FORRESTER®

The Total Economic Impact™ Of Tanium Converged Endpoint Management (XEM)

Cost Savings And Business Benefits Enabled By Tanium XEM

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY TANIUM, JANUARY 2024

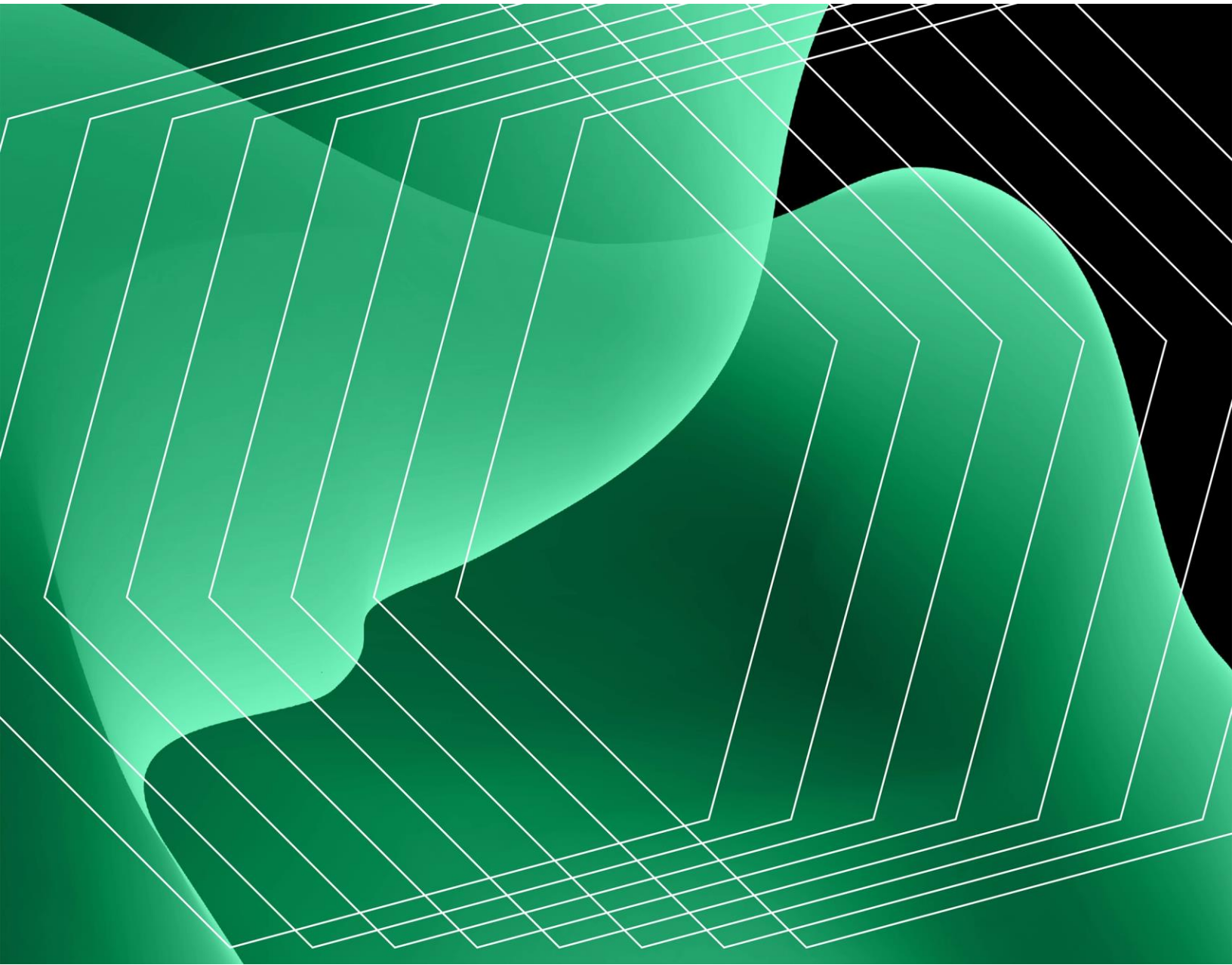


Table Of Contents

Executive Summary	3
The Tanium XEM Customer Journey	9
Analysis Of Benefits	14
Analysis Of Costs	28
Financial Summary	33

Consulting Team:

Nikoletta Stergiou

Adam Birnberg

ABOUT FORRESTER CONSULTING

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

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

Security and IT pros are struggling to keep pace with an expanding attack surface. Hybrid work, the rise of bring-your-own-device, rampant cloud adoption, and a continued interest in the internet of things (IoT) is making vulnerability and patch management more difficult than ever.[1] Tanium aims to help organizations overcome this challenge through its XEM platform approach, which provides organizations with real-time visibility and control of their endpoint environment, while maintaining security controls and performance.

The Tanium XEM platform identifies, prioritizes, and remediates IT and security issues in real time from a single console. IT and security teams are enabled to control all endpoints in their environment through streamlined workflows, increased efficiency, and reduced complexities through the displacement of multiple point solutions. Furthermore, organizations can track and reduce their endpoint risk over time, reclaim unused software assets, and reduce the likelihood of a breach or fine.

