A Forrester Total Economic Impact™
Study Commissioned By Ivanti
April 2018

The Total Economic Impact™ Of Ivanti Security Solutions

Cost Savings And Business Benefits Enabled By Security Solutions

FORRESTER®

Table Of Contents

Project Director:
Sean McCormick

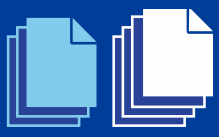
ABOUT FORRESTER CONSULTING

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

FORRESTER®

Benefits And Costs
(Three-year present value)

Reduced Risk In Cybersecurity Threats:
$585,146



Improved Productivity In Patching And Reporting:
$832,785

Ivanti Security Solution Fees:
$1,197,398

Executive Summary

Ivanti provides security solutions that help its customers reduce the risk of ransomware, malware, and other cybersecurity threats from infiltrating endpoints. Ivanti commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Ivanti Endpoint Security Solutions. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the security solutions on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with many years of experience using Ivanti. The security solutions include: automated patching for both the OS and third-party applications; application control, device control, and privilege management; Xtraction, an IT reporting dashboard; and hardware and software discovery and inventory.

Prior to using Ivanti, the customers were typically behind on their third-party patches, leaving them susceptible to ransomware and other threats. Some customers attempted to manually patch but quickly realized they had no controls to enforce updates across endpoints. These limitations led to inconsistent patching. In addition, these customers had ever-expanding application catalogs and lacked visibility into the freeware or other applications that were being installed by users on workstations across the organization. This left customers quite vulnerable to cyberattacks.

With Ivanti's security solutions, these same customers were able to reduce the size of their application catalog by whitelisting applications and ensuring all third-party applications and operating systems were up-to-date with the latest security patches installed. Customers now had visibility into all endpoints and could produce compliance reports quickly for auditors while ensuring a much higher degree of security across their organization.

Key Findings

Quantified benefits. The following risk-adjusted quantified benefits are representative of those experienced by the companies interviewed:

- Improved productivity in patching and reporting processes, leading to four and a half full-time equivalents (FTEs) of savings. Organizations were faced with large tasks to patch all endpoints on a regular basis. One interviewed customer supports 6 million patches a year across 50,000 endpoints in multiple languages. Without Ivanti, they estimated this would take nearly five times the amount of effort and resources to complete. In addition to patching, the reporting process to meet compliance was very time consuming and required multiple months of effort to manually produce the reports needed. With Ivanti, it was estimated that these reports could be produced in one-quarter the amount of time. Together, these productivity savings helped the composite organization save four and a half FTEs of effort each year. Over three years, this savings was worth $832,785.

FORRESTER®

ROI
176%

Benefits PV
$3.5 million

NPV
$2.3 million

Payback
7 months

› **Reduced risk in cybersecurity threats penetrating endpoints, saving $585,146 over three years.** Utilizing a framework provided by the US government to assess cybersecurity risk across five elements, one of the interviewed organizations measured risk across 156 standard IT department items. The results after implementing Ivanti Endpoint Security Solutions demonstrated a 40% reduction in critical and high-risk items.

› **Ivanti provides a more cost-effective solution, saving more than $850,000 annually in license fees.** Interviewed organizations had existing endpoint security solutions, including patching, in place when adopting Ivanti. Most were dissatisfied with their existing solutions as they: lacked key capabilities; didn't work as expected; and were expensive. One example of where customers were able to save costs with Ivanti was in the retirement of legacy OS and third-party application patching solutions. This reduced overall solution cost by an average of 30% to 50%.

Unquantified benefits. The interviewed organizations experienced the following benefits, which are not quantified for this study:

› **Improved customer service with reduced security risks.** Ivanti Endpoint Security Solutions maintain a strong customer experience. As stated by one security leader, "This is a product that is preventing employees from using compromised applications, but with Ivanti we can also get the correct applications to these employees quickly, in under two hours, creating a happy end user."

› **Ivanti partnership is integral in overall security strategy.** With customers attributing 40% to 80% of their overall security strategy to Ivanti, there was little need for added solutions. However, when there was need, Ivanti's partnership program allowed customers to obtain critical security solutions not offered by Ivanti. "While they may not have the entire solution, they are the willing business partner to bring others to the table and help us fortify our overall security solution."

› **Other tangible benefits from Ivanti that were not quantified include:** Hardware and software discovery and inventory, helping organizations account for all endpoints and applications operating in their environment to ensure all assets are properly secured. Additional benefits include software distribution and a self-service portal, operating system imaging, and remote control. One organization explained how they were using the remote-control capability to assist in their 14,000 annual sessions each year. They described it as "a seamless remote-control agent, both on network and associate devices not owned (BYOD), saving us about 12 minutes per session." This proved even more helpful, as they had a large amount of resources spread out across many locations and in the field.

