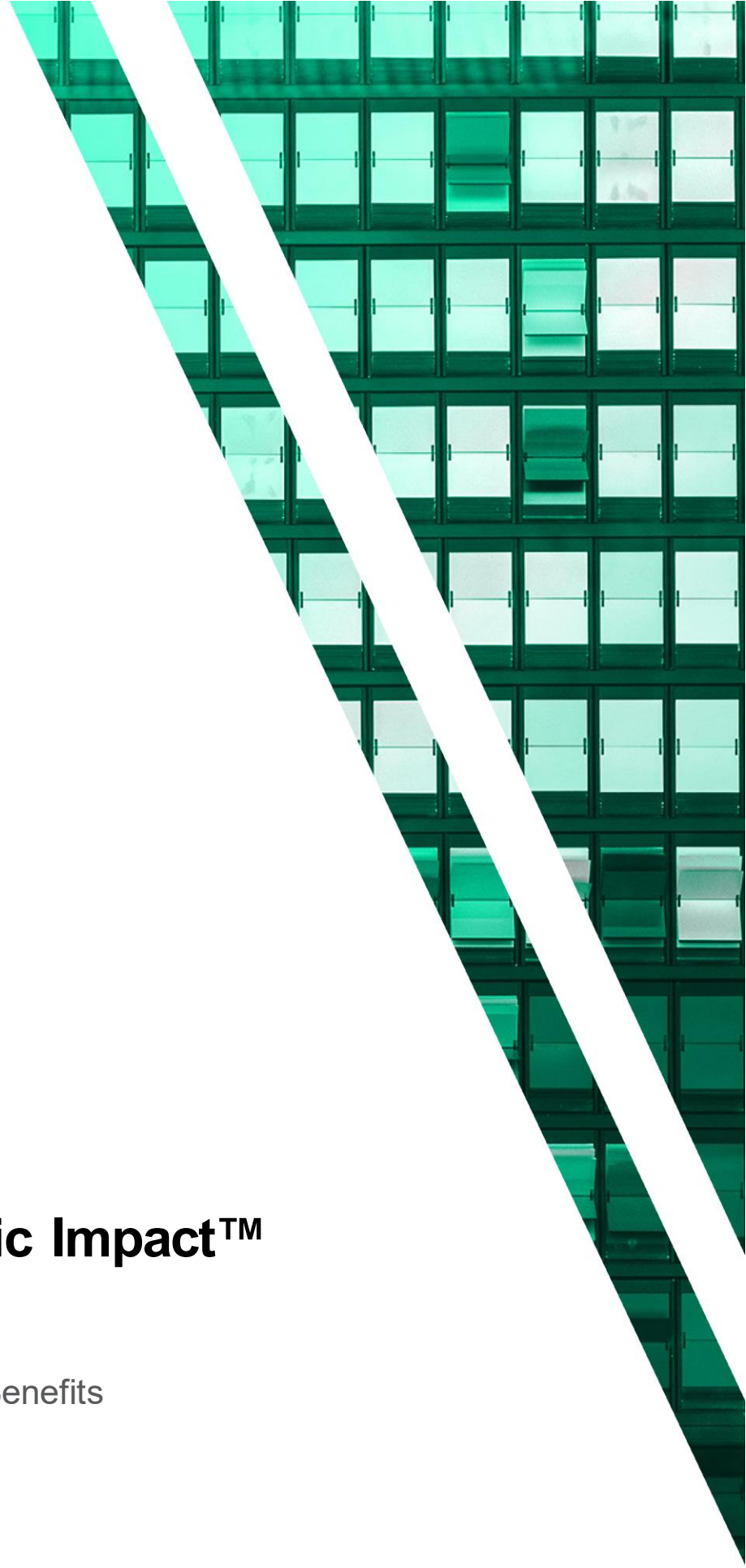
FORRESTER®



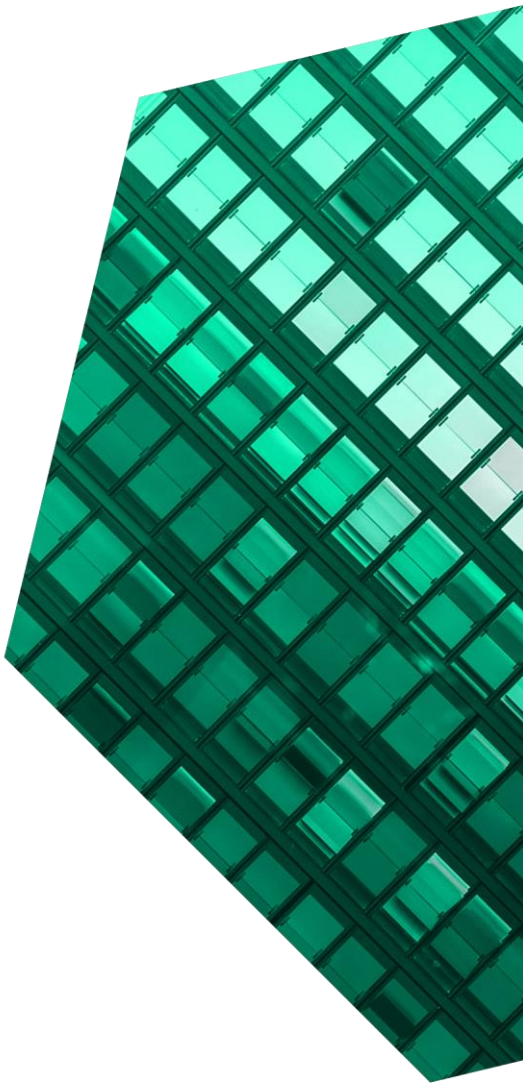
The Total Economic Impact™ Of ThreatLocker