Tanium commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Tanium XEM Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Tanium XEM on their organizations.[2]

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with experience using Tanium XEM. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results of organizations ranging from 2,200 to 140,000 endpoints into a single composite organization, which has 40,000 employees and 48,000 endpoints.

KEY STATISTICS

Return on investment (ROI)
228%

Net present value
$12.57M

Payback
<6 months

Benefits PV
$18.07M

Interviewees said that prior to using Tanium XEM, their organizations had multiple complex and decentralized solutions along with manual processes throughout their endpoint management workflows. However, prior attempts to manage their endpoint environment yielded limited success, restricting visibility into their endpoint environment and security vulnerabilities. These limitations led to high costs in software licensing and tools, overworked FTEs, security incidents or breaches, agent bloat that reduced device performance, and time-consuming data reconciliations across disjointed tools.

After deploying Tanium XEM, the interviewees were able to automate and centralize their endpoint management processes. Key results from the investment include software reclamation savings, endpoint management efficiency savings, risk mitigation cost avoidance, and tool consolidation savings.

KEY FINDINGS

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

- **Successful reclamation of unused, rarely-used or unauthorized software titles with Tanium XEM on 90% of endpoints.** Across 48,000 endpoints in the composite organization, 20% have reclaimable software. Tanium XEM enables the successful reclamation of these licenses through the solution's comprehensive visibility and control over endpoints. Over

three years, reclamation savings with Tanium XEM are worth more than $4.8 million.

- **Increased endpoint management efficiency by 60%.** The composite organization realizes efficiencies enabled by Tanium XEM on its endpoint management team by automating activities like software deployment, patching, and security assessments. Efficiencies scale over time as users increasingly utilize Tanium XEM, resulting in 60% efficiencies gained by the end of Year 3. Over three years, endpoint management efficiency savings are worth more than $1 million.
- **Reduced software vulnerabilities by 97% through improved patching.** The composite organization improves its security posture with Tanium XEM by automating patch deployment, assessing vulnerabilities, and leveraging real-time data. Improvements in OS and third-party software patching with Tanium lead to a 97% reduction in software vulnerabilities. Over three years, risk mitigation cost avoidance is worth more than $7.9 million.
- **Improved endpoint management and security tool consolidation by 70%.** Tanium XEM's platform approach and comprehensive coverage (across a range of Use Cases, such as asset management, compliance management, incident response, patch management, threat protection, and data discovery) consolidates endpoint management and security tools. Over three years, tool consolidation savings are worth more than $4.1 million.

Reduction in software vulnerabilities with Tanium patching

97%

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

- **M&A efficiency and cost savings.** Tanium XEM's capabilities enable organizations to fully understand and integrate endpoint environments after an acquisition. Tanium XEM improves the efficiency of M&A IT integration activities by 70% and avoids technical debt by identifying redundant solutions.
- **Unique technical account manager (TAM).** Tanium's unique support model, included in the price of the software, enables organizations to optimize the platform and take advantage of its full capabilities. The Tanium TAM builds a bridge between an organization and the vendor to ensure success with the platform.

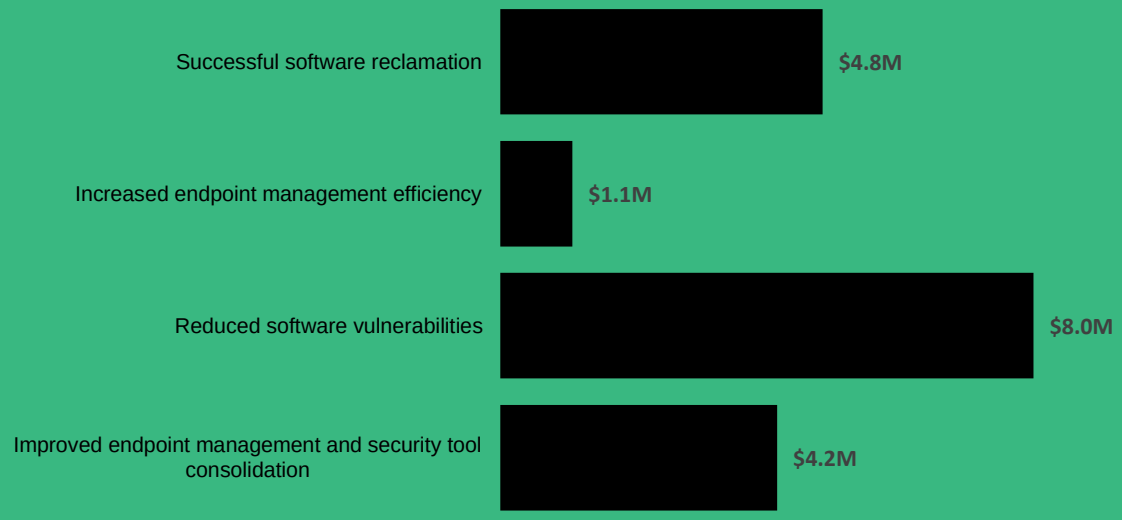
Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Licensing.** Licensing is based on the Core tier and additional solutions that cover areas such as asset management, compliance management, incident response, patch management, threat protection, and data discovery. Pricing is based on the number of endpoints.
- **Internal implementation and training.** Internal implementation and training costs include several months spent by two FTEs from the endpoint management team to fully deploy the solution. There are 30 users who spend 8 hours each on training. Organizations implementing a cloud-based installation may find the installation time significantly reduced.
- **Internal ongoing management.** The composite organization has two FTEs dedicating 50% of their time toward the ongoing management of the Tanium XEM on-prem solution. While some organizations deployed Tanium XEM on-prem, other organizations may deploy it as a cloud-based solution. This would reduce overall ongoing support costs.