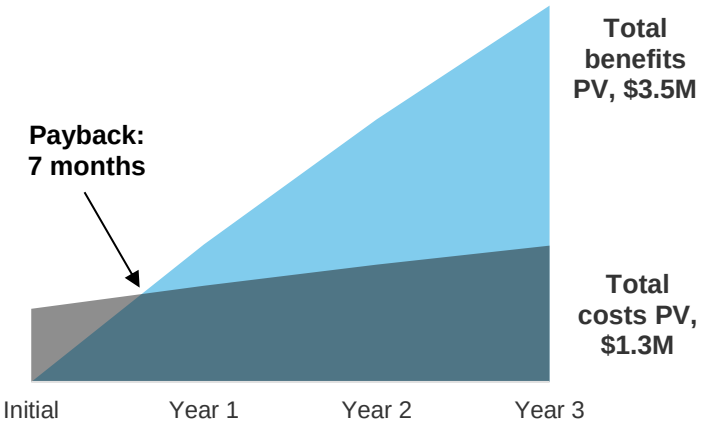
Costs. The interviewed organizations experienced the following risk-adjusted costs:

› **Ivanti license and support fees of $1,197,398 over three years.** The cost paid to Ivanti for Endpoint Security for Endpoint Manager along with Endpoint Manager (EPM), including application control and Xtraction reporting, totaled $1,197,398 over three years. This included initial license fees of $602,438 and ongoing support for 5,000 servers and 10,000 workstations. To merely extend the system center configuration manager (SCCM) with third-party patching would cost less. Please refer to the Ivanti license and support cost section for further details.

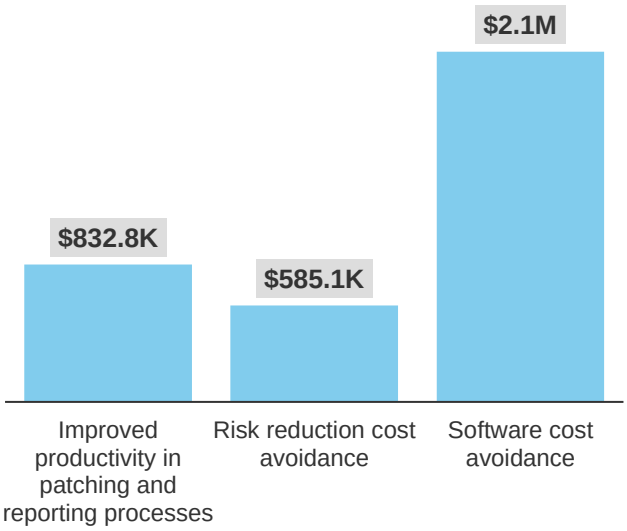
› **Implementation and training costs totaled $85,800.** With an average of 80 minutes per configuration to deploy Ivanti Endpoint Security Solutions, $85,800 of cost was incurred by the composite organization.

Forrester's interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations could experience benefits of $3,542,324 over three years versus costs of $1,283,198 adding up to a net present value (NPV) of $2,259,126 and an ROI of 176%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Ivanti Endpoint Security Solutions.

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 Ivanti Endpoint Security Solutions can have on an organization:

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

DUE DILIGENCE
Interviewed Ivanti stakeholders and Forrester analysts to gather data relative to security solutions.

CUSTOMER INTERVIEWS
Interviewed four organizations using Ivanti Endpoint Security Solutions to obtain data with respect to costs, benefits, and risks.

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

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

CASE STUDY
Employed four fundamental elements of TEI in modeling Ivanti Endpoint Security Solutions' impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Ivanti Endpoint Security Solutions Customer Journey

BEFORE AND AFTER THE ENDPOINT SECURITY SOLUTIONS INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with Ivanti Endpoint Security Solutions customers. Interviewed customers include the following:

INDUSTRY	SIZE OF ORGANIZATION	IVANTI DEPLOYMENT	NUMBER OF ENDPOINTS
Telecommunications	$10 billion+ annual revenue, 10,000+ employees	58,518 nodes, Ivanti Endpoint Management & Security Suite (EMSS)	45,000 workstations and servers
Healthcare	$5 to $10 billion annual revenue, 10,000+ employees	41,000 licenses, Total User Management Suite	38,000 workstations
Education	$1 billion annual revenue, 5,000 employees	• 7,000 nodes, Ivanti Patch for SCCM • 7,000 nodes, Ivanti Desktop Now	17,300 workstations and servers
Financial services	$5 to $10 billion annual revenue, 10,000+ employees	• 22,000 nodes Ivanti Patch for SCCM • 7,500 nodes Ivanti Desktop Now	21,000 workstations and servers

Key Challenges

The interviewed organizations had a high degree of threat exposure, as they lacked proper security controls with many of their third-party applications being out-of-date.

