FORRESTER®

NEW TECH

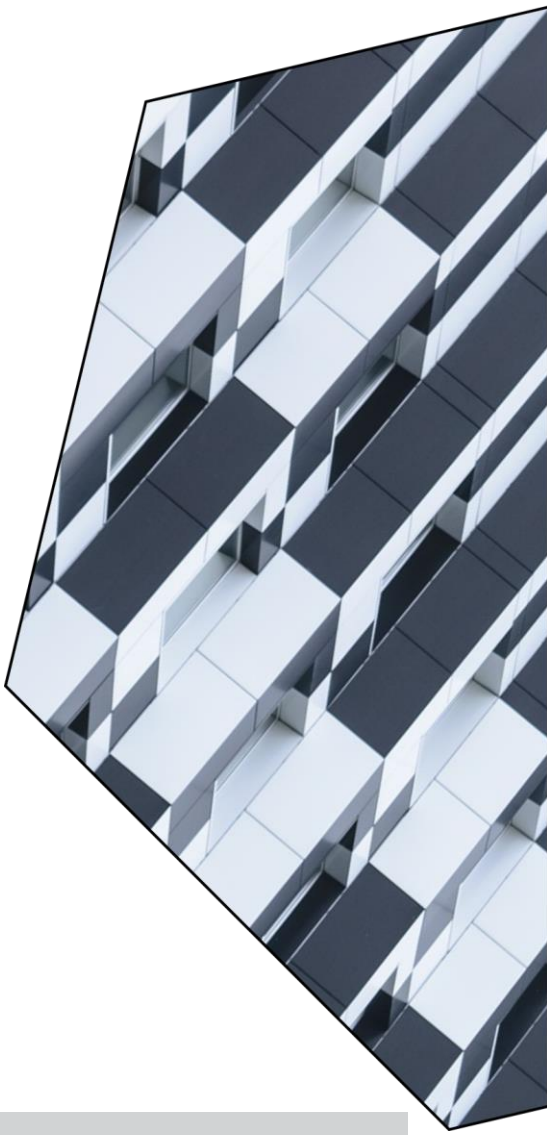
New Technology: The Projected Total Economic Impact™ Of Windows Autopatch

Cost Savings And Business Benefits Enabled By Windows Autopatch

MARCH 2023

Table Of Contents

Consulting Team: Nicholas Ferrif
Otto Leichliter
Uddhav Bagrodia



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

Unpatched software vulnerabilities continue to be among the most common vectors for bad actors to gain access to a network.[1] Amid escalating risks, many organizations rely on the same patching processes even though their device populations and workplaces have evolved. When every update not applied represents a potential attack vector, allowing Microsoft to automatically manage and monitor the updating process can improve patch success rates, which reduces vulnerabilities while freeing up valuable IT resources.

Windows Autopatch is a cloud service that automates monthly quality updates, feature updates, and zero-day patches for the Windows operating system (Windows OS) and M365 applications. Microsoft offers Windows Autopatch at no additional cost for organizations with Windows E3/E5 licenses, and devices that leverage Azure active directory (Azure AD) and Microsoft Intune are eligible for enrollment. Once an organization is onboarded and enrolls its devices, Windows Autopatch automatically creates multiple progressive deployment rings and applies the latest updates according to the organization's custom configuration and Microsoft best practices.

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 Autopatch.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Windows Autopatch on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed 10 representatives with experience using Windows Autopatch. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global, multibillion dollar conglomerate with 8,000 FTEs.

Prior to using Windows Autopatch, the interviewees' organizations typically leveraged Microsoft Configuration Manager to update and patch devices, and some interviewees' organizations leveraged cloud-based products like Intune while others used third-party tools for their monthly, feature, and zero-day patching. Interviewees said that with these tools, their organizations were stuck in labor-intensive monthly patching loops that were only moderately effective. This created ongoing resource constraints and left the organizations with difficult-to-decipher errors and unpatched vulnerabilities.

After enrolling in Windows Autopatch, Microsoft automated previously manual tasks associated with patching, and this freed up time for the organizations' IT teams to focus on value-add projects such as process improvements or building out additional automation. Windows Autopatch also improved the update success rate and the time it took to reach a compliant state each month, which improved security postures and revealed better visibility into the

KEY STATISTICS

Reduced labor associated with feature updates by
50% - 95%

Projected net present value (NPV)
$488K - $1.6M

patching process. Key results from the adoption of Windows Autopatch included: efficiency gains for patching, compliance, and reporting teams; improved patch success rates; and efficiency gains for employee end-users.

KEY FINDINGS

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

- **Savings of $848,000 in efficiency gains for the patching team.** The composite organization experiences efficiency gains for its patching process because Windows Autopatch automates many of the tasks involved with monthly quality updates, feature updates, and zero-day patches.
- **80% efficiency gain for IT teams in reporting compliance regarding patching.** Windows Autopatch enables the composite to do self-service reporting and reduces its number of ad hoc requests. Additionally, the centralized Windows Autopatch dashboard allows its teams to generate drill-down reports to help identify errors and problem solve efficiently.
- **13 percentage point increase in patch success rate, reduced disruptions to end users, and reduced number of help desk tickets.** By automating patching and shifting responsibility to Microsoft, the composite organization reduces the number of errors and unpatched devices, which subsequently reduces disruptions for end users and associated help desk tickets.
- **Savings of nearly $470,000 from reduced use of prior solutions and on-prem infrastructure.** After the composite organization implements Windows Autopatch, it reduces the use of prior solutions and infrastructure. Some organizations can completely eliminate while others still use portions of their infrastructure for alternate use cases like air-gapped networks.

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

- **Improved security posture.** Staying up to date gives the composite organization better protection against cyberthreats.
- **Shift in decision-making for patching to Microsoft.** With Windows Autopatch, the composite's IT teams rely on Microsoft to determine which updates to push, patching cadences, and other planning activities. This frees up their time to focus on how IT can help improve the business in other ways.