The representative interviews and financial analysis found that the composite organization experiences benefits of $18.07 million over three years versus costs of $5.5 million, adding up to a net present value (NPV) of $12.57 million and an ROI of 228%.

ROI	BENEFITS PV	NPV	PAYBACK
228%	**$18.07M**	**$12.57M**	**<6 months**

Benefits (Three-Year)



"Tanium XEM has positive command and control over your entire enterprise. You have all sorts of different operating systems, environments, regional pieces, and political shenanigans that will stand in your way of being able to have full command and control over your entire enterprise. Tanium XEM solves that problem in a way that no other vendor really does."

CYBER PRINCIPAL, INSURANCE

TEI Framework And Methodology

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment Tanium XEM.

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 Tanium XEM can have on an organization.

1. **Due Dilligence**
   Interviewed Tanium stakeholders and Forrester analysts to gather data relative to XEM.
2. **Interviews**
   Interviewed five representatives at organizations using XEM to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **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 interviewees.
5. **Case Study**
   Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Tanium 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 and an ROI calculator powered by Forrester available through Tanium to determine the appropriateness of an investment in Tanium XEM.

Tanium 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.

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

The Tanium XEM Customer Journey

Drivers leading to the XEM investment

Interviews				
Role	**Industry**	**Region**	**Average annual revenue (USD) and number of employees**	**Number of endpoints**
Head of enterprise IT and information technology	Retail	Headquartered in the UK, global operations	$6.8 billion 45,000 employees	17,000
Vice president	Banking	Headquartered in the US, global operations	$34.9 billion 77,000 employees	140,000
Cyber principal	Insurance	Headquartered in Canada, global operations	$12.4 billion 40,000 employees	75,000 to 80,000
Lead cyber security engineer	Insurance	Headquartered in the US	$35 billion 26,700 employees	40,000
Vice president and CISO of information technology	Healthcare	Headquartered in the US	$400 million 5,000 employees	2,200

Key Challenges

Interviewees highlighted several challenges in their environment before Tanium, including limited visibility, manual processes, security and compliance vulnerabilities, and technical debt. Complex and decentralized legacy solutions limited endpoint visibility, posing challenges in enforcing consistent security measures and effectively managing endpoints across the organization's network. This led to vulnerabilities, the potential for security breaches, and difficulties in troubleshooting. In some cases, interviewees noted their organization had manual endpoint management processes that were inefficient and time-consuming, as team members had to physically check and patch devices.

As a result of inefficient legacy solutions and processes, interviewees described poor cyber hygiene that left their organization exposed to potential security incidents and breaches — emphasizing the importance of effective endpoint management to reduce the likelihood of such breaches. For interviewees whose organizations were involved in M&A activity, technical debt hindered their

adaptability and maintenance, leading to costly integrations and potential vulnerabilities.

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

- **Limited endpoint visibility.** Interviewees highlighted limited endpoint visibility despite multiple solutions — this made it difficult to enforce consistent security measures and manage endpoints across the organization's network effectively. Thus, their organizations were exposed to vulnerabilities, potential security breaches, and faced difficulties in troubleshooting and resolving issues. The lead cybersecurity engineer at an insurance company noted: "In our prior environment, there was a lack of EDR [endpoint detection and response] visibility in all the endpoints. Most server folks had no knowledge of what Tanium XEM was essentially doing, but here we are collecting data from endpoints and our security team was able to utilize that information from improved visibility."
- Furthermore, the cyberinsurance principal at an insurance company described the impact that decentralized solutions can have on a large organization, "Our company, like many global companies, suffers from a problem around specifically large amounts of distribution and different ways things are done in different countries, locales, and regions for our IT."
- **Inefficient manual processes.** Some interviewees said their organization's manual processes in endpoint management were time-consuming for endpoint management team members. Without automated approaches, interviewees described the continuous efforts in checking software across different devices. The vice president and CISO of information technology at a healthcare company noted: "It's immeasurable because too much time was spent on endpoint management. Imagine you have a team of 10 people who are in the field and updating machines. They're not as thorough to check what software they should need, so it was just a never-ending hamster wheel."
- **Security and compliance vulnerabilities.** Interviewees highlighted poor cyber hygiene with patching in legacy solutions and processes, which exposed them to a range of potential security incidents. They highlighted

that avoiding breaches was top of mind as it related to endpoint management and risk reduction — the costly impact and reputational damage from a security incident or breach can be immeasurable. The vice president and CISO of information technology at a healthcare company noted, “The company suffered a breach and that’s part of why I got hired — to ensure that it doesn’t, or try their best to make sure it doesn’t, happen again and see what state they’re in.”