- **Manual processes made it difficult and cumbersome to update all operating system and third-party applications.** Two of the interviewed companies didn't have a way to enforce updates across all endpoints, which made it difficult to keep up-to-date with the latest patches released by third-party applications and operating systems. In some cases, they found themselves multiple instances behind the current patch version.
- **Alternative solutions were not meeting the needs of interviewed organizations.** Other interviewed companies utilized point solutions that were ineffective and in one case didn't work at all. The interviewee stated, "When we implemented our previous solution, we had issues right from the start. Detection logic wasn't finding the correct number of vulnerable endpoints." They went on to say that their previous solution, as ineffective as it was, was also more expensive than Ivanti.

> "When we implemented our previous solution, we had issues right from the start. Detection logic wasn't finding the correct number of vulnerable endpoints."
>
> *Manager deployment services, financial services*

FORRESTER®

- Strategically, organizations had a need to adopt more consistent cybersecurity practices, including patching, application control, and more. One interviewed organization developed a cybersecurity strategy adopting the Australian Signals Directorate's Essential Eight recommendations for securing enterprises.[1] This list included application whitelisting, patching applications, patching operating systems, and privilege management. After careful consideration, Ivanti was adopted as it helped the interview organization meet their new security strategy. One interviewee reported, "Prior to adopting our new security strategy, we were considered a good IT organization who had underinvested in cybersecurity."

Solution Requirements

The interviewed organizations searched for a solution that could:

- Automate patching for third-party applications and operating systems that could be agentless in virtual environments and work with existing consoles.
- Include additional features beyond patch management, like application and device control, privilege management, and reporting.
- Meet the needs of auditors in a proactive manner. Compliance reporting was critical for these companies.

After an extensive RFP and business case process evaluating multiple vendors, the interviewed organizations chose Ivanti Endpoint Security Solutions and began deployment.

- Different profiles were created with multiple deployment groups to develop patching cycles and cadences for each group.
- Servers and workstations were then onboarded and tested.
- Rules were developed for application whitelisting and privilege management.
- In total, it took approximately 80 minutes per configuration for implementation and deployment.

> "Ivanti has allowed us to grow and operate with a lean staff and has proven a reliable technology that is very effective."
>
> *Associate director of infrastructure security, telecommunications company*

Key Results

The interviews revealed these key results from the Ivanti Endpoint Security Solutions investment:

> "Had we not patched, we'd most likely have had a breach or incident with WannaCry."
>
> *Associate director of infrastructure security, telecommunications company*

- **Risk of cybersecurity threats was reduced by 40%.** With Ivanti Endpoint Security Solutions, organizations were able to cover the essential components of their security strategy, including the first five security controls on the Center for Internet Security's Critical Security Control list: hardware and software inventory as well as application control, continuous vulnerability management, controlled administrative privileges, and secure configuration.[2] Many of the interviewed companies attributed 40% to 80% of their security strategy to Ivanti, due to the breadth of security it provided along with the critical nature of its capabilities. One interviewed organization, after deployment of Ivanti, made a concerted effort to rapidly deploy patches to protect against the WannaCry ransomware threat. Soon after deployment, the interviewed organization began to see hits on both their firewall and network security sources that would have led to a compromise had they not implemented the correct updates. Another customer interviewed said, "With the help of Ivanti, we've massively increased and embedded cybersecurity into our culture over the last 18 months." They discussed how they used to rate themselves as a one out of 10 in cybersecurity, and now they have improved to be a five out 10, with the number of critical and high-risks items being reduced by up to 50%.
- **Automated patching helped improve productivity.** The interviewed organizations had thousands of endpoints that required numerous patches on operating systems and third-party applications. Without Ivanti's automated patching, this task would be much more time consuming, require many more resources, and would lack the extensive coverage of the Ivanti catalog. As stated by one interviewee: "We deploy 6 million patches across all the endpoints each year in multiple languages and we only need five people to support 50,000 devices. Without automated patching with Ivanti, we would need 25 people." Another customer said that they don't skip any monthly patches now that they have Ivanti. A third customer spoke to the benefit of being able to categorize applications as critical and non-critical and how it's helped them keep applications updated within 48 hours of releases.
- **Compliance reporting saved time and costs.** One of the reasons companies adopt Ivanti Endpoint Security Solutions is to help them meet and maintain compliance standards. Oftentimes auditors will require numerous reports to verify they are meeting or exceeding standards, and with Ivanti these reports were provided with ease. One customer said, "With Xtraction dashboards, we have been able to create reporting that was accepted during our last two software audits." Overall, Xtraction reporting has helped with compliance metrics and software licensing and is also used for reporting security metrics around encryption. Another customer said: "It greatly simplified our software audits. It showed the query and the data, and the reports could be emailed with high confidence." They went on to describe that the amount of time spent on reporting was reduced by 75%.
- **Privilege management helped protect users from themselves and from threats infiltrating the organization.** One of the customers interviewed had a large portion of their user base utilizing shared platforms. Often, they didn't know who was using the workstation and what they were using it for. With Ivanti, they were able to control access on workstations and ensure they could only run approved applications.

