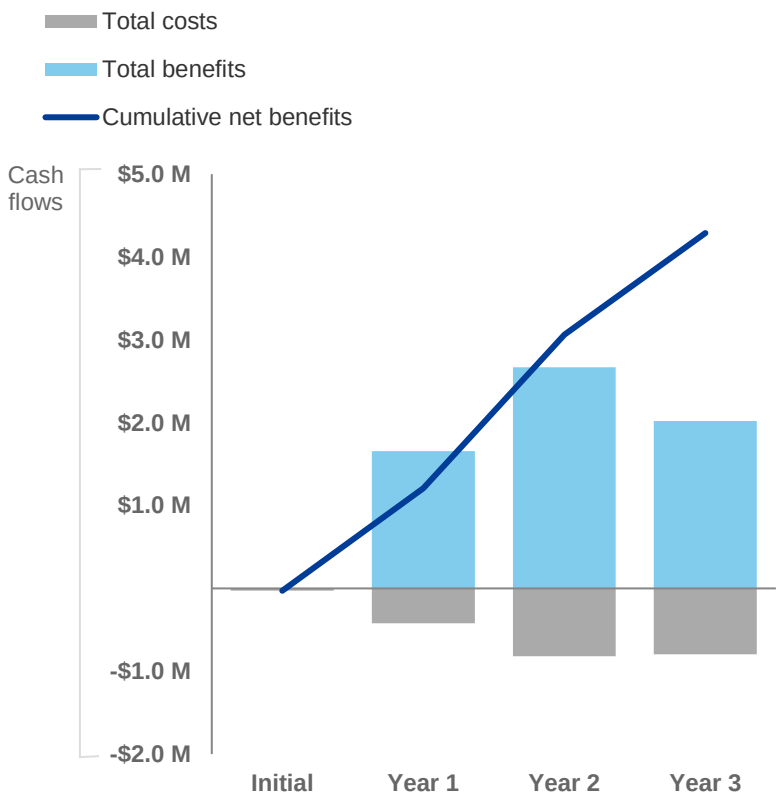
Cost 2: Implementation Costs Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Planning and preparation for uninstalling third-party security solutions	120h * B8	$7,200			
E2	SCCM preparation	0.5 * 12 weeks * 40h/week * B8	$14,400			
E3	Number of automated migrations performed	Composite organization		7,500	7,500	
E4	Percent of failed migrations requiring manual updates	Composite organization		2%	2%	
E5	Hours required to initiate manual update	Composite organization		1	1	
Et	Implementation costs	E1 + E2 + E3*E4*E5* (B8+B9)	$21,600	$16,500	$16,995	$0
	Risk adjustment	↑30%				
Etr	**Implementation costs (risk-adjusted)**		**$28,080**	**$21,450**	**$22,094**	**$0**

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($28,080)	($418,950)	($817,094)	($795,000)	($2,059,124)	($1,681,523)
Total benefits	$0	$1,658,123	$2,668,801	$2,021,648	$6,348,573	$5,231,900
Net benefits	($28,080)	$1,239,173	$1,851,708	$1,226,648	$4,289,449	$3,550,377
ROI						211%
Payback period						< 1 year

FORRESTER®

Microsoft Windows 10 Security Features: Overview

The following information is provided by Microsoft. Forrester has not validated any claims and does not endorse Microsoft or its offerings.

Designed to be the most secure Windows yet

Addressing today's threats requires a new approach, one that engineers the attack vectors out of the platform itself and quickly detects and responds to the ones that remain. With Windows 10, you get holistic protection for addressing malware and hacking threats, protecting information, securing identities and access control, and management.

Pre-Breach Threat Resistance

Windows 10 is designed to disrupt the malware and hacking industry, and it moves the playing field to one where your adversaries will lose the very attack vectors that they depend on.

Windows Defender Antivirus

Windows Defender Antivirus, an enterprise-grade antivirus solution, uses the cloud, vast optics, machine learning, and behavior analysis to rapidly respond to emerging threats.

Microsoft Edge

Attacking devices through the browser is a top technique for attackers. Microsoft Edge has been designed specifically to systemically disrupt phishing, malware, and hacking attacks.

Device Guard

Application Control is your best defense in a world where there are more than 300,000 new malware samples each day. Block all unwanted apps with Device Guard.

Trusted Boot

UEFI Secure Boot and Windows Trusted Boot help maintain the integrity of the system by ensuring malware is unable to start before system defenses.

Trusted Platform Module (TPM)

Windows 10 devices include TPM providing hardware isolated capabilities to securely create and store keys and enable advanced conditional access.

Containers

Windows 10 uses containers to isolate sensitive system services and data, enabling them to remain secure even when the OS has been compromised.

FORRESTER®

Post-Breach Detection and Response

Windows Defender Advanced Threat Protection enables you to detect, investigate, and respond to advanced threats and data breaches on your networks.

Detect the undetectable

Take advantage of IOCs powered by sensors and unique optics that are made possible through Microsoft Intelligence Security Graph and the human expertise behind it.

Built into Windows 10

Agentless with high performance and low impact, cloud-powered; easy management with no deployment.

Built-in one-click responses

Respond to incidents by isolating machines, blocking or quarantining files, collecting data, and executing suspicious files in a secure cloud based.

Identity Protection

Windows 10 provides next-generation technology to help protect your users' identities from abuse.

Windows Hello

Windows Hello is a password alternative that uses multiple factors to provides enterprise-grade security using biometrics, a PIN, or even a companion device.

Credential Guard

Credential Guard protects against NTLM-based Pass the Hash (PtH) attacks by isolating user credentials inside a hardware-based container.

Information Protection

Windows 10 provides comprehensive data protection while meeting compliance requirements and maintaining user productivity.

BitLocker

BitLocker enables organizations to protect sensitive information from unauthorized access with military grade encryption when a device is lost or stolen.

Windows Information Protection

Business data is separated and contained to prevent it from accidentally leaking to unauthorized users, documents, apps, or locations on the web.

Azure Information Protection

Azure Information Protection, included separately, works with WIP and provides additional capabilities to classify, assign advanced permissions, and share sensitive data.

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 calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, 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.

FORRESTER®