Costs. The three-year, risk-adjusted PV costs for the composite organization include:

- **$229,000 in labor costs for existing resources to deploy, run, and monitor Windows Autopatch over three years.** Once the composite organization fully deploys Windows Autopatch, it's managed by one IT maintenance staffer who is responsible for multiple solutions. As such, the composite doesn't incur any additional managent costs. For deployment, Windows Autopatch fits well within the composite's current workstreams, and the patching team realizes time savings quickly. There are no other direct costs.

Forrester modeled a range of projected low-, medium-, and high-impact outcomes based on evaluated risk. This financial analysis projects that the composite organization accrues the following three-year net present value (NPV) for each scenario by enabling Windows Autopatch:

- Projected high impact of a $1.6 million NPV.
- Projected medium impact of a $1.1 million NPV.
- Projected low impact of a $488,000 NPV.

Because the benefits can be viewed as incremental benefits to leveraging a Windows E3 or E5 license, Forrester did not include an ROI analysis.

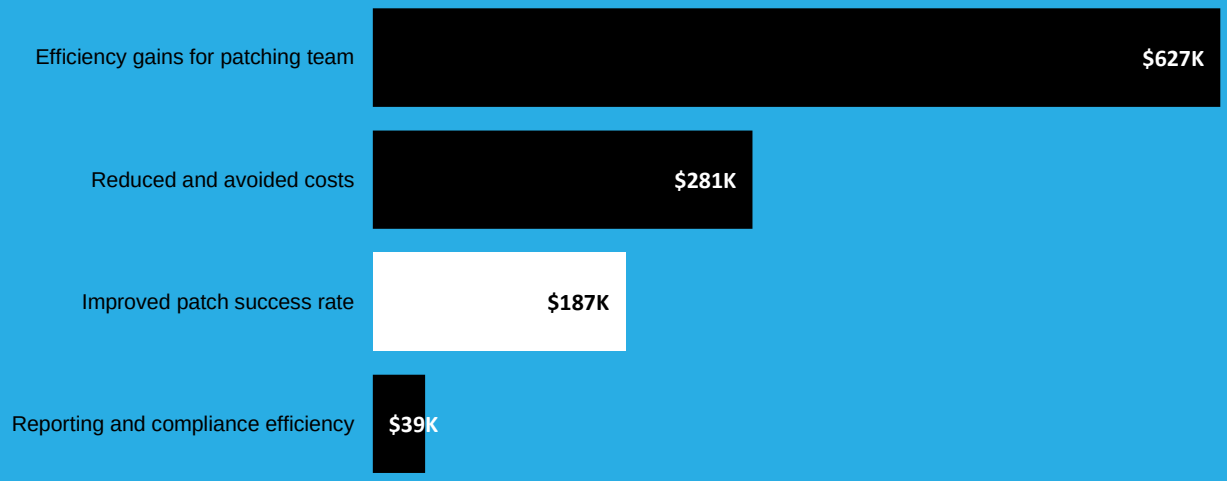
REDUCED LABOR FOR QUALITY UPDATES
Up to 45%

REDUCED LABOR FOR FEATURE UPDATES
Up to 95%

REDUCED LABOR FOR COMPLIANCE AND REPORTING
Up to 80%

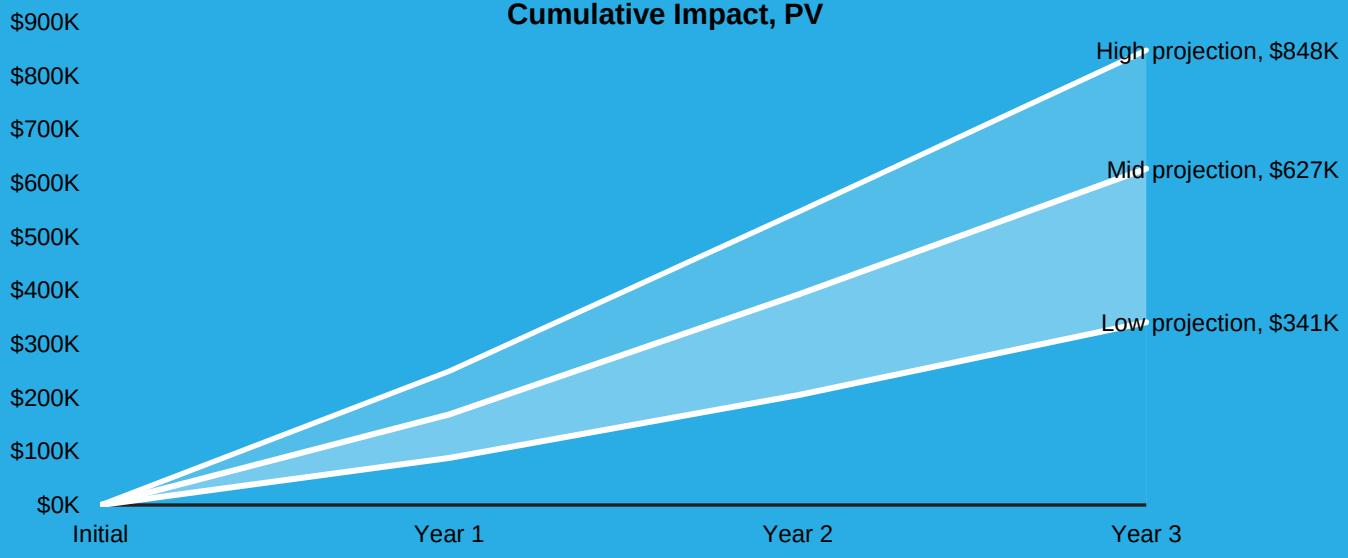
ACHIEVE CONSISTENT PATCH SUCCESS RATE
95%+

Projected Benefits (Three-Year)



Figures in the chart below are projections for the mid-case scenario.

Efficiency Gains For Patching Team Module: Range Of Three-Year Cumulative Impact, PV



NEW TECH TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a New Technology: Projected Total Economic Impact™ (New Tech TEI) framework for those organizations considering an investment in Windows Autopatch.

The objective of the framework is to identify the potential cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the projected impact that Windows Autopatch can have on an organization.

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 study to determine the appropriateness of an investment in Windows Autopatch.

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.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Windows Autopatch.