> "Ivanti Xtraction greatly simplified our software audits; it showed the query and the data. And the reports could be emailed with high confidence."
>
> *Director of end user computing, healthcare organization*

Composite Organization

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

The composite organization is a multinational financial service and insurance company with annual revenues of $7.5 billion. They have 10,000 employees working across numerous locations around the world. The organization has a strong brand, a global operations presence, a large customer base, and a strong online and offline presence.

The organization has 5,000 servers and 10,000 workstations that require constant updates and attention in order to protect customer data and maintain compliance with financial regulations across the globe. They purchased Ivanti Endpoint Security for Endpoint Manager along with Endpoint Manager (EPM), including application control and Xtraction reporting.

Key assumptions

$7.5 billion annual revenue

10,000 employees

10,000 workstations

5,000 servers

250 management servers

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Improved productivity in patching and reporting processes	$334,875	$334,875	$334,875	$1,004,625	$832,785
Btr	Risk reduction cost avoidance	$235,296	$235,296	$235,296	$705,888	$585,146
Ctr	Software cost avoidance	$854,250	$854,250	$854,250	$2,562,750	$2,124,393
	Total benefits (risk-adjusted)	**$1,424,421**	**$1,424,421**	**$1,424,421**	**$4,273,263**	**$3,542,324**

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $3.5 million.

Improved productivity in patching and reporting processes

One of the most basic, yet critical, aspects of a cybersecurity strategy is patching. Seemingly easy enough, ensuring all systems, including third-party applications, are up to date with the latest patches can be quite time consuming and difficult for organizations without the right tools. Based on the interviews with Ivanti customers, the security solutions, and specifically patch management, helped them to fulfill this aspect of their cybersecurity strategy in a cost-effective manner. One interviewee said, “Patch management and application whitelisting were the most basic things we could do to help improve our cybersecurity.” Another customer said, “Cost was a primary factor in choosing Ivanti. It was significantly cheaper per workstation.”

- **Prior to adopting Ivanti, patching was a manual process that consumed a considerable amount of resources and time**. For the interviewed organizations, adopting Ivanti Endpoint Security Solutions helped them reduce the number of resources required to support patching activities. Before Ivanti, the organization would not be able to schedule patches and reboots, as the process for patching would be tediously manual. Organizations would have to push out patches to small subsets, monitor for issues, then decide whether it was safe to push out to the entire organization. One organization said, “If we had to patch servers manually, it would take five times as many people.”

  In order to streamline their patching process, another interviewed organization had multiple solutions for different environments; however, this only caused more complications. They said, “Having one process for one part of the environment and another for a different part of the environment would require us to work with multiple organizations and have multiple tools, leading to more points of failure and twice the amount of work.”

- **With Ivanti, patching could be automated and require less resources to complete**. With Ivanti patching, deployment groups and profiles would be set up, i.e., a file server or print server, and each group would be assigned a different frequency of patching. This would help reduce the amount of upfront workload required to identify and schedule patches. In addition, once set up, vulnerability assessment could be run to identify any systems that needed to be incorporated into a patching group or profile. Ad hoc patching is also available for specific issues that arise, as well as the ability to pull back patches that may cause issues. Overall, the automated patching capability reduced the amount of resources required to complete patching activities by two-thirds.
- Ivanti Xtraction reporting can be leveraged to streamline compliance reporting and improve visibility into cybersecurity metrics. Xtraction dashboards (part of the Ivanti Endpoint Security Solution) are the reporting solution that helps provide compliance metrics, software licensing information, and other cybersecurity metrics. Interviewed organizations stated that Ivanti reporting helped to reduce the time it took to meet their auditors' needs. With Xtraction, dashboards could be set up and used to track compliance metrics. Then, when it came time for the compliance audit, these reports could be emailed to the auditor with ease. One company said: "The process was simplified. It was much less data intensive, as we didn't have to waste time giving them access to all the data. Instead, we knew what to look for and could focus our time on sending them that specific information." They went on to say that the overall time savings in their audit process was 75%.

Simplified reporting with Ivanti reduced audit process by 75%.

For the composite organization, Forrester assumes that:

- Six FTEs were required to support manual patching processes before adopting Ivanti. The composite organization experienced a 67% reduction of effort in patching after Ivanti, resulting in a savings of four FTEs' worth of effort each year.
- For compliance reporting savings, the composite organization utilized one FTE to support the audits before Ivanti reporting was available. With a 75% reduction in effort to support the audit process, the composite organization saved three-quarters of an FTE each year.
- With the average fully loaded salary for an FTE of $75,000, the composite organization was able to save $334,875 per year or $1,004,625 over three years.