- **Technical debt from M&A activity.** Interviewees discussed the impact of technical debt from their organization’s M&A activity as it hindered their organization’s ability to adapt, scale, and maintain its environment effectively. This led to costly integrations and potential vulnerabilities through system downtime. The head of enterprise IT and information security at a retail organization noted: “Tanium XEM helped us avoid inheriting technical debt. In one of our most recent acquisitions, we haven’t had to bring some of the technologies over because we’ve got better technology that was in place prior to us acquiring them.”

Investment Objectives

The interviewees’ organizations searched for a solution that could:

- Improve their organization’s security posture.
- Improve endpoint visibility.
- Improve efficiency through automated processes.
- Centralize and consolidate solutions.

> “The speed and efficiency at which Tanium operates allow our security teams, our endpoint management teams, and IT teams in general to be able to collect information and gain visibility quicker than any other solution we’ve had in the organization, which extends to efficiencies across the board.”
>
> LEAD CYBERSECURITY ENGINEER, INSURANCE

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 five interviewees, and it is used to present the aggregate financial analysis in the next section. Other organizations may deploy Tanium XEM as a cloud-based solution and with other characteristics that may impact benefits and costs. The composite organization has the following characteristics:

Description of composite. The composite organization is headquartered in the United States and has global operations. It has 40,000 employees and 48,000 endpoints. On average, the composite has one acquisition per year.

Deployment characteristics. The composite organization seeks a solution for endpoint management and security to gain visibility, control, and protection over endpoints. It deploys Tanium XEM as an on-premises solution. The organization invests in the Core X1 tier which includes Tanium Core and the Asset, Discover, and Benchmark modules. It also chooses to add solutions including Endpoint Management (Provision, Patch, and Deploy modules), Risk & Compliance

(Comply, Integrity Monitor, Reveal modules), and Incident Response (Threat Response and Impact modules).

KEY ASSUMPTIONS

40,000 employees

48,000 endpoints

One acquisition per year

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Successful software reclamation	$1,944,000	$1,944,000	$1,944,000	$5,832,000	$4,834,440
Btr	Increased endpoint management efficiency	$224,640	$449,280	$673,920	$1,347,840	$1,081,850
Ctr	Reduced software vulnerabilities	$3,216,638	$3,216,638	$3,216,638	$9,649,915	$7,999,303
Dtr	Improved endpoint management and security tool consolidation	$1,406,250	$1,687,500	$1,968,750	$5,062,500	$4,152,188
	Total benefits (risk-adjusted)	$6,791,528	$7,297,418	$7,803,308	$21,892,255	$18,067,781

Successful Software Reclamation

Evidence and data. Interviewees described the impact that Tanium XEM had on software reclamation through the solution's comprehensive visibility and control over endpoints. With Tanium XEM, interviewees could identify and assess unused, underutilized, and unauthorized software on endpoints, allowing for effective reclamation efforts. They noted how Tanium XEM's endpoint management capabilities enabled their teams to remotely uninstall software, which ensured that licenses were efficiently reclaimed and reduced software costs.

- The cyber principal at an insurance company commented on Tanium XEM's ability to provide greater detail in discovery than other solutions: "We use Tanium Discover specifically because it goes to a much higher level of discovery than a lot of other tools. It utilizes N-map scanning from the agent and it's efficient. It doesn't cause a lot of network consternation when it occurs."

- The head of enterprise IT and information security at a retail organization shared a use case example of removing software to prepare for an audit: “We’re able to use Tanium’s Asset module to tell us everywhere in the environment where [software] was installed and billable. We were able to use Tanium XEM to find those systems, find that software, get it removed and show it as evidence back to auditors that the software is no longer in the environment.”
- The lead cybersecurity engineer at an insurance company highlighted how Tanium XEM had also been used on some occasions to reclaim hardware: “We found instances where systems were set to retire in our CMDB [configuration management database], and we used Tanium XEM to find that they actually weren’t retired or retired incorrectly and are still active.”

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- There are 48,000 endpoints.
- Twenty percent of these endpoints have reclaimable software.
- With Tanium XEM, 90% of the software titles on endpoints with reclaimable software are successfully reclaimed.
- The average reclamation value of software on each endpoint is $250.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of endpoints.
- Percentage of endpoints with reclaimable software.
- Reclamation value per endpoint.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.83 million.

Endpoints successfully reclaimed with Tanium XEM

90%

"When I first implemented Tanium XEM at another company, we had 4,000 endpoints. In three minutes, I was able to tell my CTO how many endpoints were compromised, and in the next two minutes, I remediated them."

