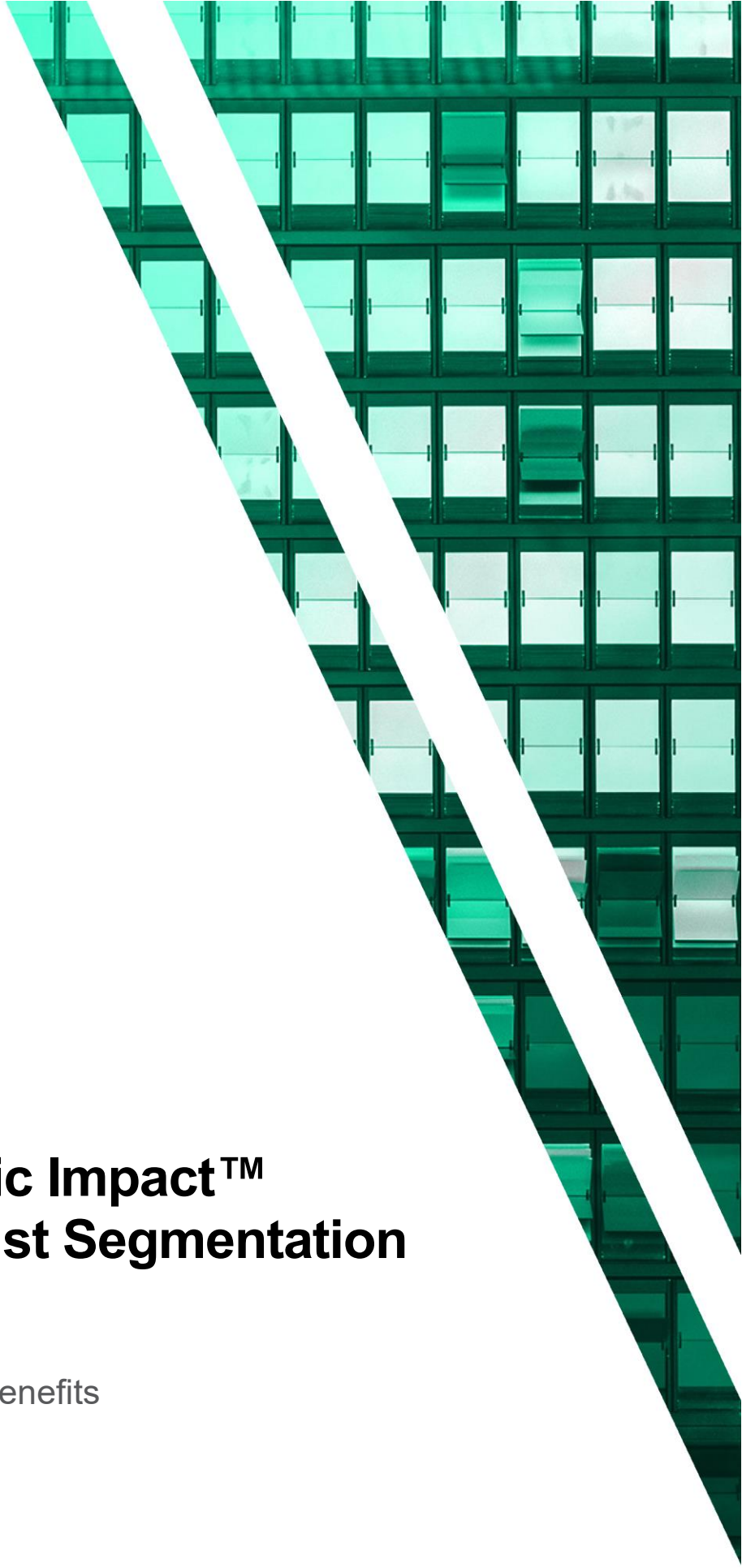
FORRESTER®



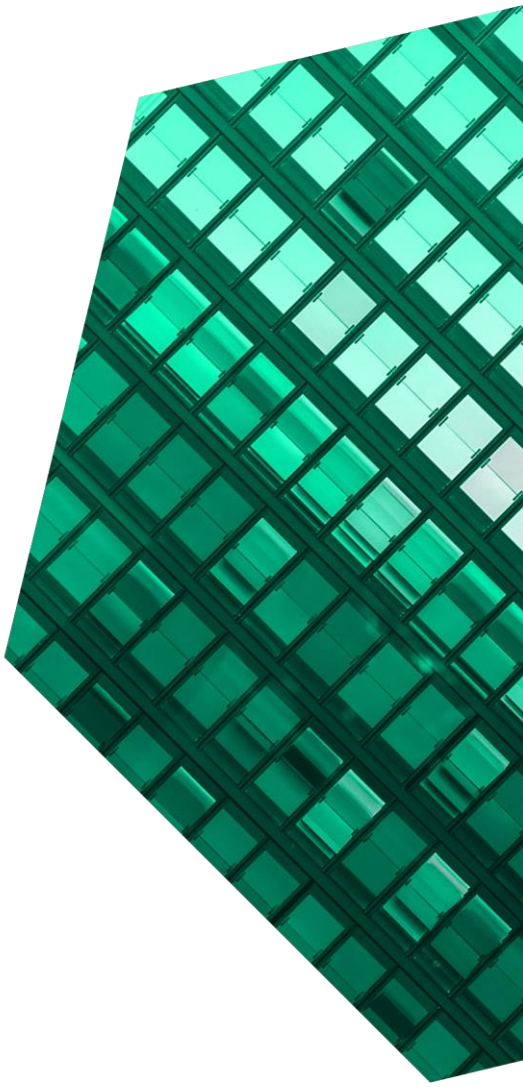
The Total Economic Impact™ Of Illumio Zero Trust Segmentation (ZTS)

Cost Savings And Business Benefits Enabled By Illumio ZTS

MARCH 2023

Table Of Contents

Consulting Team: Nick Ferrif
Henry Huang
Otto Leichliter
Marianne Friis



ABOUT FORRESTER CONSULTING

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

Executive Summary

Organizations are growing and becoming more complex. Applications and data are sprawling across a diverse attack surface, and the traditional perimeter defense approach is inadequate. The Illumio Zero Trust Segmentation (ZTS) Platform is a simplified and scalable platform to enable visibility and segmentation for containing breaches. Using Illumio ZTS, organizations can stop breaches and ransomware from spreading and drastically reduce the negative impact on their business.

Illumio prevents breaches and ransomware from spreading across hybrid IT with Zero Trust Segmentation (ZTS), including microsegmentation. Its ransomware mitigation and segmentation solutions enable employees at modern organizations to see their organizations' risk, isolate attacks, and secure their data. Leveraging a host-based approach that works across hybrid clouds, on-premises, containers, and endpoints, organizations can automate segmentation policy creation and segment down to individual devices, workloads, and cloud assets. Illumio ZTS is infrastructure-agnostic and can be used for both visibility and enforcement simultaneously.

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

Reduced effort using Illumio ZTS compared to traditional segmentation methods.

90%

KEY STATISTICS

Return on investment (ROI)
111%

Net present value (NPV)
$5.4M

Forrester interviewed six representatives with experience using Illumio ZTS to better understand the benefits, costs, and risks associated with this investment. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global, multibillion-dollar conglomerate with B2B and B2C sales channels.

Prior to using Illumio ZTS, the interviewees noted how their organizations leveraged a traditional approach to network security by securing a hardened outer perimeter while leaving their internal networks relatively flat, open, and soft. However, prior attempts at segmentation with barriers inside the network yielded limited success. This left their organizations with large, sprawling networks that utilized multiple hardware vendors with a myriad of software tools for management, as well as disparate security and policy enforcement. These limitations made it expensive and challenging to adopt segmentation with the scale, flexibility, and granularity they required, and

ultimately left these organizations potentially exposed to a significant security event should their perimeter defenses be breached.

After the investment in Illumio ZTS, the interviewees were able to quickly gain visibility into network traffic, immediately shut off ports that are the most common ransomware vectors, and work with application owners to update policies, restrict internal communication, and segment and secure high-value assets. Key results from the investment include operational efficiency gains for infosec and network teams, significantly reduced impact of a data breach, reduced outages and downtime, along with cost savings and architectural advantages related to Illumio ZTS adoption.