Automated patching saves two-thirds the effort that was required before Ivanti.

The overall benefit for patching support and reporting efficiencies was risk-adjusted down to account for the following risks:

- The number of FTEs required to support patching and reporting, both before Ivanti and after adoption, could vary from organization to organization depending on the complexity of the organization, the compliance requirements they have, and the size of the environment they are supporting as well as the number of third-party applications.
- The fully loaded salary for an FTE could change based on the level of experience and where the organization is located.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $832,785.

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

Improved Productivity In Patching And Reporting Processes: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
A1	Patching: FTEs supporting patching before Ivanti		6.0	6.0	6.0
A2	Patching: FTEs supporting patching with Ivanti	1/3*A1	2.0	2.0	2.0
A3	Reporting: FTEs supporting reporting before Ivanti		1.0	1.0	1.0
A4	Reporting: FTEs supporting reporting with Ivanti	1/4*A3	0.3	0.3	0.3
A5	Average fully loaded FTE salary		$75,000	$75,000	$75,000
At	Improved productivity in patching and reporting processes	(A1-A2+A3-A4)*A5	$352,500	$352,500	$352,500
	Risk adjustment	↓5%			
Atr	**Improved productivity in patching and reporting processes (risk-adjusted)**		**$334,875**	**$334,875**	**$334,875**

Risk Reduction Cost Avoidance

A primary need for all the interviewed organizations was to improve their cybersecurity. With ransomware and other threats on the rise, it became increasingly important for these organizations to act. One company, after malware infected a small number of their critical components, said they had plans to protect against these threats, but that the incident became the final push to accelerate those plans and invest in their cybersecurity strategy. Having Ivanti Endpoint Security Solutions address the first five controls (and more) of the Center for Internet Security's Critical Security Control list gave the interviewed organizations confidence that they would be able to cover the essential aspects of a cybersecurity strategy and reduce their overall risk. As one interviewee stated, "Application whitelisting and patching has reduced the eight critical security items down to four, and the 56 high-risk items down by 50%."

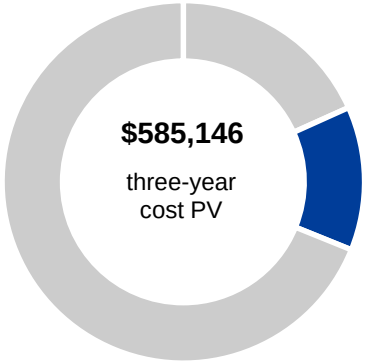
In addition to improving their overall cybersecurity, companies were able to reduce the number of minor incidents requiring help desk support and reimaging. One company said, "By limiting the software that could be installed from random places across the internet, we reduced the amount of reimages from five per week to zero."

For the composite organization, Forrester assumes that:

- Ivanti reduces the risk of a large data incident (one involving more than 1,000 records) by 40%.
- An average cost for a large data incident or breach was $4 million according to the 2017 Ponemon Institute study.[3]
- The average probability of a breach greater than 1,000 records is 14% per year based on the 2017 Ponemon Institute study.[4]
- Ten workstations were infected with malware or other threats each week, and two hours of remediation effort were required for each workstation.

The risk reduction cost avoidance will vary with:

- The industry and region in which the breach occurred.



Risk reduction cost avoidance: **17%** of total benefits

FORRESTER®

- The number of records impacted by the breach. Typically, the more records, the higher the cost of a breach.
- The faster the data breach is contained, the lower the cost.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $585,146.

Risk Reduction Cost Avoidance: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
B1	Average cost per large incident	Ponemon Institute	$4,000,000	$4,000,000	$4,000,000
B2	Percent of risk reduced by Ivanti		40%	40%	40%
B3	Average probability of breach or large incident	Ponemon Institute	14%	14%	14%
B4	Large incident cost avoidance	B1*B2*B3	$224,000	$224,000	$224,000
B5	Average number of reimages avoided with Ivanti, weekly		10	10	10
B6	Average remediation effort per reimage avoided with Ivanti (hours)		2	2	2
B7	Average fully loaded FTE hourly rate	$75,000/2080	$36	$36	$36
B8	Reimage cost avoidance	B5*52*B6*B7	$37,440	$37,440	$37,440
Bt	Risk reduction cost avoidance	B4+B8	$261,440	$261,440	$261,440
	Risk adjustment	↓10%			
Btr	**Risk reduction cost avoidance (risk-adjusted)**		**$235,296**	**$235,296**	**$235,296**

Software Cost Avoidance

Prior to adopting Ivanti Endpoint Security Solutions, the interviewed organizations had deployed other patching solutions that lacked automation capabilities or didn't function as expected. These legacy solutions were soon retired once Ivanti was deployed, saving the interviewed companies an average of 30% to 50% in license and support costs. One interviewee said: "We saw substantial benefit through Ivanti's ability to patch third-party applications with automated rules for different categories. Ivanti would download, publish, and deploy automatically."