EARLY-IMPLEMENTATION INTERVIEWS

Interviewed 10 representatives at organizations using Windows Autopatch to obtain data with respect to projected costs, benefits, and risks. Some of the interviewees' organizations had fully enrolled in Windows Autopatch while others were in pilot or beta stages.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

PROJECTED FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of New Tech TEI in modeling the investment's potential 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.

The Windows Autopatch Customer Journey

Drivers leading to the Windows Autopatch investment

Interviews			
Role	**Industry**	**Region**	**Number of Windows devices**
IT infrastructure architect and strategic lead	Government	UK	2,250
IT enterprise architect and head of global deployment services	Pharmaceutical	Global	100,000
Technical services manager	Manufacturing	Global	56,000
Senior cloud engineer	Government	Australia	4,500
Hardware network manager	Government	UK	1,800
CTO of industrial business	Retail/manufacturing	Global	8,000
CISO and chief data protection officer	Digital services	Global	7,500
Program manager for cloud platform	Manufacturing	Global	15,000
System analyst	Construction and logistics	Global	4,000
Manager of computing solutions	Chemicals	Global	8,000

KEY CHALLENGES

Interviewees reported that prior to enrolling in Windows Autopatch, their organizations struggled to consistently achieve high patch success rates, they lacked visibility into their patching processes, and their IT teams dedicated too many resources to patching. These challenges delayed other more impactful projects.

The interviewees noted how their organizations struggled with common challenges, including:

- **Difficulty developing and defending patching cadence and general best practices.** The organizations' patching processes including planning, cadence, and success rates are often reported directly to their executive teams or their boards, which forces IT professionals to constantly explain and defend their decisions. An IT enterprise architect and head of global

"Before [enrolling in Windows] Autopatch, by the time we had targeted all 100,000 systems, the new patch was already released. So, we would have to decide between fixing the systems that didn't get last month's patch or focusing on getting this month's patch rolled out."

IT enterprise architect and head of global deployment services, pharmaceutical

deployment services from a pharmaceutical company said, "What attracted me to Windows Autopatch was the management from the Microsoft side [and] having that set of people from Microsoft monitoring it and watching over it."

- **A need to increase visibility and improve reporting of issues.** One of the most used vectors for a cyberattack is through an unpatched device or system.[3] That's why it is crucial for organizations to be able to accurately monitor patching success on each endpoint and remediate issues when they occur. A system analyst for a construction and logistics company said: "Previously, before [enrolling in] Windows Autopatch, there were some issues where we weren't getting everything patched that we were expecting. Reports weren't really giving us what we were looking for. We would deploy a patch, and a month later, we would find out a couple hundred machines didn't get patched correctly."
- **A mix of devices, configurations, and versions on the network.** Multiple interviewees reported that their organization struggled to reach acceptable patch compliance rates because it supports many different versions of Windows, various tools, and device/OS configurations in its environment.

"We've invested heavily in the Microsoft stack, and Windows Autopatch adds to the value for money."

IT infrastructure architect and strategic lead, government

- **End users experiencing recurring issues with patching.** One of the challenges interviewees mentioned was that issues or bugs that occurred in the patching process caused disruptions to end users' experiences. A CISO and chief data protection officer for a digital services company said, "Depending on the type of issue or bug, there could be disruptions to end users' experiences that [could] last from a few hours to a day or two."

WHY WINDOWS AUTOPATCH?

The interviewees' organizations searched for a solution that could:

- **Make patching processes more efficient.** Interviewees said one of the benefits their organizations were looking to get from Windows Autopatch was having less direct involvement in monthly quality updates and annual feature updates. Interviewees said they are excited to push some of the responsibility, research, and planning to Microsoft.

  A technical services manager from a manufacturing organization said: "Windows Autopatch gives us an opportunity to do more than we were. It gives us the opportunity to let us make the improvements that need to be made and to automate the patching process."

  A system analyst for a construction and logistics company said, "It helps that determining patching cadence is now on Microsoft's plate instead of ours."
- **Address vulnerabilities and quality updates as soon as possible.** A technical services manager with a manufacturing organization said: "We are joined at the hip with our security team when it comes to patching and lifecycle management. We are embracing new terminology and a new culture around attack-surface reduction and minimizing risk vectors into

our network, and Windows Autopatch is helping with that."

- **Move to modern management.** Windows Autopatch delivers a cloud-based patching mechanism that is identical regardless of a device's location. An IT enterprise architect and head of global deployment services with a pharmaceutical company said: "My hope for Windows Autopatch is to give users the same experience patching their work devices that they have at home. It is going to be very close to the consumer experience."

COMPOSITE ORGANIZATION

Based on the interviews, 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 10 interviewees, 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 composite organization is a global, multibillion-dollar conglomerate headquartered in the US, and it has both B2C and B2B sales channels. The composite organization is an existing Microsoft customer with a Windows E3 license, so Windows Autopatch is included in the contract at no extra cost. The composite has 8,000 eligible devices with a roughly 1:1 ratio for Windows devices to employees. The team responsible for managing monthly patches, feature updates, and zero-day patches consists of six FTEs. Prior to enrolling in Windows Autopatch, the composite organization primarily relied on Configuration Manager for quality updates. It performed quality updates monthly, and this would take between three and four weeks before starting the process over again for the next month. The composite planned annual feature updates, but it only executed them every 18 months due to resource constraints and configuration challenges.

Deployment characteristics. The composite organization starts by piloting Windows Autopatch with 300 devices spread throughout its global network. After three successful quality update cycles for the pilot group, the composite organization enrolls all 8,000 devices (which includes issuing new/upgraded devices for any out-of-compliance devices) into Windows Autopatch. Once all the devices are enrolled, the composite organization also pushes out a feature update to all devices with minimal manual effort to get all of them to the same version.

Key Assumptions

- **Global, multibillion-dollar conglomerate**
- **8,000 Windows devices**
- **Six FTEs responsible for patching**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Projected Benefits

Projected Benefits	Year 1	Year 2	Year 3	Total	Present Value
Total projected benefits (low)	$137,137	$203,623	$259,351	$600,111	$487,808
Total projected benefits (mid)	$324,445	$489,824	$576,695	$1,390,964	$1,133,042
Total projected benefits (high)	$470,018	$679,976	$789,887	$1,939,881	$1,582,707

EFFICIENCY GAINS FOR PATCHING TEAM

Evidence and data. Interviewees noted that Windows Autopatch automated many of the processes involved with monthly quality updates, annual feature updates, and zero-day patches.