VICE PRESIDENT AND CISO OF INFORMATION TECHNOLOGY, HEALTHCARE

Successful Software Reclamation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of endpoint devices	Composite	48,000	48,000	48,000
A2	Percent of endpoints with reclaimable software	Composite	20%	20%	20%
A3	Percent of endpoints successfully reclaimed with Tanium	Interviews	90%	90%	90%
A4	Average reclamation value per endpoint	Composite	$250	$250	$250
At	Successful software reclamation	A1*A2*A3*A4	$2,160,000	$2,160,000	$2,160,000
	Risk adjustment	↓10%			
Atr	Successful software reclamation (risk-adjusted)		$1,944,000	$1,944,000	$1,944,000
	Three-year total: $5,832,000			**Three-year present value: $4,834,440**	

Increased Endpoint Management Efficiency

Evidence and data. Interviewees described the impact of automation and real-time data with Tanium XEM to increase efficiencies across endpoint management. With Tanium XEM, they could save on hiring multiple FTEs dedicated toward endpoint management activities such as software deployment, patching, and security assessments.

- The lead cybersecurity engineer at an insurance company highlighted the efficiencies in real-time data with Tanium XEM: “Tanium skyrockets above other solutions. With other point solutions, I have to tell the server, ‘Hey, go get me this information from all the endpoints.’ I may have to wait a day or two before that information comes back after it is collected by the endpoint and sent back to the server. With Tanium, I can get it in 10 seconds.”
- The vice president and CISO of information technology at a healthcare organization commented on Tanium XEM’s quick patching capabilities which impacted the workforce needed for endpoint management: “Tanium allows me to manage endpoints without hiring 10 people. I set it up so I can see what’s in my environment. Get it up to the right version, patch it quickly, and train someone who’s never used it before to then be an expert in just pushing out code to do the things to clean up.”
- The lead cybersecurity engineer at an insurance company shared the impact that Tanium has had across different departments in their organization: “We reduced staffing across multiple parts of the corporation — not just our server teams and workstation teams but also [potentially] our security teams and our DevOps teams by 20% to 30% across the platforms.”

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- There are 10 endpoint management FTEs.
- With Tanium XEM, there is a 20% efficiency improvement in Year 1, 40% in Year 2, and 60% in Year 3.

- The average fully burdened annual salary of an endpoint management FTE is $156,000.
- Forrester assumes an 80% productivity recapture to account for an improved work life balance.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of endpoint management FTEs.
- Average fully burdened annual salary of an endpoint management FTE.
- Productivity recapture.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.08 million.

Efficiency improvement with Tanium by Year 3

60%

"Comparable organizations are probably twice the size of what we are. We've really been able to keep a strong lean team. I'd say we've been able to save around five FTEs with Tanium."

HEAD OF ENTERPRISE IT AND INFORMATION SECURITY, RETAIL

Increased Endpoint Management Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of endpoint management FTEs	Composite	10	10	10
B2	Percent efficiency improvement with Tanium	Interviews	20%	40%	60%
B3	Average endpoint management FTE fully burdened annual salary	Composite	$156,000	$156,000	$156,000
B4	Productivity recapture	Composite	80%	80%	80%
Bt	Increased endpoint management efficiency	B1*B2*B3*B4	$249,600	$499,200	$748,800
	Risk adjustment	↓10%			
Btr	Increased endpoint management efficiency (risk-adjusted)		$224,640	$449,280	$673,920
	Three-year total: $1,347,840			**Three-year present value: $1,081,850**	

Reduced Software Vulnerabilities

Evidence and data. Interviewees highlighted how Tanium XEM's patch management and software deployment capabilities mitigated risk and improved their organization's overall security posture by automating patch deployment, assessing vulnerabilities, and providing real-time data. Patch management included fixing underlying operating system vulnerabilities while software deployment capabilities fixed, installed, or removed third-party software. Interviewees described the effectiveness of patching with Tanium XEM, which ensured endpoints were protected with the latest patches. Ultimately, the improvement in OS and third-party software reduced the risk of potential security incidents and/or breaches.

- The cyber principal at an insurance company noted the impact that Tanium XEM's visibility and quick response had on resolving zero-day vulnerabilities: "It's about the visibility and the ability to respond to things and increasing efficiency to do it. Tanium's whole motto is like, 'we give you the ability to ask any question you want and get it back very quickly. Not only do we offer you the ability to do that, it's the opportunity to resolve whatever that problem is.' That could be from a patch context, a zero-day vulnerability context, or an enforcement or compliance mechanism."

- The vice president at a bank shared an incident in which Tanium XEM stopped a malformed software update from updating on thousands of servers: “We needed to stop a service on 20,000 servers. So how do you stop a service on 20,000 servers without a tool like Tanium XEM? You could do it with another point solution, but you’re scripting it and you’re having to identify all the computer names you don’t retain. But if you talk about a 20-minute turnaround to have any given service on the entire infrastructure turned off, I don’t know of another tool that can do that.”
- The vice president and CISO of information technology at a healthcare company highlighted how Tanium played a critical role in risk mitigation management: “It enabled us to identify that our machines are subpar so we are upgrading them, and it will take this long. But in identifying the risk to the business in which you better quantify its uptime versus downtime, it allows us to pinpoint our energy and resources into the things that causes the downtime in the network, the Wi-Fi etc. Tanium XEM is that tool that helps us focus our energies in the right place to maximize the uptime and the continuity of the business.”