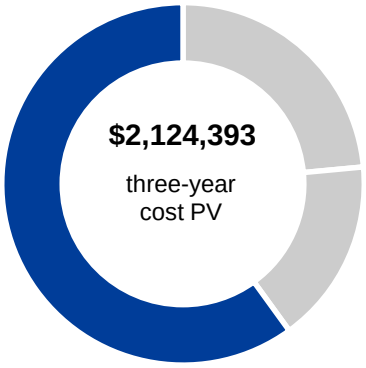
For the composite organization, Forrester assumes the following:

- The average software solution cost per management server and per endpoint was $1,000 per year and $42 per year, respectively.
- The composite organization has 250 management servers, 5,000 servers, and 10,000 workstations.

The legacy software cost avoidance will vary with:

- The cost of the previous solution.
- The number of management servers and endpoints (servers and workstations).

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $2,124,393.



Software cost avoidance: **59%** of total benefits

FORRESTER®

Software Cost Avoidance: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
C1	Average legacy software cost per management server		$1,000	$1,000	$1,000
C2	Number of management servers		250	250	250
C3	Average legacy software cost per endpoint		$42	$42	$42
C4	Number of endpoints		15,000	15,000	15,000
C5	Planning and server configuration avoidance		125,000	125,000	125,000
Ct	Software cost avoidance	C1*C2+ C3*C4+C5	$1,005,000	$1,005,000	$1,005,000
	Risk adjustment	↓15%			
Ctr	**Software cost avoidance (risk-adjusted)**		**$854,250**	**$854,250**	**$854,250**

Unquantified Benefits

Additional benefits were reported by the interviewed organization that were either qualitative in nature or were not quantified due to limited information and supporting data.

- **Improved customer experience with security risk reduction.** One common user complaint with any endpoint security solution is that it is too restrictive. Oftentimes, application whitelisting can leave users without access to important software. This can be detrimental to user productivity, especially if they cannot do their job without specific applications that are not approved. However, with Ivanti, it has been stated that applications can be provisioned and made available to workstations in under two hours.
- **Ivanti partnerships help improve organizations' overall security.** Having a strong cybersecurity strategy can sometimes require organizations to work with other companies outside of Ivanti. This typically will happen when Ivanti doesn't have the solution needed to fulfill the organization's needs. In these cases, Ivanti offers a partnership network and will suggest partners that can help fill the need. One customer said, "Ivanti is a huge part of our security posturing, and they bring other solutions they don't own through their partner program, helping us meet all our cybersecurity needs."

Ivanti reduces cybersecurity risk while improving the customer experience.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Ivanti Endpoint Security Solutions and later realize additional uses and business opportunities, including:

- **With Ivanti, other products outside the security solutions are available to customers.** Ivanti offers other solutions, including IT Asset Management (ITAM) and IT Service Management (ITSM) tools that add value beyond the security solutions adopted by customers.

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

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

FORRESTER®

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Ivanti license and support cost	$602,438	$239,243	$239,243	$239,243	$1,320,165	$1,197,398
Etr	Implementation and training cost	$85,800	$0	$0	$0	$85,800	$85,800
	Total costs (risk-adjusted)	**$688,238**	**$239,243**	**$239,243**	**$239,243**	**$1,405,965**	**$1,283,198**

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of $1.3 million.

Ivanti License And Support Cost

The cost savings provided by retiring legacy solutions was partially offset by the license and support cost for Ivanti Endpoint Security Solutions. With Ivanti, license costs were calculated based on the number of endpoints (workstations and servers). License and support costs were assessed annually and depended on the number of servers and workstations license as well as the products purchased from Ivanti. The composite organization's deployment included Endpoint Security for Endpoint Manager along with Endpoint Manager (EPM), including application control and Xtraction reporting.

For the composite organization, Forrester assumed:

- Five thousand servers and 10,000 workstations for a total of 15,000 endpoints or nodes.
- An initial cost of $38.25 per node for Endpoint Manager and Endpoint Security for Endpoint Manager was incurred as a perpetual license with $7.19 per year for maintenance per node.
- Ongoing Ivanti content subscription costs of $8 per year were also incurred.

The license and support costs will vary with:

- The components of the security solution utilized, i.e., patch management or application control. Alternatively, organizations that have an existing SCCM environment can utilize Ivanti Patch for SCCM and Ivanti Application Control for SCCM at a lower annual cost than EPM.
- The level of discount negotiated, typically due to multi-solution discounts, including ITAM or ITSM.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $1,197,398.