- Prior to enrolling in Windows Autopatch, interviewees said they had to perform the same set of manual tasks month after month to keep devices up-to-date and protect their organizations' networks. Tasks such as planning which patches to push, creating test groups, and troubleshooting devices that failed would lock valuable staff resources in never-ending loops, which made it much more difficult to contribute to projects or add value to the businesses.
- With Windows Autopatch, the organizations' IT teams gained the ability to completely eliminate many manual tasks through automation, and they can now monitor progress from the central dashboard. A senior cloud engineer in government said, "I'm really excited about Microsoft handling the auto-zoning of the clients to the different rings and how to manage that."
- Each interviewee said they were excited that Windows Autopatch allowed their teams to automate the feature-update process and that they reported significantly fewer issues and less effort. Interviewees said that with Windows Autopatch, they feel confident that their organizations can accelerate the pace of feature updates and eliminate a significant amount of labor.
- Interviewees said that prior to enrolling in Windows Autopatch, their organizations had mixed success deploying zero-day patches and they found the processes to be disruptive. They said with Windows Autopatch, they feel their organizations are better protected, and they are happy to let Microsoft determine the best timing and methods to push out those patches.

> **"We used to have to stage it. We used to have to communicate. We used to have to do all these different things when we did it [with Configuration Manager]. Now, with Windows Autopatch, we basically let it look after itself."**
>
> *IT infrastructure architect and strategic lead, government*

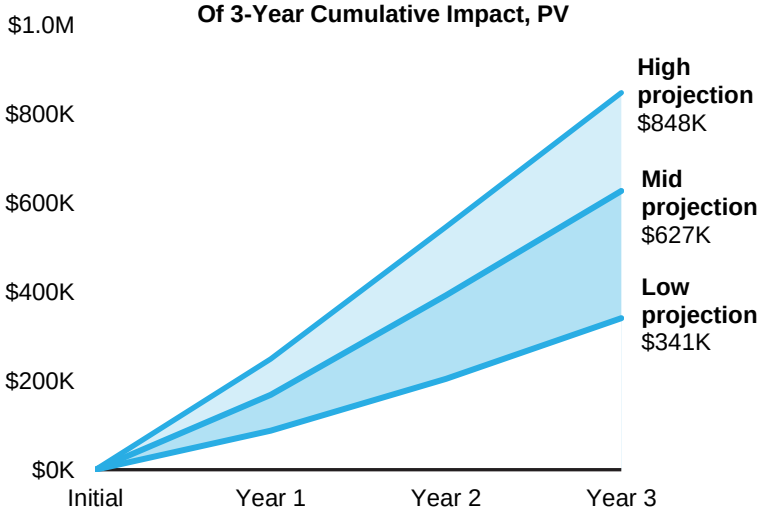
- A CISO and chief data protection officer in the IT industry said: “If we’re able to save 20% to 30% of the time for our support teams from the existing patching exercise and move those orders to Windows Autopatch, then that 30% [of] time can be leveraged by those IT support staff on other projects that are getting pushed out because they’re just too busy with the patching cycle.”
- An IT enterprise architect and head of global development services in the pharmaceutical industry claimed that their organization saves one week’s worth of effort for its IT resources responsible for patching every month during its patch cycle. They said: “With [Windows] Autopatch, we go to test ring on patch Tuesday and then the completion target is by the end of the month, which, at worst case scenario, will give us eight days between the end of one patching round and the beginning of the next. So … I expect that we’re going to consistently see a one-week improvement.”

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite dedicates six FTEs to patching Windows devices, and this includes conducting quality, feature, and zero-day updates.
- The average fully burdened salary of a patching team member is $135,000 per year.
- With Windows Autopatch, the composite organization expects to reduce manual effort related to monthly quality updates and zero-day patches by between 20% and 45%. Organizations with more third-party applications or non-Windows apps and devices may experience the lower range while organizations that highly leverage the Microsoft suite can expect to achieve greater efficiency gains.
- The composite organization completes one feature update annually, and it takes 600 labor-hours to complete it.
- With Windows Autopatch, the composite organization reduces the manual effort associated with feature updates by between 50% and 95%. Organizations that have more consistent configurations, devices, and versions can expect to achieve greater efficiency gains.

Results. This yields a three-year projected PV ranging from $341,000 (low) to $848,000 (high).

Efficiency Gains For Patching Team Module: Range Of 3-Year Cumulative Impact, PV



“[Windows Autopatch] provides a more automated [and] efficient solution that reduces our risk and frees up our resources’ time to go work on strategic initiatives that are value-add or growth-focused. From that perspective, [Windows] Autopatch is kind of a no-brainer.”

CTO of industrial business, retail/manufacturing

Efficiency Gains For Patching Team					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Team members responsible for monthly patching (e.g., planning, testing, monitoring, troubleshooting)	Composite	6	6	6
$A2_{Low}$	Monthly patching process efficiency gain with Windows Autopatch	Composite	10%	15%	20%
$A2_{Mid}$			20%	30%	35%
$A2_{High}$			30%	40%	45%
A3	Annual salary of a patching team member	TEI standard	$135,000	$135,000	$135,000
$A4_{Low}$	Subtotal: Efficiency gain for monthly patches	A1*A2 low*A3	$81,000	$121,500	$162,000
$A4_{Mid}$		A1*A2 mid*A3	$162,000	$243,000	$283,500
$A4_{High}$		A1*A2 high*A3	$243,000	$324,000	$364,500
A5	Feature update frequency	Composite	1	1	1
A6	Feature update effort (hours)	Composite	600	600	600
$A7_{Low}$	Feature update efficiency gain with Windows Autopatch	Composite	40%	50%	50%
$A7_{Mid}$			60%	70%	75%
$A7_{High}$			80%	90%	95%
$A8_{Low}$	Subtotal: Efficiency gain for feature updates	A5*A6*A7 low*A3/2,080	$15,577	$19,471	$19,471
$A8_{Mid}$		A5*A6*A7 mid*A3/ 2,080	$23,365	$27,260	$29,207
$A8_{High}$		A5*A6*A7 high*A3/2,080	$31,154	$35,048	$36,995
At_{Low}	Efficiency gains for patching team	A4 low+A8 low	$96,577	$140,971	$181,471
At_{Mid}		A4 mid+A8 mid	$185,365	$270,260	$312,707
At_{High}		A4 high+A8 high	$274,154	$359,048	$401,495
Three-year projected total: $419,019 to $1,034,697			**Three-year projected present value: $340,644 to $847,614**		