Cost Savings And Business Benefits Enabled By ThreatLocker

JANUARY 2022

Table Of Contents

Consulting Team: Alexander Parsons



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

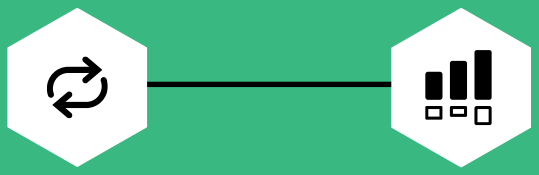
Executive Summary

Increasing threats from ransomware, malware, and data encryption are requiring organizations of all sizes and industries to reevaluate their internal IT security stacks. ThreatLocker offers companies a comprehensive Zero Trust endpoint security solution to transition away from a reliance on threat detection within traditional antivirus tools. With allowlisting and ringfencing, organizations can significantly reduce the risk and financial impacts of security breaches while increasing internal operational efficiencies.

ThreatLocker provides a comprehensive Zero Trust endpoint security solution that employs a default-deny approach through its allowlisting and ringfencing capabilities to secure an organization's internal network. By creating application, access, and storage policies, companies improve control over their internal infrastructure, reduce the risk factors for data security, and gain greater visibility to internal and external activity.

ThreatLocker commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying ThreatLocker.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of ThreatLocker on their organizations.

KEY STATISTICS



Return on investment (ROI)
166%

Net present value (NPV)
$1.94M

Reduction in risk and impact of a data breach:

Risk
45%

Impact
50%

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using ThreatLocker. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using ThreatLocker, interviewees' companies relied on antivirus and endpoint detection and response (EDR) solutions to identify known or suspected data security risks. However, these solutions were ill-equipped to address zero-day threats like ransomware. While organizations attempted to fill gaps in their security stack through fine-tuning and manual checklisting, this left the organizations at risk of a major security breach.

After the investment in ThreatLocker, the interviewees noted that their organizations experienced a significant drop in data security incidents and financial losses, while utilizing their solutions to improve visibility into internal and external data factors. Moreover, they saw an improvement in the productivity of security teams responsible for threat remediation and prevention.

> **I think what ThreatLocker does, besides the kind of one-two punch of allowlisting and ringfencing is give us a view into something that none of us had before.**
>
> — Chief information security officer, JetBlue

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Avoided risk of data breach costs of nearly $1.6 million.** Through allowlisting policy creation, organizations were able to enable a default-deny approach and prevent zero-day attacks from evolving crimeware threats. Companies could conservatively expect a 45% decrease in the number of data breaches based on their investment in ThreatLocker.
- **Decreased impact of financial breaches nearing $1 million.** Interviewees described how they were able to use ringfencing to limit application and storage use to its intended purpose, ultimately preventing attacks from having a widespread impact on their internal networks. These capabilities kept applications from maliciously running other programs like PowerShell and exposing the company to outside risk while limiting the exposure from internal attacks.
- **Increased efficiencies for incident remediation and maintenance contributing to more than $150,000 in improvements for security operations.** ThreatLocker significantly reduced malware incidents that had previously required significant resources from security operations teams. Additionally, security analysts were 25% more efficient through deflected alerts and process improvements attributable to ThreatLocker.
- **Enhanced and streamlined security stack for savings of more than $442,000.** Interviewees' organizations were able to reduce their reliance on antivirus and EDR solutions to meet their endpoint data security needs. This led to savings through decommissioning or downgrading legacy tools after deploying ThreatLocker.

"Our sister company in Canada [which doesn't use ThreatLocker] was hit hard by ransomware. [It affected] servers, backups, workstations, which cost them millions. The loss of productivity and financial loss was just crazy. … My next call was to ThreatLocker to throw up our shields because we were in learning mode. I felt very relaxed after I made that call and have been since."

IT infrastructure manager, infrastructure

Unquantified benefits. Benefits that are not quantified for this study include:

- **Improved operational efficiencies for supporting user access requests.** Interviewees' companies were able to streamline and enhance internal processes for standard and elevated access requests. This led to operational improvements for their IT desktop support teams and eliminated the need to invest in additional access-elevation software.
- **Improved control and visibility within internal network.** ThreatLocker's unified audit and ringfencing capabilities helped organizations to better understand internal and external activity within their network while granting more appropriate access to each of its users.