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

Ivanti License And Support Cost: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
D1	Ivanti Endpoint Manager and Security license cost per endpoint/node		38.25			
D2	Number of endpoints/nodes		15,000	15,000	15,000	15,000
D3	Ivanti annual maintenance cost	$7.19*D2		107,850	$107,850	$107,850
D4	Ivanti content subscription cost	$8*D2		120,000	120,000	120,000
Dt	Ivanti license and support cost	D1*D2+D3+D4	$573,750	$227,850	$227,850	$227,850
	Risk adjustment	↑5%				
Dtr	**Ivanti license and support cost (risk-adjusted)**		**$602,438**	**$239,243**	**$239,243**	**$239,243**

Implementation And Training Cost

Before Ivanti Endpoint Security Solutions could start running, organizations had to set up and define the software rules or configure each group of systems.

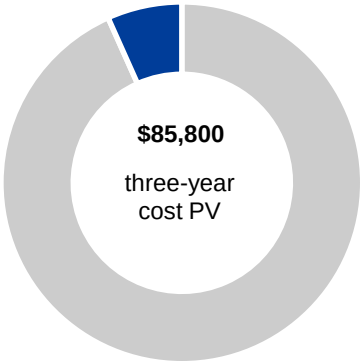
- For patch management, this mostly meant defining the groups and profiles in which the endpoints belonged and then setting the frequency in which patches would be automatically pushed out. Once the servers and workstations were onboarded, some testing was done to ensure there were no issues with the deployment.
- For application control, organizations had the ability to take two approaches. The first, most common, and least time-intensive approach is to build a trusted owner list whose responsibility is to approve application usage. The second, which is more time intensive to set up and maintain, is the traditional whitelisting approach. This requires an approved application list to be determined and rolled out across all endpoints. It is recommended that in cases where NTFS is not being utilized, the customer utilizes the traditional whitelisting approach to build out and maintain an approved application list.
- For privilege management, security profiles had to be defined and determined.

For the composite organization, Forrester assumed:

- Eighty minutes of effort were required per configuration to complete the rule definitions, testing, and deployment.
- On average, it was assumed that employees spend five minutes to learn how the application whitelisting system worked and what to expect in reboots and updates. This typically could be accomplished through corporate communications, emails, and FAQs.

The implementation and training cost could vary with:

- The complexity of the environment and the number of issues that arose from testing and the degree to which users required training.
- The average fully loaded hourly rate for an FTE could change based on the location in which the organization is located.



Implementation and training cost: **7%** of total costs

Total implementation and deployment time: **80 minutes per configuration**

FORRESTER®

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $85,800.

Implementation And Training Cost: Calculation Table

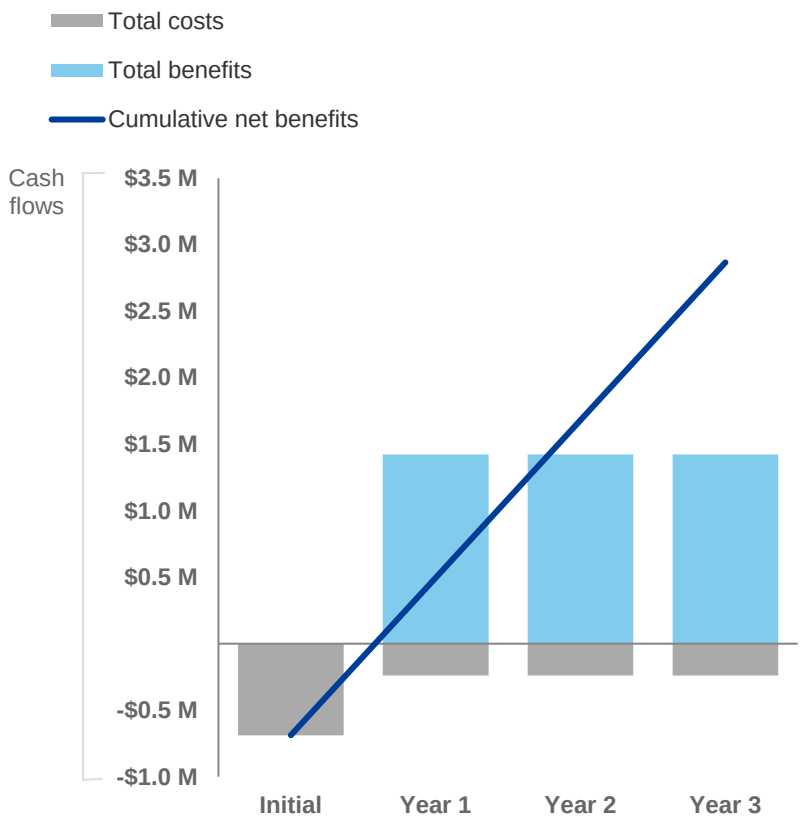
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Minutes to implement on each configuration	Minutes	80			
E2	Number of configurations		1,000			
E3	Minutes of training per staff	Minutes	5			
E4	Number of staff trained	Assumption	10,000			
E5	Average fully loaded FTE hourly rate	Assumption	$36.00			
E6	Implementation cost	(E1*E2*E5)/60	$48,000			
E7	Training cost	(E3*E4*E5)/60	$30,000			
Et	Implementation and training cost	E6+E7	$78,000	$0	$0	$0
	Risk adjustment	↑10%				
Etr	**Implementation and training cost (risk-adjusted)**		**$85,800**	**$0**	**$0**	**$0**