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- The average cost of a security breach for an organization of 40,000 employees is $2,167,400 per security breach, with an average of three security breaches per year.[3]
- Tanium XEM’s OS and third-party software patching reduces 97% of software vulnerabilities.[4]

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Average cost of a security breach.
- Frequency of security breaches.
- Percentage of security breaches caused by software vulnerabilities, weak or stolen credentials, and exploitation of lost/stolen assets.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $8 million.

Security breaches from software vulnerabilities, use of weak or stolen credentials, and exploitation of lost/stolen assets

60%

"When it comes to risk mitigation, Tanium is instrumental in being able to identify if there are endpoints in the environment that need remediation."

VICE PRESIDENT, BANKING

Reduced Software Vulnerabilities					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Cost of security breach	Forrester	$2,167,400	$2,167,400	$2,167,400
C2	Frequency of security breach (annual)	Forrester	3	3	3
C3	Percent of security breaches as a result of software vulnerabilities, use of weak or stolen credentials, and exploitation of lost/stolen assets	Forrester	60%	60%	60%
C4	Reduction in software vulnerabilities with Tanium patching	Interviews	97%	97%	97%
Ct	Reduced software vulnerabilities	C1*C2*C3*C4	$3,784,280	$3,784,280	$3,784,280
	Risk adjustment	↓15%			
Ctr	Reduced software vulnerabilities (risk-adjusted)		$3,216,638	$3,216,638	$3,216,638
	Three-year total: $9,649,915		**Three-year present value: $7,999,303**		

Improved Endpoint Management And Security Tool Consolidation

Evidence and data. Interviewees described cost savings for their organization related to the consolidation of various security and endpoint management tools in their prior environment. With Tanium XEM, some tools were completely eliminated as a result of Tanium XEM's comprehensive coverage in areas including asset management, compliance management, incident response, patch management, threat protection, and data discovery.

- The vice president of a bank described the replacement of a couple of security tools with Tanium XEM: "It was a one-to-one replacement. For Integrity Monitor, another point solution was being used only on a specific part of the population, but with Tanium XEM, we could cover the entire population. Threat Response was being served by another point solution which we replaced that functionality with Tanium XEM."
- The vice president and CISO of information technology at a healthcare organization highlighted the elimination of endpoint management point solutions: "We removed all AV [antivirus] products. One legacy solution was breached while on my watch. Luckily, we had Tanium XEM deployed — thus, we executed with the Tanium team to build packages so I could immediately remove that solution from my environment. I was able to do that in under two days."
- The head of enterprise IT and information security at a retail organization noted the displacement of several legacy solutions: "We've displaced legacy solutions related to remote desktop, the patch management side, and vulnerability management."

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- There were five legacy solutions in the environment before Tanium.
- The average licensing costs per legacy solution is $625,000 including supporting infrastructure and FTE labor to support the solutions.

- With Tanium XEM, 50% of legacy solutions are decommissioned in Year 1, 60% in Year 2, and 70% in Year 3.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of legacy solutions.
- Average cost of legacy solutions.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.15 million.

Legacy solutions decommissioned with Tanium by Year 3

70%

"Because of Tanium's one-agent architecture, you end up saving in resource utilization. Using fewer agents for specific tasks results in lower endpoint resource overhead. Having one agent reduces complexity and effort for in-house teams towards fixing multiple agents when they break."

VICE PRESIDENT, BANKING

Improved Endpoint Management And Security Tool Consolidation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of legacy solutions	Composite	5	5	5
D2	Average licensing cost per legacy solution	Composite	$625,000	$625,000	$625,000
D3	Percent of legacy solutions decommissioned with Tanium	Interviews	50%	60%	70%
Dt	Improved endpoint management and security tool consolidation	D1*D2*D3	$1,562,500	$1,875,000	$2,187,500
	Risk adjustment	↓10%			
Dtr	Improved endpoint management and security tool consolidation (risk-adjusted)		$1,406,250	$1,687,500	$1,968,750
	Three-year total: $5,062,500			**Three-year present value: $4,152,188**	

Unquantified Benefits

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

- **M&A efficiencies and cost savings.** Interviewees highlighted how Tanium XEM drove M&A efficiencies (e.g., integration) and helped them to manage / reduce technical debt — which led to overall time savings related to acquisitions and cost savings from eliminating technical debt. The head of enterprise IT and information security at a retail organization commented: “Installing Tanium has really enabled us to map out that environment and understand exactly what we bought as part of the acquisition. We can then look to ring-fence the environment and either move the data over, or if we see that there are parts of the environment we don’t want, we can just fully shut off.”
- **Unique technical account manager (TAM) model.** Interviewees highlighted the unique support provided by Tanium compared to other solutions to help accelerate value from their investment. The cyber principal at an insurance company noted: “We get a lot of support from our technical account team for anything and everything we’re trying to do. They are very passionate about their product and how they can support their customers with the capabilities that they have.”