REPORTING AND COMPLIANCE EFFICIENCY

Evidence and data. Interviewees noted that Windows Autopatch enabled their organizations to use self-service for reporting, which reduced the number of ad hoc requests to support teams and improved compliance.

- Before enrolling in Windows Autopatch, it was difficult to track which devices were successfully patched and which weren't and what went wrong. With a centralized dashboard, managers and teams gained the ability to access an array of reports to solve problems efficiently. A manager of computing solutions in the chemicals industry explained: "If machines weren't getting patched, that was up to somebody else to decide. But now I've got a centralized dashboard I can look at and I [can] share this very easily with the other folks and say, 'Hey, come check your report. See how

your devices are doing.' They have the information so they can go and troubleshoot and diagnose and get the endpoint patched."

- Compliance efficiency has a domino effect on various aspects of a firm, such as reduced help desk tickets for support teams and improved security posture. An IT enterprise architect and head of global deployment services in the pharmaceutical industry said: "Working towards that 99% success rate is important. The hidden security benefit of this is those issues that cause noncompliance are much easier to address and resolve with Windows Autopatch's reporting, so we have fewer vulnerabilities."
- The speed with which an organization reaches compliance is also imperative to the operations, even if the level of compliance remains constant. The same interviewee explained: "[If] we can increase the speed at which we can reach compliance — even if we continue to reach the current compliance level — that, for me, is another benefit of [Windows] Autopatch. And from what we have seen so far, we are achieving higher compliance at faster speeds already."
- A hardware network manager working in government explained the importance of the improved reporting capabilities on their organization like this: "We undergo a cybersecurity framework assessment every year, and patching and vulnerability management is one of the most important areas of the assessment. Windows Autopatch gives us the ability to document and prove that our patching is up to date. We can see it running in the dashboard, we know it's working, and — if we want — we can set up an automated report and push it to the assessment team."

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Prior to enrolling in Windows Autopatch, the composite organization spent 40 hours per month on reporting activities related to patching.
- Windows Autopatch improves reporting capabilities, and this reduces reporting work for the IT team by between 20% and 80%, depending on the tools and configuration used in the prior patching process.
- Members of the IT patching team are paid $65 per hour.

Results. This yields a three-year projected PV ranging from $15,600 (low) to $62,000 (high).

Reporting And Compliance Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Hours dedicated to ad hoc reporting requests and compliance reporting regarding updates/patches (monthly)	Composite	40	40	40
$B2_{Low}$			20%	20%	20%
$B2_{Mid}$	IT reporting efficiency gains	Composite	50%	50%	50%
$B2_{High}$			80%	80%	80%
B3	Hourly salary for patching team member	A3/2,080	$65	$65	$65
Bt_{Low}			$6,240	$6,240	$6,240
Bt_{Mid}	Reporting and compliance efficiency	B1*12*B2*B3	$15,600	$15,600	$15,600
Bt_{High}			$24,960	$24,960	$24,960
	Three-year projected total: $18,720 to $74,880			**Three-year projected present value: $15,518 to $62,072**	

IMPROVED PATCH SUCCESS RATE

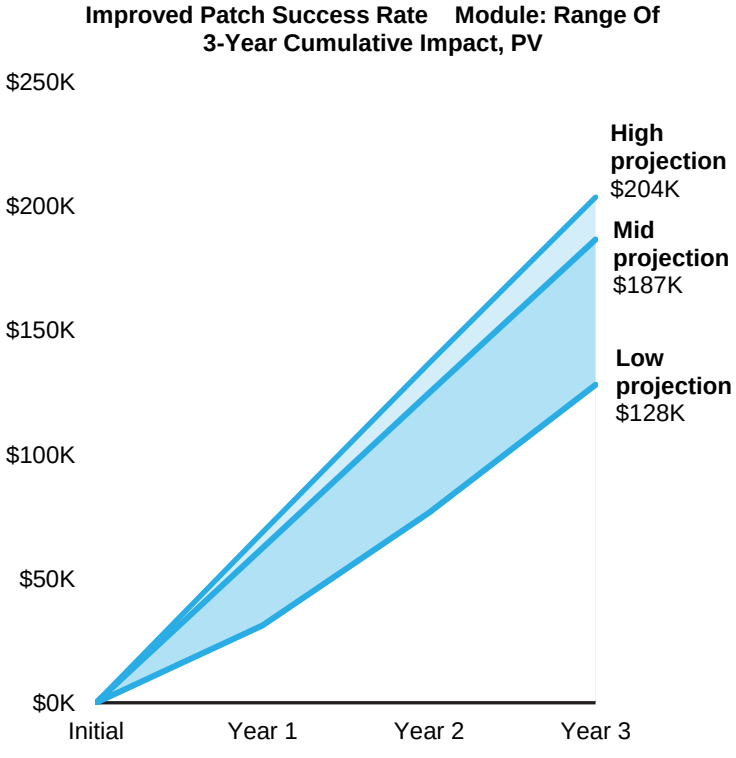
Evidence and data. Interviewees said that with Windows Autopatch, their organizations achieved higher patch success rates in less time and with less effort from IT teams as compared to with their prior solutions. This reduced vulnerabilities and improved security postures.