Costs. Risk-adjusted PV costs include:

- **Licensing fees of $900,000 comprised 77% of total costs.** ThreatLocker license fees are dependent on the solutions purchased and may vary based on the number of endpoints. Over a three-year period, the composite organization paid $902,479 in license fees.
- **Implementation costs of just over $160,000 over a three-year period accounted for security and IT team member time.** Organizations required an average period of three months and a small team for the initial integration of the product as well as establishing allowlisting and ringfencing policies before launching ThreatLocker. Additional IT resources performed end user deployment and support.
- **Software maintenance, training, and development cost $100,000 over three years.** Interviewees typically required 10 hours of weekly maintenance related to updating policies and end user support requests. Additional investment was necessary from an educational standpoint to ensure security analysts were fully up to speed on solution functionality and trends in data security.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $3.11M million over three years versus costs of $1.17M, adding up to a net present value (NPV) of $1.94M and an ROI of 166%.

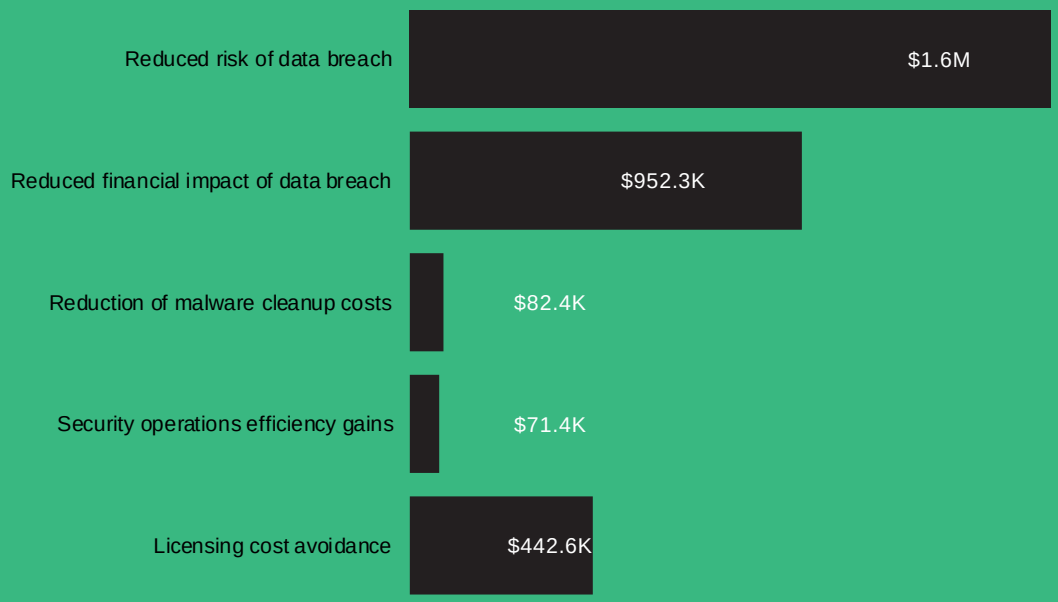
ROI
166%

BENEFITS PV
$3.11M

NPV
$1.94M

PAYBACK
<6 months

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

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

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 ThreatLocker can have on an organization.

DUE DILIGENCE

Interviewed ThreatLocker stakeholders and Forrester analysts to gather data relative to ThreatLocker.

DECISION-MAKER INTERVIEWS

Interviewed four decision-makers at organizations using ThreatLocker to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' 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 decision-makers.

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.

The ThreatLocker Customer Journey

Drivers leading to the ThreatLocker investment

Interviewed Decision-Makers

Interviewee	Industry	Revenue	Deployed Endpoints
Chief information security officer, JetBlue	Transportation	$1 billion to $10 billion	11,000
IT infrastructure manager	Infrastructure	$1 billion to $10 billion	1,300
Director of IT	Medical services	$1 million to $10 million	500
President	Security	$1 million to $10 million	1,500
Director of technology	Security	$1 million to $10 million	1,500

KEY CHALLENGES

Prior to their investment in ThreatLocker, interviewees noted that their organizations faced increasing concerns with endpoint security threats leading to security breaches within their organizations. Most commonly, organizations were dependent on antivirus and EDR solutions to meet their data protection needs.

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

- **Evolving needs for endpoint security.** Interviewees described their prior solutions as reactive in nature, targeting known or suspected threats rather than default-deny techniques. This put their organizations at risk of zero-day attacks. Additionally, vulnerability to known weaknesses manifested into other applications within their networks. The director of IT in medical services said, "ThreatLocker is proactive, antivirus is reactive, so [with] things like ransomware, most of the time before you identify, they've already done damage."
- **Data breaches resulting in lost data, financial loss, and loss of reputation.** Interviewed decision-makers discussed the increasing prevalence of ransomware, data encryption, and other types of security attacks that their current solutions were less effective at protecting against. Not only were they experiencing attacks within their own networks but they also witnessed larger attacks to their partners and competitors. The director of technology at the security company explained, "The bad actors are working just as hard to try to circumvent the tools as anybody."