FORRESTER®

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($688,238)	($239,243)	($239,243)	($239,243)	($1,405,965)	($1,283,198)
Total benefits	$0	$1,424,421	$1,424,421	$1,424,421	$4,273,263	$3,542,324
Net benefits	($688,238)	$1,185,179	$1,185,179	$1,185,179	$2,867,298	$2,259,126
ROI						176%
Payback period						7 months

FORRESTER®

Ivanti Security Solutions: Overview

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

Ivanti Endpoint Security Solutions provide the endpoint security controls global experts agree create the highest barriers to real-world attacks:

- Discovery and inventory.
- Whitelisting.
- Patch and privilege management.
- Secure configuration of hardware and software.

(Note: For the purposes of this report, this overview focuses on solutions implemented by participating customers.)

- **Ivanti patch management tools can be up and running in minutes** to help discover, assess, and remediate the Windows, macOS, Linux, and UNIX systems across an organization, automatically. Simplify patching across physical and virtual systems. Find online and offline workstations and servers. Scan for missing patches and deploy them. And patch everything from the OS and apps to virtual machines (VMs), virtual templates, and the ESXi hypervisor. In addition, Ivanti offers a plug-in to Microsoft System Center Configuration Manager that automates and simplifies the process of discovering and deploying third-party app patches through the SCCM console.
- **Patching won't protect against zero-day exploits**, and many organizations are running legacy systems for which there is no patch, or they have concerns that patching will break something in their environment. To provide the next layer of defense, Ivanti helps block unauthorized applications with tools like application whitelisting and privilege management. With Ivanti Application Control, organizations can even prevent unauthorized code execution without making IT manage extensive lists manually, and without creating obstacles to user productivity. Trusted Ownership™ automatically prevents the execution of any code, even unknown, that a non-trusted owner (a typical user account, for example) introduces. Organizations can manage user privileges and policy just as easily, at a granular level, while allowing for self-elevation when exceptions occur. Users get the privileges they need to fulfil their roles — no more, no less.
- **Ivanti's security suites combine discovery capabilities with integrated secure configuration management**. Organizations can use the AV Ivanti provides or manage theirs from the same console they use to orchestrate patch management, application control, protection against fileless attacks (malicious scripts that hijack legitimate software without installing themselves on the hard drive at all), and device control (controlling removable device usage and enforcing encryption on removable devices and hard drives). They can also limit access to authorized networks or IP addresses, and customize firewall configurations for individual systems or groups of systems, including configuring the latest Windows firewalls. Remote-control capabilities help them isolate, investigate, and clean endpoints across the network. They can take control of machines that are running sluggishly or otherwise present a security concern. Real-time information helps them find a problem's root cause quickly — display information about app reputation, discovery/running time, and other metadata — and remediate from the same console. And Ivanti Endpoint Security for Endpoint Manager integrates with Ivanti Endpoint Manager to enable security and systems management from the same console.
- **Finally, Ivanti can help organizations know their results**. Since they have no real defense without real insight into their environment, Ivanti Xtraction turns reporting into a checkbox, with data on demand and the ability to create new dashboards and reports to get the right data into the hands of executives, directors, lines-of-business (LOBs), and application owners. Prebuilt connectors for nearly every tool (service desks, monitoring and ITAM toolsets, phone systems, etc.) mean no coding, business intelligence gurus, or spreadsheets — and no data silos. Xtraction can be customized to connect to even more, so everyone can view their data enterprise-wide in context — cutting through the mass of information to the critical insights that matter — to make smarter, faster decisions with ease.

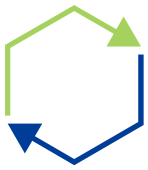
Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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



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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

FORRESTER®

Appendix B: Endnotes

[1] Source: Australian Signals Directorate's (ASD) strategies to mitigate cyber security incidents; the essential eight (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN).
[2] Source: Center for Internet Security and the critical security control list (https://www.cisecurity.org/controls/).
[3] Source: 2017 Ponemon Institute study (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN).
[4] Source: Ibid.