Improvement in M&A efficiencies

70%

"We've been able to really reduce the amount of third parties that we use. They were [previously in a] heavily outsourced environment, but because of a tool like Tanium XEM, it's meant that we don't need that outsourced third party to monitor and detect certain vulnerabilities in that environment."

HEAD OF ENTERPRISE IT AND INFORMATION SECURITY, RETAIL

> “Tanium XEM’s support structure is absolutely outstanding. They come in, help our organization achieve goals by utilizing their product, help develop custom things — that’s just part of what they do, not something that we pay extra for. They want to see us succeed with their tool as best as possible.”
>
> LEAD CYBERSECURITY ENGINEER, INSURANCE

Flexibility

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer can take advantage of additional Tanium XEM Use Cases and derive incremental business value, including:

- **Reduced cyberinsurance premiums.** Interviewees noted how Tanium XEM impacted their organization’s overall cyber hygiene, which ultimately impacted cyber insurance premiums. The vice president and CISO of information technology at a healthcare organization attributed about half of their reduction in cyberinsurance premiums to Tanium XEM: “Our cyberinsurance decreased by 10%, which was unheard of this year from prior years due to a combination of things. I think the root of that is Tanium XEM, because of hygiene, how we do things, and how quickly we remediate things, in addition to my entire risk platform.”
- **Reduced shadow IT.** Forrester research defines shadow IT as the deployment and use of unauthorized or unmanaged IT devices, systems, applications, or services by line-of-business teams within an organization.

Interviewees shared that Tanium XEM offered the ability to set rules on what software can be on devices, which reduced or eliminated shadow IT. The vice president and CISO of information technology at a healthcare organization commented: “Our shadow IT exists on the acquisition of software. With Tanium XEM, we’ve set some rules when we are cleaning up the software people can have on their machines. Tanium XEM sort of shuts [the potential occurrence of shadow IT] down.”

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

> “I think Tanium XEM did about 4% to 6% of the 10% reduction in our cyberinsurance premium because it did the lion’s share of the work in preparing for that.”
>
> VICE PRESIDENT AND CISO OF INFORMATION TECHNOLOGY, HEALTHCARE

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	Licensing	$0	$2,016,000	$2,016,000	$2,016,000	$6,048,000	$5,013,494
Ftr	Internal implementation and training	$61,050	$0	$0	$0	$61,050	$61,050
Gtr	Internal ongoing management	$0	$171,600	$171,600	$171,600	$514,800	$426,744
	Total costs (risk-adjusted)	$61,050	$2,187,600	$2,187,600	$2,187,600	$6,623,850	$5,501,288

Licensing

Evidence and data. Tanium offers a range of packages which include a Core Tier and Solutions that can be added to provide additional functionality and capabilities. These packages cover areas such as asset management, compliance management, incident response, patch management, threat protection, and data discovery. Each package is designed to address specific IT and security challenges, allowing organizations to enhance their overall cybersecurity and endpoint management capabilities.

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- Licensing for each endpoint costs $40.
- **Risks.** Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:
- Number of endpoints.
- Price. Contact Tanium for additional details.

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 $5.01 million.

Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Number of endpoints	Composite		48,000	48,000	48,000
E2	Cost per endpoint	Composite		$40	$40	$40
Et	Licensing	E1*E2		$1,920,000	$1,920,000	$1,920,000
	Risk adjustment	↑5%				
Etr	Licensing (risk-adjusted)		$0	$2,016,000	$2,016,000	$2,016,000
	Three-year total: $6,048,000			**Three-year present value: $5,013,494**		

Internal Implementation And Training

Evidence and data. Interviewees discussed internal implementation and training costs associated with Tanium XEM. Depending on the size of their organization, interviewees estimated deployment from under a month to several months with several FTEs dedicated toward the implementation as it was deployed as an on-premises solution. Interviewees also highlighted that training was subjective and up to users to dedicate time toward learning the Tanium XEM platform.

While some organizations deployed Tanium XEM on-prem, other organizations may deploy it as a cloud-based solution. This would reduce overall internal implementation, training, and ongoing support costs.

- The head of enterprise IT and information technology at a retail organization commented on the initial deployment, “It took a few months to fully deploy Tanium XEM, but some of that was down to confidence of the tool which would occur with any new tool.”
- The vice president and CISO of information technology at a healthcare organization described training users on Tanium, “We had about three sessions on training users on Tanium. Each session was about 1 to 2 hours.”

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- There are two endpoint management FTEs implementing Tanium.
- Each FTE spends 250 hours on internal implementation.
- There are 30 Tanium XEM users.
- Each Tanium XEM user requires 8 internal training hours.
- The average fully burdened hourly rate per user is $75.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Whether Tanium is deployed as an on-prem or cloud-based solution. Cloud-based will significantly reduce costs as implementation duration time will be shorter in this area.
- Number of endpoint management FTEs implementing Tanium XEM.
- Hours spent implementing Tanium XEM.
- Number of Tanium XEM users.
- Average fully burdened hourly rate for an endpoint management FTE.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $61,000.