"The nightmare for anybody that's in charge of IT is a breach of security. We have a lot of confidential information."

Director of IT, medical services

- **Loss of productivity while remediating malware incidents.** Interviewees' organizations dedicated significant internal resources related to endpoints impacted by malware and other attacks. Cleaning machines of viruses required time-intensive processes such as application or workstation reloads, which affected IT security analysts and end users alike.

"We adopted ThreatLocker because we felt like ThreatLocker was more of a peace-of-mind, robust security product that was going to help us sleep at night."

President, security

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Provide a Zero Trust endpoint architecture that incorporates an allowlisting application with default-deny approach to their security stack.
- Limit zero-day threats beyond known vulnerabilities through ringfencing capabilities.
- Increase productivity of security analysts.
- Expand visibility into internal and external user and application activities.
- Provide ability to easily configure internal policies for allowlisting and ringfencing.

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 four decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The US-based global conglomerate includes operations in North America, Europe, and Australia. It has an annual revenue of $4.5 billion and more than 10,000 employees. The company provides most of its workers with laptop/desktop computers. The organization has an existing security platform with an antivirus/EDR solution that it previously used to address its endpoint security needs.

Deployment characteristics. The composite organization deploys ThreatLocker across its desktop/laptop endpoints after a three-month implementation period. A team of 10 security analysts supports the tool.

Key assumptions

- **$4.5 billion in revenue**
- **10,000 endpoints deployed**
- **Headquartered in the US with global operations**
- **10 security analysts**

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	Reduced risk of data breach	$626,631	$626,631	$626,631	$1,879,893	$1,558,339
Btr	Reduced financial impact of data breach	$382,941	$382,941	$382,941	$1,148,823	$952,318
Ctr	Reduction of malware cleanup costs	$33,150	$33,150	$33,150	$99,450	$82,439
Dtr	Security operations efficiency gains	$28,730	$28,730	$28,730	$86,190	$71,447
Etr	Licensing cost avoidance	$0	$280,500	$280,500	$561,000	$442,562
	Total benefits (risk-adjusted)	$1,071,452	$1,351,952	$1,351,952	$3,775,357	$3,107,105

REDUCED RISK OF DATA BREACH

Evidence and data. Interviewees shared that ThreatLocker's allowlisting capabilities improved their coverage against endpoint security risks and reduced the risk of potential security breaches. By employing a default-deny approach, organizations felt better prepared to stop zero-day threats from both internal and external sources.

- Companies saw immediate benefits for risk prevention after deployment. Interviewees' organizations were able to develop policies for the current applications running on their systems based on a learning-mode period during implementation. The process helped to automate the experience without having a significant impact on end users.
- The chief information security officer at JetBlue described their experience, "In terms of effectiveness, I can't think of very many solutions or end solutions that compare with the potential effectiveness of [ThreatLocker]."

  He continued: "[Allowlisting] is a paradigm shift when you're talking about endpoint security in that since [crimeware] was first created, we've always gone down the road of detection. Antivirus is about detecting heuristic patterns of behavior which are anomalous or signatures. Watching that battle go back and forth for decades literally, you realize that there needs to be a different approach."
- All four interviewees saw a significant drop in security breaches from ransomware, including three interviewees reporting no incidents since implementing ThreatLocker's solutions.

"Now with ThreatLocker, things don't run unless we allow them to run. So even if [employees] happen to click a link they shouldn't have, it didn't run anything bad."

Director of technology, security

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

- Has 2.5 data breaches annually at a cost of $655,300 for an organization with $4.5 billion revenue and 10,000 endpoints deployed, based on Forrester's proprietary research.[2]
- Can conservatively expect a 45% decrease in the number of security breaches.

Risks. The reduced financial impact of a data breach will vary with:

- The baseline security strength, exposure, and posture of the organization.
- The skill set and salary levels of the organization's security team.
- The organization's size, industry, and location.

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 $1.6 million.

Reduced Risk Of Data Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of data breaches per year prior to deploying ThreatLocker	Forrester research	2.5	2.5	2.5
A2	Reduction in data breaches	Interviews	45%	45%	45%
A3	Number of data breaches per year after deploying ThreatLocker	A1*(1-A2)	1.375	1.375	1.375
A4	Average cost per data breach	Forrester research	$655,300	$655,300	$655,300
At	Reduced risk of data breach	(A1-A3)*A4	$737,213	$737,213	$737,213
	Risk adjustment	↓15%			
Atr	Reduced risk of data breach (risk-adjusted)		$626,631	$626,631	$626,631
	Three-year total: $1,879,893		**Three-year present value: $1,558,339**		

REDUCED FINANCIAL IMPACT OF DATA BREACH

Evidence and data. Beyond the ability to reduce data breaches, interviewees' organizations were able to utilize ringfencing and ThreatLocker's Storage Control solution to limit the effectiveness of data security threats such as ransomware and data encryption.