KEY FINDINGS

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

- **Increased operational efficiency gains for infosec teams saving $1.6 million.** Illumio's simplified approach to segmentation reduced the time and effort to implement Zero Trust Segmentation policies, saving the composite organization 90% in security operations labor. Over three years, the increase in efficiency is worth more than $1.6 million.
- **Decreased overall risk exposure worth $1.8 million.** With Illumio ZTS, lateral movement is prevented within the network, reducing the severity of impact, or the blast radius, of a breach by 66%. Risk reduction benefits from Illumio ZTS are also critical for compliance and business requirements. Additionally, security operations center (SOC) teams use insights from Illumio ZTS to aid with incident investigations. The decrease in overall risk exposure enables savings of $1.8 million over three years.
- **Reduced cost and impact of downtime by $3.8 million.** Minimizing the impact of a data breach also minimizes downtime for end users and revenue-generating applications. The composite organization is also able to reduce unplanned downtime related to general network activities like migrations, updates, and patches. Reducing downtime with Illumio ZTS saves the composite organization a total of $3.8 million.
- **Tool consolidation and reduced firewall costs totaled $3 million.** The composite organization can repurpose and reduce costs associated with traditional network segmentation, thus saving $3 million.

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

- **Improved institutional knowledge.** IT workers and application owners have a better understanding of the network architecture, as well as how the applications and systems relate to each other and communicate.
- **Satisfies current and future cybersecurity insurance requirements.** Microsegmentation with Illumio ZTS exceeds any standards that cyber insurance providers require.
- **Regulatory compliance benefits.** Visibility into all network traffic makes it easier to prove compliance and troubleshoot issues.
- **Improved accuracy and granularity of configuration management database (CMDB).** Interviewees can synchronize Illumio ZTS visibility data with their CMDB to produce a more accurate catalog of all network assets.

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

- **Licensing and service contracts.** Illumio's pricing consists of licensing and service costs. The composite organization deploys just over 16,500 Virtual Enforcement Nodes (VENs) in a mix of visibility and enforcement mode along with

associated support contracts to support the entire ZTS initiative. This amounts to a PV cost of $4.3 million over three years.

- **Implementation and ongoing costs.** Illumio offers ease in implementation and management. Implementation and ongoing costs total $486,000 over three years.

The representative interviews and financial analysis found that a composite organization experiences benefits of $10.2 million over three years versus costs of $4.8 million, adding up to a net present value (NPV) of $5.4 million and an ROI of 111%.

"Illumio immediately gave us a return on the investment by providing that level of visibility into what was going on in our data centers and what was going on between our servers."

Cybersecurity engineer, logistics

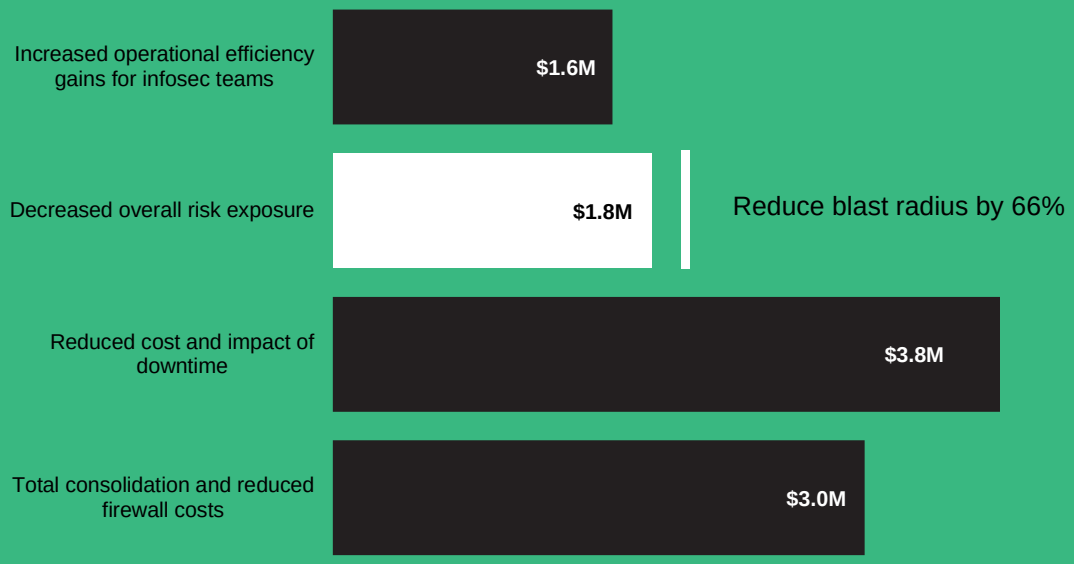
ROI
111%

BENEFITS PV
$10.2M

NPV
$5.4M

PAYBACK
6 months

Benefits (Three-Year)



“Illumio allowed us to secure our most critical assets that we felt were previously exposed.”