- Each interviewee said their organization was looking to improve its monthly patch success rate with Windows Autopatch, and all reported an increase in the number of overall patched devices after enrolling. A manager of computing solutions in the chemicals industry said: "We want to make sure that we are hitting full compliance each month, and we want to be able to get this stuff out as quickly as we can. [Windows] Autopatch gives us that visibility and the reliability of getting better patch results than we've had before."
- While improving patch success rates is crucial for security, it also has a benefit to end users: Fewer patching issues means fewer end users are impacted by IT teams trying to remediate issues, and fewer end user issues translates to a reduction in help desk tickets related to patches and updates.
- Additionally, with the improved efficiency for feature updates, interviewees reported that end users can take advantage of new features sooner than they did previously could. In some cases, feature updates had been stalled for more than 12 months, so those organizations were excited to be able to finally let their workforces leverage the latest and greatest tools, integrations, and updates from Microsoft.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- In its prior state, the composite organization achieved a consistent 85% patch rate after four weeks.
- With Windows Autopatch, the composite organization improves its monthly patch success rate to between 95% and 98% after three years. Some interviewees said their organizations were limited by the use of very old or unsupported technology, which capped the patch success rate until those devices are either replaced or decommissioned.
- When errors do occur during the composite's patching process, only 10% of those errors impact end users.
- Each error that impacts an end user causes 3 hours of downtime for that end user while the composite's IT team remediates the patch.
- The average fully burdened hourly salary for an employee at the composite organization is $32.
- Half of the errors that impact end users generate a help desk ticket, and each ticket costs $15.

Results. This yields a three-year projected PV ranging from $128,000 (low) to $204,000 (high).



Improved Patch Compliance Rate

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average monthly path success prior to enrolling in Windows Autopatch	Interviews	85%	85%	85%
$C2_{Low}$			90%	93%	95%
$C2_{Mid}$	Average monthly patch success rate with Windows Autopatch	Interviews	95%	96%	97%
$C2_{High}$			96%	97%	98%
C3	Number of Windows endpoints	Composite	8,000	8,000	8,000
C4	Percent of errors that impact end users	Interviews	10%	10%	10%
$C5_{Low}$			40	64	80
$C5_{Mid}$	Reduction in errors that impact end users (monthly)	(C2-C1)*C3*C4	80	88	96
$C5_{High}$			88	96	104
C6	End-user downtime associated with update errors (hours)	Interviews	3	3	3
C7	Average hourly rate of employee	TEI standard	$32	$32	$32
$C8_{Low}$			$46,080	$73,728	$92,160
$C8_{Mid}$	Subtotal: End-user impact reduction	C5*C6*C7*12	$92,160	$101,376	$110,592
$C8_{High}$			$101,376	$110,592	$119,808
C9	Cost per help desk ticket	Composite	$15	$15	$15
$C10_{Low}$			20	32	40
$C10_{Mid}$	Reduction in help desk tickets (monthly)	C5*50%	40	44	48
$C10_{High}$			44	48	52
$C11_{Low}$			$3,600	$5,760	$7,200
$C11_{Mid}$	Subtotal: Reduced help desk tickets	C9*C10*12	$7,200	$7,920	$8,640
$C11_{High}$			$7,920	$8,640	$9,360
Ct_{Low}			$49,680	$79,488	$99,360
Ct_{Mid}	Improved patch success rate	C8 + C11	$99,360	$109,296	$119,232
Ct_{High}			$109,296	$119,232	$129,168
	Three-year projected total: $157,872 to $247,104		**Three-year projected present value: $128,152 to $203,754**		

REDUCED AND AVOIDED COSTS

Evidence and data. Interviewees said that after implementing Windows Autopatch, their organizations were able to retire prior solutions and infrastructure to different extents. In some cases, the organization completely eliminated prior solutions and infrastructure, but in other cases, the organization kept some prior infrastructure and tools in use for alternate use cases.

- Interviewees said that prior to leveraging Windows Autopatch, their organizations primarily leveraged Microsoft Configuration Manager on-premises for their monthly quality and feature updates. Some of the organizations had additional third-party tools they could fully or partially decommission once they successfully had Windows Autopatch up and running.

  A CISO and chief data protection officer for a digital services company said, “We are paying a significant amount for our prior solution, and 90% of the cost is related to patching. With Windows Autopatch, I only need licenses for the remaining 10%. So, there will potentially be significant cost savings. We are already looking at retiring [Microsoft Configuration Manager] and other tools, so are expecting to see cost savings there, too.”

- Interviewees said that with Windows Autopatch, their organizations could remove some on-premises infrastructure associated with prior endpoint management software like Microsoft Configuration Manager, and they reduced or eliminated any third-party applications that aided in patching Windows devices. Interviewees noted that the device management capabilites with Intune met their organizations’ needs and, in some cases, it allowed them to fully sunset on-premises Microsoft Configuration Manager.

- Interviewees from organizations that leveraged Intune typically said they saw less cost savings because the firms were less reliant on on-premises infrastructure and third-party tools to manage their Windows devices.

- Other than the license cost of third-party patching solutions, interviewees said management and maintenance of the prior tools also added costs, while not necessarily creating additional value. An IT enterprise architect and head of global deployment services in the pharmaceutical industry mentioned, “There [are costs] associated with those tools, including [for] licensing and maintenance, which would all be considered cost [savings] when we decommission.”

- Some interviewees said their organization is intent on removing on-premises infrastructure related to Microsoft Configuration Manager but that their firm still relies on it to patch certain pieces of its infrastructure (e.g., server operating systems). So, while they may not experience immediate cost savings, these organizations should rely less on on-premises infrastructure.