- Interviewees described how their organizations could set up ringfencing policies to restrict the functionality of applications to their intended purposes. This decreased the effectiveness of

"Another feature I like about it [is] that if I have to put in something new or allow something, I don't have to sit down and create the rule. I just have to put it on learning mode, get it done, and then it captures the rule for me. It doesn't get better than that."

Director of IT, medical services

attacks and prevented them from spreading within a company's internal network.

- The chief information security officer at JetBlue shared: "Ringfencing closes the gap on authorized applications, which have weaknesses that are undisclosed.… I don't think prior to this application, anybody had identified that it is unnecessary for IE or Chrome or Windows applications to instantiate PowerShell. It's actually important to [set policies] now that you have the ability to take action with ringfencing."
- Additionally, companies could provide protection for storage and removable storage (such as USBs) within their organizations by setting policies to limit how users interact with data. including determining read/write capabilities or limiting the types of files they can interact with (e.g., JPG, XLS, DOC, etc.). Security teams were able to quickly evaluate and set up appropriate controls.
- None of the interviewed organizations experienced substantial financial losses from security breaches after implementing ThreatLocker.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- After deployment of ThreatLocker, the composite organization experiences 1.375 annual data breaches.
- The cost of a data breach for the composite is $655,300 for an organization with $4.5 billion in revenue and 10,000 endpoints deployed based on Forrester's proprietary research.[3]
- The composite organization can conservatively expect a 50% decrease in the impact of a data security breach.

Risks. Several factors may affect the impacts organizations experience:

- The baseline security strength, exposure, and posture of the organization.
- The skill set and salary levels of the organization's security team.
- The organization's size, industry, and location.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of more than $952,000.

"Having something that actually has absolute blocking or absolute allow for things that you know are fine to run — that's an unmeasurable, but a very comforting feeling"

Chief information security officer, JetBlue

Reduced Financial Impact Of Data Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of data breaches per year after deploying ThreatLocker	A3	1.375	1.375	1.375
B2	Average cost per data breach	Forrester research	$655,300	$655,300	$655,300
B3	Reduced data breach impact with Zero Trust security	Interviews	50.0%	50.0%	50.0%
Bt	Reduced financial impact of data breach	B1*B2*B3	$450,519	$450,519	$450,519
	Risk adjustment	↓15%			
Btr	Reduced financial impact of data breach (risk-adjusted)		$382,941	$382,941	$382,941
	Three-year total: $1,148,823			**Three-year present value: $952,318**	

REDUCTION OF MALWARE CLEANUP COSTS

Evidence and data. Before making the investment in ThreatLocker, frequent malware and data encryption incidents required significant internal resources to remediate, rebuild, and replace endpoints. By reducing cleanup efforts through allowlisting and ringfencing, interviewed organizations realized significant operational efficiencies.

- The director of technology for a security organization explained their experience: "Before ThreatLocker, we were trying to clean [machines] from virus infections or reloading the workstations and reloading all their applications because they were infected, and we didn't trust the machine without reloading it. You can easily spend several hours rebuilding that machine and getting it all up and running. We haven't had to do any of those last year [since deployment]."
- Interviewees reported having up to a 100% decrease in malware incidents, which allowed their organizations to redeploy security resources to other priorities.

Modeling and assumptions. Based on the customer interviews, Forrester estimates for the composite organization:

> **"Less effort trying to remove unauthorized software. We can't install unauthorized software now whether it's malware or anything at all that wasn't on our list."**
>
> *IT infrastructure manager, infrastructure*

- The composite organization averages seven malware incidents per 100 endpoints annually before deployment of ThreatLocker.
- The organization sees a reduction of 600 malware incidents annually based on 10,000 endpoints deployed.
- Remediation of the average malware incident required 2 hours of security analyst resource time.
- The average fully burdened hourly rate of a security analyst is $65.

- A conservative time savings estimate factors in a time recapture metric of 50%.

Risks. The value of this benefit may vary for other organizations due to:

- Their relative size, industry, and number of endpoints deployed.
- The skill level, efficiency, and salaries of analysts.
- Their security posture and exposure.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of more than $82,000.