— Head of cyber defense, financial services

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 Illumio ZTS.

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 Illumio ZTS can have on an organization.

The Illumio ZTS Customer Journey

Drivers leading to the Illumio ZTS investment

Interviews

Role	Industry	Region	Revenue	Number Of Employees
IT technician	Manufacturing	Headquartered in Europe	$3 billion	20,000
Head of cyber defense	Financial Services	Headquartered in Australia	$12 billion	40,000
Cybersecurity engineer	Logistics	Headquartered in North America	$90 billion	250,000
Director of infrastructure	Law	Headquartered in North America	$500 million	1,500
Head of security strategy	Insurance	Headquartered in Australia	$20 billion	12,000
Senior executive	Software	Headquartered in North America	$25 billion	74,000

KEY CHALLENGES

Interviewees reported that prior to their investment in Illumio ZTS, their networks were flat and heavily interconnected. Cybersecurity efforts prior to Illumio ZTS were focused on protecting the outside perimeter instead of internal segmentation. Interviewees also referenced their lack of visibility into network traffic and how data was flowing.

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

- **Traditional segmentation was expensive and labor intensive to set up and manage.** The cost of doing segmentation using traditional or legacy firewall segmentation methodology was expensive, labor intensive, and difficult to manage once implemented. Many of the interviewees stated that it would be near impossible to adopt segmentation methodologies in their prior state. Segmenting at scale was also particularly difficult for many of the organizations.

  The senior executive in the software industry explained: “With Illumio, our security engineering teams were able to build automated tools to orchestrate and deploy network policies. Without Illumio, the engineering efforts would have been tied up with hardware evaluations, policy deployment workarounds and that sort of thing.”

- **Lack of visibility into network communications.** Application owners, security teams, and network engineers had no clear way to monitor or view network traffic and therefore did not know exactly what and how applications were communicating, or what access was

> **“Like most organizations, we traditionally had a flat network internally. We have a perimeter that is pretty hardened, and then we had an internal network that was very soft, gooey, flat and interconnected.”**
>
> *Head of cyber defense, financial services*

permitted. This lack of visibility made it difficult to monitor data flows, posing a serious security risk.

The head of cyber defense in the financial services industry said: “From a security point of view, we were always concerned that should there be a breach, how would we know? How would we know what they talked to and when? We didn’t know how we would be able to reconstruct that timeline.”

The IT technician in the manufacturing industry said: “One really good thing with Illumio ZTS is that it gives us a clear representation of our network and gives us good documentation of what is actually happening in the network. We did not have this capability before.”

- **Previous environments consisted of old, new, and disparate technologies.** Interviewees’ networks had grown over multiple years and acquisitions, hence the need for a segmentation solution that was vendor- and technology-agnostic, and would function across a wide range of environments and appliances.

  The architecture strategist in the insurance industry noted: “Our network grew organically over twenty years through multiple acquisitions — we had one of everything. A host-based solution was the clear fit for what we had and where we were going, and we are very happy with what Illumio has done for us.”

  The director of infrastructure in the legal industry shared: “We needed something that would work well no matter the platform. We’re going to always have some sort of on-prem footprint for various reasons, and we absolutely want to leverage the cloud, so I wanted a product that would work regardless of on-prem or in the cloud, and I found that Illumio gave me that flexibility.”

“We know that a security breach is going to occur so we use Illumio to limit the ability for the adversary to move laterally through the network, and to disrupt the standard techniques they use.”

Head of cyber defense, financial services

WHY ILLUMIO ZTS?

The interviewees’ organizations searched for a solution that could:

- **Provide vendor- and technology-agnostic deployment.** Interviewees said their organizations used Illumio ZTS to secure their environment regardless of their underlying hardware and technology infrastructure. Interviewees also mentioned how quick and easy it is to deploy Illumio ZTS.