Modeling and assumptions. Forrester assumes the following about the composite organization:

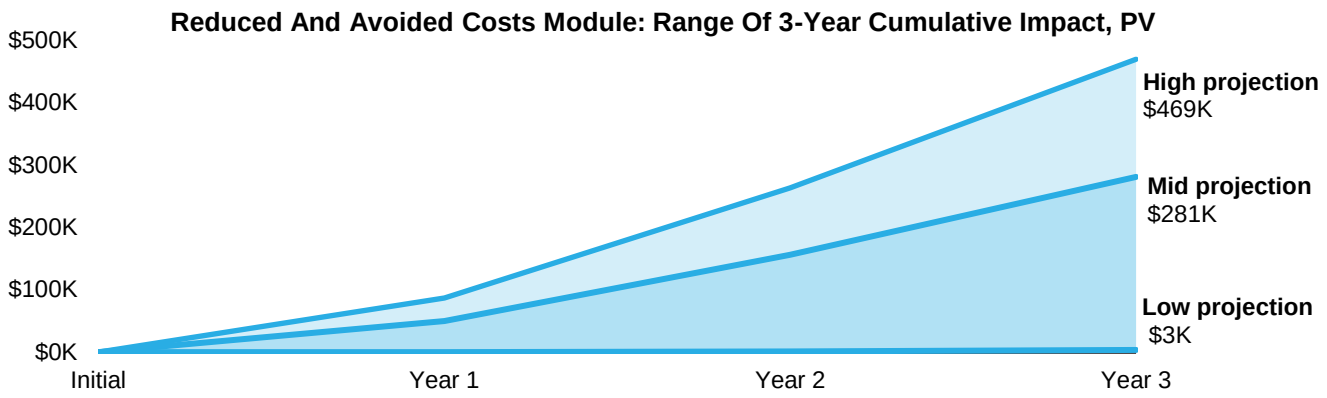
- The composite dedicates 25 on-premises servers to Microsoft System Center Configuration Manager (Microsoft SCCM), and each costs $1,000 per year in maintenance and service.

- Windows Autopatch allows the composite organization to remove between 20% and 100% of its on-premises infrastructure by reducing or eliminating reliance on Microsoft SCCM.

- The composite pays $0 to $60 per user per year for third-party tools that aid in patching.

- With Windows Autopatch, the composite expects to reduce reliance on third-party tools by 30% in Year 1 and that this reduction reaches 90% in Year 3 when the deployment is more mature.

Results. This yields a three-year projected PV ranging from $3,000 (low) to $469,000 (high).



Reduced And Avoided Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	On-premises servers dedicated to prior update process	Composite	25	25	25
$D2_{Low}$			0%	10%	20%
$D2_{Mid}$	Reduction in on-premises infrastructure	Composite	20%	50%	70%
$D2_{High}$			60%	80%	100%
D3	Average cost of maintenance and service per server	Composite	$1,000	$1,000	$1,000
$D4_{Low}$			$0	$2,500	$5,000
$D4_{Mid}$	Subtotal: Hardware/infrastructure savings	D1*D2*D3	$5,000	$12,500	$17,500
$D4_{High}$			$15,000	$20,000	$25,000
$D5_{Low}$			$0	$0	$0
$D5_{Mid}$	Third-party costs related to update/patching (e.g., software/tools, managed service provider)	Composite	$36	$36	$36
$D5_{High}$			$60	$60	$60
D6	Reduction in third-party costs with Windows Autopatch	Interviews	30%	70%	90%
$D7_{Low}$			$0	$0	$0
$D7_{Mid}$	Subtotal: Third-party savings	C3*D5*D6	$86,400	$201,600	$259,200
$D7_{High}$			$144,000	$336,000	$432,000
D8	Attribution to Windows Autopatch	Composite	60%	60%	60%
Dt_{Low}			$0	$1,500	$3,000
Dt_{Mid}	Reduced and avoided costs	(D4+D7)*D8	$54,840	$128,460	$166,020
Dt_{High}			$95,400	$213,600	$274,200
	Three-year projected total: $4,500 to $583,200		**Three-year projected present value: $3,494 to $469,267**		

UNQUANTIFIED BENEFITS

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

- **Improved security posture.** Interviewees said Windows Autopatch helps protect their organizations against possible vulnerabilities by regularly applying Windows quality updates to endpoints and that Windows Autopatch greatly reduces the number of vulnerabilities at any given time. An IT enterprise architect and head of global deployment services in the pharmaceutical industry stated: "[Windows Autopatch is essential to] ensuring [our] devices [are] protected, up to date, and [that] all the vulnerabilities identified and addressed [are] part of the Zero Trust network architecture we're trying to implement."
- **Shift in decision-making for patching to Microsoft.** Interviewees said their organizations have been able to defer the management of their patching and compliance processes to Microsoft. This greatly reduced pressure on IT teams and decision-makers and let them increase focus on improving business and other tasks that would be neglected due to limited resources. An IT enterprise architect and head of global deployment services in the pharmaceutical industry said, "What attracted me to [Windows] Autopatch was the management from the Microsoft side [and] having that set of people from Microsoft monitoring it and watching over it."

"By making sure that our software is current, there are fewer vulnerabilities and threats for those devices. It reduces that security gap for us."

CISO and chief data protection officer, digital services

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Windows Autopatch and later realize additional uses and business opportunities, including:

- **Significant additional patching-team efficiency gains due to support for OS upgrades, additional Microsoft products, and support for third-party applications.** Interviewees said they are excited about the prospect of using Windows Autopatch for upgrading from Windows 10 to Windows 11, and they said that once possible with Windows Autopatch, this will save their organizations significant amounts of time and effort. They also said including more Microsoft or Windows products would expand use cases and generate additional efficiency.
- **Improved visibility and response time for security teams.** As the interviewees' organizations get more comfortable using Windows Autopatch and explore its visibility and reporting capabilities, security teams can take advantage of the data Autopatch collects and reports to ensure vulnerabilities are properly patched and managed. They can also use data and reporting to aid in investigations and compliance audits.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	Ongoing costs	$141,750	$35,438	$35,438	$35,438	$248,063	$229,878
	Total costs (risk adjusted)	$141,750	$35,438	$35,438	$35,438	$248,063	$229,878

ONGOING COSTS

Evidence and data. Windows Autopatch is included with Windows E3 and E5 licenses, and there are no fees or other costs associated with enrolling eligible devices. Interviewees said Windows Autopatch generated more value from their organizations' Microsoft investments, and they highlighted the benefits of Windows Autopatch when discussing the overall value of their Microsoft licenses.