Decrease in malware incidents with ThreatLocker

86%

Reduction Of Malware Cleanup Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of deployed endpoints	Composite	10,000	10,000	10,000
C2	Malware incidents (per 100 endpoints annually)	Interviews	7	7	7
C3	Annual reduction of incidents (per 100 endpoints)	Interviews	6	6	6
C4	Annual reduction of incidents	(C1/100)*C3	600	600	600
C5	Average number of hours per remediation	Interviews	2	2	2
C6	Average fully burdened hourly compensation rate for a security analyst	TEI standard	$65	$65	$65
C7	Productivity recapture rate	Assumption	50%	50%	50%
Ct	Reduction of malware cleanup costs	C4*C5*C6*C7	$39,000	$39,000	$39,000
	Risk adjustment	↓15%			
Ctr	Reduction of malware cleanup costs (risk-adjusted)		$33,150	$33,150	$33,150
	Three-year total: $99,450			**Three-year present value: $82,439**	

SECURITY OPERATIONS EFFICIENCY GAINS

Evidence and data. The capabilities of ThreatLocker's tools and deflected incidents helped to decrease the time security analysts dedicated to endpoint data security at interviewees' companies.

- Leveraging ThreatLocker's easy-to-use interface and support, organizations were able to transition away from manual tasks and the need for constant tuning of detection solutions to try to address evolving crimeware behavior.
- Deflected incidents and more robust coverage through ringfencing had positive downstream impacts on network-based security solutions as well.
- The chief information security officer at JetBlue discussed the firm's internal shift in security focus since implementing ThreatLocker, saying, "It's shifted from endpoint to more time, more focus on network-based, which is definitely higher value."
- Overall, organizations decreased the time dedicated to endpoint security by 25% and redeployed resources to higher-value tasks within the organization.

Modeling and assumptions. To quantify the value of this benefit, Forrester assumes:

- The composite organization has 10 security analysts who dedicate 20% of their time to endpoint security.
- Security analysts see a 25% improvement in their overall efficiency based on the deployment of ThreatLocker's solutions.
- The average fully burdened hourly rate of a security analyst is $65.
- A conservative time savings estimate factors in a time recapture metric of 50%.

> **"[ThreatLocker is] constantly developing new things. They've taken suggestions of ours and implemented them. The interface changes often. They're always enhancing it. They don't rest over there, apparently."**
>
> *IT infrastructure manager, infrastructure*

Risks. The value of this benefit may vary in other organizations due to:

- Their relative size, industry, and number of endpoints deployed.
- The skill level, efficiency, and salaries of analysts within an organization.
- The security posture and exposure of the composite organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of more than $71,000.

Security Operations Efficiency Gains					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of security analyst FTEs	Interviews	10	10	10
D2	Average fully burdened hourly compensation rate for a security analyst	TEI standard	$65	$65	$65
D3	Percentage of time spent on alerts and incident support prior to ThreatLocker	Assumption	20%	20%	20%
D4	Time gains from deflected alerts and process improvements with ThreatLocker deployment	Assumption	25%	25%	25%
D5	Productivity recapture rate	Assumption	50%	50%	50%
Dt	Security operations efficiency gains	D1*D2*D3*D4*D5* 52 weeks*40 hours	$33,800	$33,800	$33,800
	Risk adjustment	↓15%			
Dtr	Security operations efficiency gains (risk-adjusted)		$28,730	$28,730	$28,730
	Three-year total: $86,190			**Three-year present value: $71,447**	

LICENSING COST AVOIDANCE

Evidence and data. After deploying ThreatLocker, companies were able to reevaluate their security stack based on the solution's capabilities. Interviewees shared that their organizations were able to decommission or downgrade licensing related to their EDR and endpoint protection platform (EPP) solutions. Most organizations waited for a period after ThreatLocker's deployment before making changes to their security stacks.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- Organizations are able to reevaluate and decommission annual spend on licensing for antivirus and EDR solutions totaling $33 per endpoint based on Forrester's research.
- The composite organization realizes savings for 10,000 endpoints starting in the second year after deploying ThreatLocker.

Risks. The total licensing cost avoidance benefit will vary with:

- The desired endpoint protection and coverage of the organization.
- The number of legacy tools.
- The cost of legacy tools.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of nearly $443,000.

Licensing Cost Avoidance					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Number of retired third-party licenses	Composite	0	10,000	10,000
E2	Individual annual licensing cost	Forrester research	$33	$33	$33
Et	Licensing cost avoidance	E1*E2	$0	$330,000	$330,000
	Risk adjustment	↓15%			
Etr	Licensing cost avoidance (risk-adjusted)		$0	$280,500	$280,500
	Three-year total: $561,000			**Three-year present value: $442,562**	