> “I would say about three people, and that’s the beauty for Tanium XEM. About three people, meaning one of Tanium’s engineers, one of your internal engineers, and a leader to remove the roadblocks, you can get it deployed.”
>
> VICE PRESIDENT AND CISO OF INFORMATION TECHNOLOGY, HEALTHCARE

Internal Implementation And Training						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Number of endpoint management FTEs implementing Tanium	Composite	2			
F2	Number of hours spent on implementation	Composite	250			
F3	Average FTE fully burdened hourly rate	Composite	$75			
F4	Subtotal: internal implementation	F1*F2*F3	$37,500			
F5	Number of Tanium users	Composite	30			
F6	Number of training hours	Composite	8			
F7	Subtotal: internal training	F3*F5*F6	$18,000			
Ft	Internal implementation and training	F4+F7	$55,500	$0	$0	$0
	Risk adjustment	↑10%				
Ftr	Internal implementation and training (risk-adjusted)		$61,050	$0	$0	$0
	Three-year total: $61,050			**Three-year present value: $61,050**		

Internal Ongoing Management

Evidence and data. Interviewees estimated their organization's ongoing management of the Tanium platform to several FTEs. In some cases, FTEs dedicated partial time toward the ongoing management while larger organizations dedicated more time. The vice president and CISO of information technology described minimal ongoing management effort: "The beauty of Tanium XEM is that it's not a solution you need to manage. I call those solutions pets. You must nourish and feed them, but Tanium XEM is a hunting bird, so you put in what you want it to go hunt and it reports back."

Modeling and assumptions. Based on the customer interviews, Forrester assumes the following about the composite organization:

- Two endpoint management FTEs dedicate 50% of their time to the ongoing management of Tanium XEM. These costs are lower for organizations using Tanium Cloud.

- The average fully burdened annual salary of an endpoint management FTE is $156,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of FTE hours spent on ongoing management.
- Average fully burdened annual salary for an endpoint management FTE.

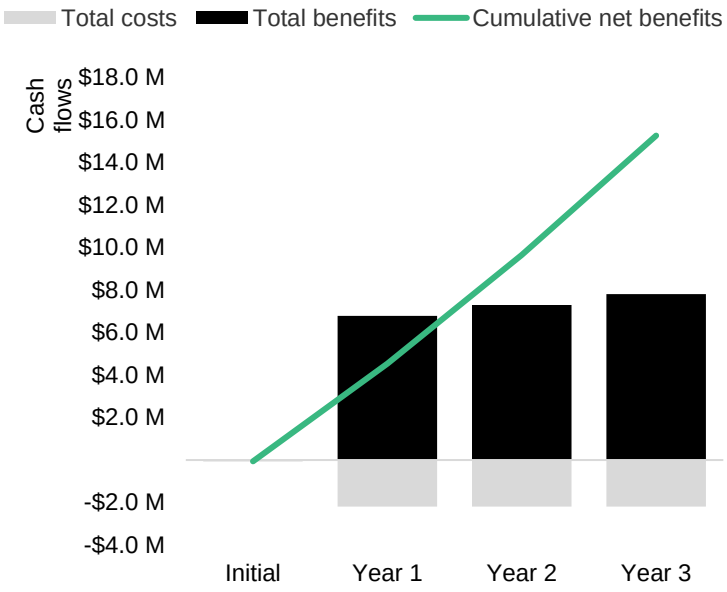
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $427,000.

Internal Ongoing Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Number of FTEs	Composite		2	2	2
G2	Percent of time spent on ongoing management of Tanium	Composite		50%	50%	50%
G3	Average FTE fully burdened salary (annual)	Composite		$156,000	$156,000	$156,000
Gt	Internal ongoing management	G1*G2*G3		$156,000	$156,000	$156,000
	Risk adjustment	↑10%				
Gtr	Internal ongoing management (risk-adjusted)		$0	$171,600	$171,600	$171,600
	Three-year total: $514,800			**Three-year present value: $426,744**		

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 Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($61,050)	($2,187,600)	($2,187,600)	($2,187,600)	($6,623,850)	($5,501,288)
Total benefits	$0	$6,791,528	$7,297,418	$7,803,308	$21,892,255	$18,067,781
Net benefits	($61,050)	$4,603,928	$5,109,818	$5,615,708	$15,268,405	$12,566,493
ROI						228%
Payback period (months)						<6

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."

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.

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.

Appendix B: Endnotes

[1] Source: “Assess Your Vulnerability Risk Response And Patch Management Maturity,” Forrester Research, Inc., July 10, 2023.

[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] This cost is inclusive of average remediation and reporting labor costs, average costs of response and notification, fines, damages, compliance costs, customer compensation, average lost business revenues and additional costs to acquire customers, and end-user downtime as it relates to a security breach across the organization; Source: Forrester Consulting Cost Of A Security Breach Survey, Q4, 2020.

[4] Source: Forrester’s Security Survey, 2022.

FORRESTER®