- A program manager for cloud platform in the manufacturing industry explained: "We have the right license, so we view Windows Autopatch as a service that Microsoft added to the portfolio that we could easily start to use. We enrolled our devices and saw the benefits from it right away."
- Interviewees reported that there are no out-of-pocket costs associated with enrolling or running Windows Autopatch and that patching teams were able to easily adopt the service.
- Some interviewees said their organizations found that some old or out-of-compliance devices were not eligible for enrollment. These organizations either upgraded the devices as part of their regular lifecycles or updated their OS so the devices became eligible. Interviewees did not report these device updates and upgrades as additional costs because their organizations would have needed them with or without Windows Autopatch.
- Interviewees said that once their organizations were fully enrolled, IT technicians responsible for managing multiple tools and platforms within their environments managed Windows Autopatch.
- Typically, they dedicated one FTE to planning and executing the Windows Autopatch pilot and deployment during the initial period. This FTE would help develop workflows, communication plans, and best practices.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization holds a Windows E3 license for all employees.
- The fully burdened annual salary for an IT technician is $135,000.
- One FTE is responsible for the composite's initial planning and deployment.
- An IT technician who manages many other tools will spend 25% of their time managing Windows Autopatch once it's deployed.
- Costs may vary. Contact Microsoft for additional details.

Risks. This cost may vary due to the speed and success of the organization's initial deployment and its enrollment efforts.

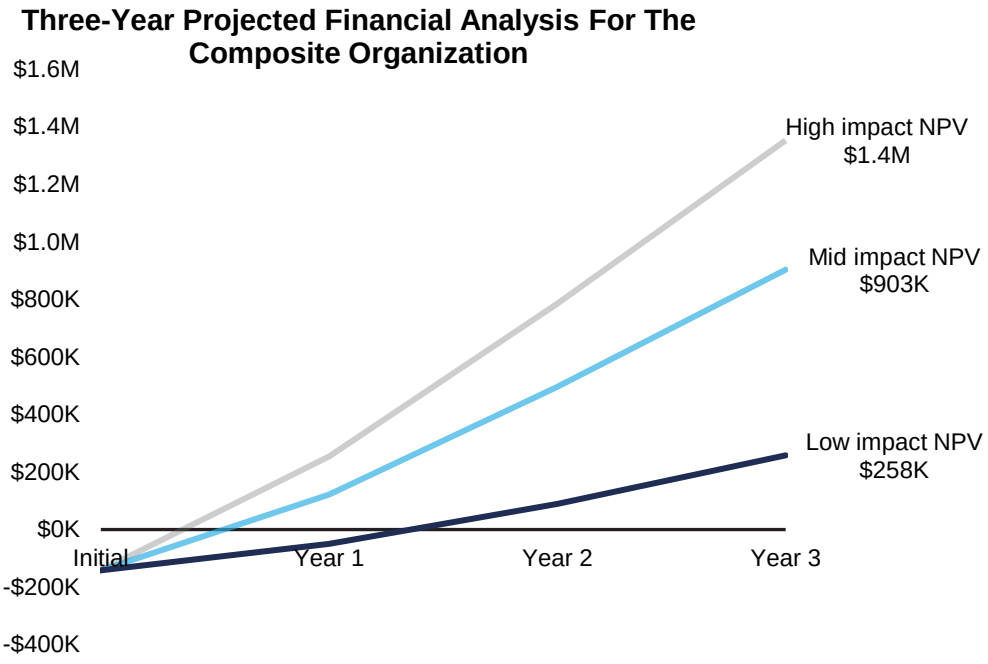
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $230,000.

Ongoing costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	FTEs needed to run/monitor Windows Autopatch	Interviews	1.0	0.25	0.25	0.25
E2	Salary of FTE	TEI standard	$135,000	$135,000	$135,000	$135,000
Et	Ongoing costs	E1*E2	$135,000	$33,750	$33,750	$33,750
	Risk adjustment	↑5%				
Etr	Ongoing costs (risk-adjusted)		$141,750	$35,438	$35,438	$35,438
	Three-year total: $248,063			**Three-year present value: $229,878**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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

These risk-adjusted PROI and projected NPV values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($141,750)	($35,438)	($35,438)	($35,438)	($248,063)	($229,878)
Total benefits (low)	$0	$137,137	$203,623	$259,351	$600,111	$487,808
Total benefits (mid)	$0	$324,445	$489,824	$576,695	$1,390,964	$1,133,042
Total benefits (high)	$0	$470,018	$679,976	$789,887	$1,939,881	$1,582,707
Net benefits (low)	($141,750)	$101,699	$168,186	$223,914	$352,049	$257,930
Net benefits (mid)	($141,750)	$289,008	$454,386	$541,257	$1,142,901	$903,164
Net benefits (high)	($141,750)	$434,580	$644,539	$754,450	$1,691,819	$1,352,829

Appendix A: New Technology: Projected Total Economic Impact

New Technology: Projected Total Economic Impact (New Tech TEI) is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value of their products and services to clients. The New Tech TEI methodology helps companies demonstrate and justify the projected tangible value of IT initiatives to senior management and key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

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

Projected Costs consider all expenses necessary to deliver the proposed value of the product. The projected cost category within New Tech TEI captures incremental ongoing costs over the existing environment that are 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.

PROJECTED NET PRESENT VALUE (PNPV)

The projected 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.

PROJECTED RETURN ON INVESTMENT (PROI)

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%.

Appendix B: Supplemental Material

Related Forrester Research

"The Future Of Endpoint Management," Forrester Research, Inc., June 6, 2022

"How To Manage Your Vulnerability Risk Program Amidst Skill And Labor Shortages," Forrester Research, Inc., October 28, 2022

"The Infrastructure Automation Landscape, Q4 2022," Forrester Research, Inc., December 22, 2022

"Boost Your Security Technology Stack," Forrester Research, Inc., February 15, 2022

"Top Cybersecurity Threats In 2022," Forrester Research, Inc., April 8, 2022

"How To Strengthen Vulnerability Risk Management With Remediation Prioritization," Forrester Research, Inc., December 21, 2022

Online Resources

"Windows Autopatch Prerequisites," Microsoft, Feb. 17, 2023

Appendix C: Endnotes

[1] Source: Forrester's Security Survey, 2022.

[2] 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.

[3] Source: Forrester's Security Survey, 2022.


FORRESTER®