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Improved operational efficiencies and cost avoidance from automation of the access process for users and administrators.** ThreatLocker's Elevation Control solution streamlined and enhanced the approval process for access requests. ThreatLocker quickly gave users access or elevated access for specified or perpetual time periods. This helped interviewees' companies realize process improvements for their IT organizations. Companies could also avoid or decommission an investment in an administration elevation tool with ThreatLocker.
- **Enhanced visibility to end-user and application activity.** Each of the interviewees shared how ThreatLocker's features and interface improved their ability to understand internal and external activity at their organizations. Moreover, companies could realize gains to desktop support processes and potentially lower monitoring costs by utilizing ThreatLocker's unified audit log. The IT infrastructure manager in infrastructure explained: "It has [an] amazing audit trail, audit system. We have found files that were deleted, which is really not a [core] ThreatLocker function, but it's logged in there."
- **Improved administrative control over the internal network.** ThreatLocker helped limit administrative access for users within interviewees' organizations to their intended purposes. The chief information security officer at JetBlue stated: "Shadow IT becomes another conduit for criminal activities to compromise the things that are untested, unlicensed. There are ramifications for IT, cost control, visibility, resiliency, and then there are costs for security, and that is obviously a redirection of resources. With ThreatLocker, you can make those decisions once you get the details back from learning mode."
- **Provided partnership and support.** Interviewees' organizations took advantage of ThreatLocker's internal support and network of customers for ongoing improvements at no additional cost. The IT infrastructure manager said: "Their support is phenomenal. They're very responsive. They're easy to get ahold of, they're very thorough, they research things, and they've gotten back to us when it's something that couldn't be resolved immediately."

FLEXIBILITY

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

- **Potential sales and revenue impacts for managed service providers.** Interviewees stated that they were able to increase revenue with their customers where they were serving as a managed service provider based on their investment in a Zero Trust security solution.
- **Improved computer longevity and usage.** Three out of four interviewees' companies saw an improvement in how their managed laptops and desktops functioned based on how they were able to clean up applications running on machines. One interviewees' company decreased internal resources for their standard maintenance processes by 50% based on being able to reevaluate their refresh processes.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Ftr	Enterprise license fees (annual)	$0	$362,900	$362,900	$362,900	$1,088,700	$902,479
Gtr	Implementation costs	$163,262	$0	$0	$0	$163,262	$163,262
Htr	Software maintenance, training, and development costs	$3,738	$40,365	$40,365	$40,365	$124,833	$104,119
	Total costs (risk-adjusted)	$167,000	$403,265	$403,265	$403,265	$1,376,795	$1,169,860

ENTERPRISE LICENSE FEES (ANNUAL)

Evidence and data. The interviewees reported that their organizations incurred annual licensing fees for ThreatLocker per endpoint.

Modeling and assumptions. For the analysis, Forrester assumes the following:

- The composite organization pays annual enterprise licensing fees of $36.29 per endpoint for ThreatLocker's full suite of products.
- The organization enrolls 10,000 endpoints.

Risks. Licensing fees will vary from organization to organization based on:

- The licensing agreement and specific solutions an organization chooses.
- The number of endpoints enrolled.

Results. Forrester did not identify risk in this cost category and calculated a three-year, risk-adjusted total PV (discounted at 10%) of $902,000.

Enterprise License Fees (Annual)						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Number of endpoint licenses	Composite		10,000	10,000	10,000
F2	Cost per endpoint license (annual)	Interviews		$36.29	$36.29	$36.29
Ft	Enterprise license fees (annual)	F1*F2	$0	$362,900	$362,900	$362,900
	Risk adjustment	0%				
Ftr	Enterprise license fees (annual) (risk-adjusted)		$0	$362,900	$362,900	$362,900
	Three-year total: $1,088,700			**Three-year present value: $902,479**		

IMPLEMENTATION COSTS

Evidence and data. Interviewees described the implementation process as straightforward, effective, and easy due to the ease of integration, strong partner support of ThreatLocker, and automated policy-setting.

- The integration took three months on average for organizations. This included a one- to two-week period of running ThreatLocker in learning mode upfront to develop automated allowlisting and ringfencing policies.
- Internal resources including IT analysts, security analysts, and business leaders spent additional time reviewing and updating policies, integrating the tool within their security infrastructure, and navigating the tool's functionality.
- The initial launch of ThreatLocker to end users required some time on the part of the desktop support team for the actual deployment and an initial, temporary increase in support questions.

"It was really, really amazing. I mean, I would say it's one of the easiest security implementations I've ever had. Just about 2 hours because all the data was just downloaded into the servers and pushed into all the computers."

Director of IT, medical services

Modeling and assumptions. Forrester assumes the following conditions surrounding implementation:

- ThreatLocker is deployed over a 12-week period.
- The implementation requires 25% of a 10-person team's time with an aggregate fully loaded hourly rate of $94.
- Deployment requires 5 minutes of support for each of the composite's 10,000 endpoints.
- The average fully burdened hourly rate of a desktop support analyst is $35.

Risks. These costs may vary for other organizations due to several factors:

- The skill set and salary levels of the implementation team.
- The complexity of the organization's existing internal IT infrastructure.
- Whether the solution requires a longer (or shorter) time to install and test or requires different resources from the IT team.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $163,000.

Implementation Costs						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of people involved in the implementation process	Interviews	10			
G2	Average fully loaded hourly rate for the aggregated implementation team	TEI standard	$94			
G3	Weeks spent on implementation tasks	Interviews	12			
G4	Percentage of time allocated to implementation of ThreatLocker	Interviews	25%			
G5	Subtotal: software implementation, policy creation, and baselining	G1*G2*G3*G4* 40 hours per week	$112,800			
G6	Number of endpoints	Composite	10,000			
G7	Endpoint installation time (minutes)	Interviews	5			
G8	Average fully loaded hourly compensation rate for a desktop IT analyst	Assumption	$35			
G9	Subtotal: software deployment to endpoints	G6*(G7/60)*G8	$29,167			
Gt	Implementation costs	G5+G9	$141,967	$0	$0	$0
	Risk adjustment	↑15%				
Gtr	Implementation costs (risk-adjusted)		$163,262	$0	$0	$0
	Three-year total: $163,262		**Three-year present value: $163,262**			

SOFTWARE MAINTENANCE, TRAINING, AND DEVELOPMENT COSTS

Evidence and data. Interviewees described requiring additional internal resources for ongoing maintenance, continuing education, and internal development based on their investment in ThreatLocker.

- Beyond a larger upfront investment in learning and development, organizations reserved time for their security operations team to engage in online training through ThreatLocker University to stay up to date on security trends and the solution's functionality.
- Internal teams of three to 20 FTEs performed ongoing maintenance for policy creation and supported end users, depending on the size and support models of the interviewees' organizations.

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

- Five security analysts spend 10 hours each on learning and development during the initial implementation.
- Ten security analysts spend 10 total hours weekly on maintenance. Additionally, each analyst spends 2 hours annually on learning and development for continuing education.
- The average fully burdened hourly rate of a security analyst is $65.

Risks. Organizations will face varying software maintenance, learning, and development costs depending on:

- The complexity and support model of the organization's IT infrastructure.
- The skill level, efficiency, and salaries of analysts within an organization.
- The security posture and exposure of the composite organization.
- The number of security analysts trained on ThreatLocker.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $104,000.

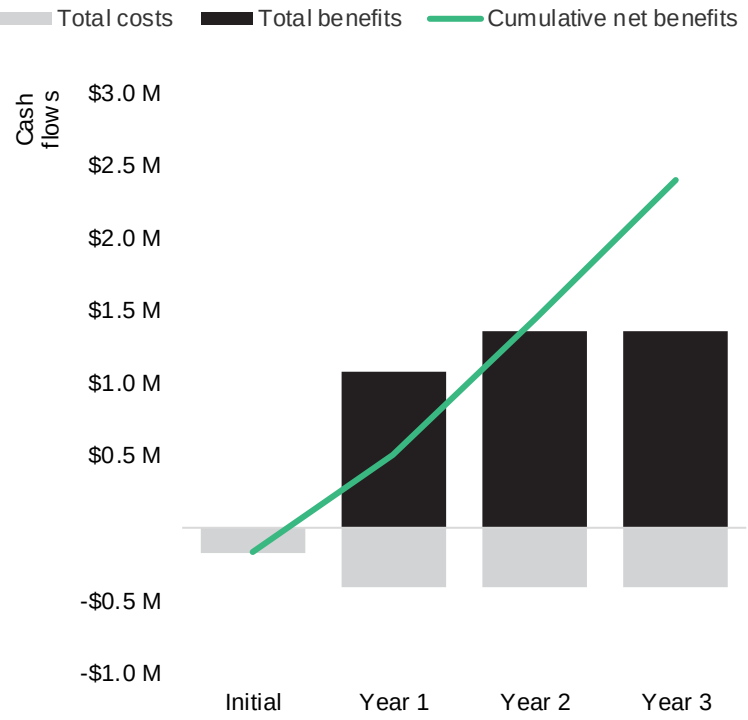
Software Maintenance, Training, And Development Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Security analysts FTEs	Interviews	5	10	10	10
H2	Average fully burdened hourly rate for a security analyst	TEI standard	$65	$65	$65	$65
H3	Hours per week spent on maintenance and end-user support	Interviews		10	10	10
H4	Subtotal: software maintenance	H2*H3*52	$0	$33,800	$33,800	$33,800
H5	Annual hours spent on learning and development per security analyst	Interviews	10	2	2	2
H6	Subtotal: training for security analysts	H1*H2*H5	$3,250	$1,300	$1,300	$1,300
Ht	Software maintenance, training, and development costs	H4+H6	$3,250	$35,100	$35,100	$35,100
	Risk adjustment	↑15%				
Htr	Software maintenance, training, and development costs (risk-adjusted)		$3,738	$40,365	$40,365	$40,365
	Three-year total: $124,833			**Three-year present value: $104,119**		

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	($167,000)	($403,265)	($403,265)	($403,265)	($1,376,795)	($1,169,860)
Total benefits	$0	$1,071,452	$1,351,952	$1,351,952	$3,775,357	$3,107,105
Net benefits	($167,000)	$668,187	$948,687	$948,687	$2,398,562	$1,937,245
ROI						166%
Payback (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."

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

Appendix B: Endnotes

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

[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[3] Ibid.


FORRESTER®