  The cybersecurity engineer in the logistics industry explained, “For us, what pushed Illumio ahead of their competitors was that Illumio is vendor agnostic to the environments it supports.”

- **Provide a scalable solution to segmenting their environment.** Interviewees cited scalability as a main reason for choosing Illumio over alternative solutions, as it was less costly and time-consuming to deploy on a large scale and had more potential to succeed at scale. The sheer number of virtual or physical firewalls required for segmentation and the action necessary to enact and enforce policies was daunting to many interviewees. However, Illumio ZTS could be rapidly deployed across thousands of servers with far less time and money spent than alternatives.

The senior executive in the software industry shared, “Illumio was the solution that scaled as the workloads in our data centers expanded, and we could automatically orchestrate that scaling as opposed to having to try to run around and constantly do the capacity management and then track things after the fact.”

“The alternatives to Illumio cannot be scaled up to bigger environments — it just becomes unworkable.”

Head of cyber defense, financial services

- **Enforce Zero Trust methodologies.** Interviewees recognized Illumio ZTS as a Zero Trust solution that supports the other Zero Trust initiatives they are working on at their organizations. Additionally, interviewees recognized that Illumio ZTS is a future-proof solution because it is flexible and aligns with Zero Trust methodologies on mitigating the damage caused by breaches.

  The director of infrastructure in the legal industry said, “We ended up with Illumio because their methodology was Zero Trust, [which] was a requirement for both my team and the security team.”

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 six interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. It is a global, multibillion-dollar conglomerate with B2B and B2C sales channels. It has global operations with multiple lines of business and is subject to regulations and data laws in the US, Europe, and APAC. The composite organization leveraged a traditional approach to network security, a hardened perimeter with little internal controls.

The composite organization had a proliferation of homegrown applications and microservices, many of which had dependencies across the network — in the cloud and on-premises. It was pivotal to find a way to ensure that the exploitation of a vulnerability in one of these resources could not potentially expose the rest of the network to threat actors. Developers and operations teams would need to be brought into the conversation and embrace a new Zero Trust paradigm.

Deployment characteristics. The composite organization has global operations across three data centers and over 16,000 servers. There are 30 FTEs who are end users of Illumio ZTS and leverage the platform regularly. They initially deployed Illumio ZTS in visibility mode across the entire network, segmenting critical applications to protect high-value assets before moving on to the rest of the network.

Key Assumptions

- **Global, multibillion-dollar conglomerate**
- **Three data centers and 16,000 servers**
- **30,000 FTEs**

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	Increased operational efficiency gains for infosec teams	$1,066,542	$484,792	$290,875	$1,842,209	$1,588,777
Btr	Decreased overall risk exposure	$459,630	$766,050	$1,011,186	$2,236,866	$1,810,663
Ctr	Reduced cost and impact of downtime	$1,044,225	$1,617,975	$2,003,535	$4,665,735	$3,791,750
Dtr	Tool consolidation and reduced firewall costs	$2,437,934	$597,606	$416,164	$3,451,704	$3,022,863
	Total benefits (risk-adjusted)	**$5,008,331**	**$3,466,423**	**$3,721,760**	**$12,196,514**	**$10,214,053**

INCREASED OPERATIONAL EFFICIENCY GAINS FOR INFOSEC TEAMS

Evidence and data. Interviewees noted how Illumio ZTS easily deployed to all of their organization's servers and endpoints, providing immediate visibility into all network traffic and improving institutional knowledge about how their network operates.

- Illumio ZTS provides a real-time application dependency map that gives interviewees visibility into their network traffic that was not possible with legacy tools. The head of cyber defense in the financial services industry explained, "Illumio was the first time we were able to see flows end-to-end between workloads and be able to see what's going on."
- Security was a top priority, but having flexibility was also important. The director of infrastructure in the legal industry said, "While Illumio is keeping us safe, it also allows us to have a certain amount of fluidity in the network, which is important because we implement a lot of new products every year."
- Zero Trust was also top of mind of course, as organizations sought to implement controls earlier in the attack chain to mitigate potential incidents. This is effectively a dead end for many organizations as they found it too difficult to enact Zero Trust using traditional firewalls and stop-gap measures.
- All the interviewees were looking for a Zero Trust solution that was flexible enough to leverage their current infrastructure while helping them plan for the future. The senior executive in the software industry said: "We used Illumio to retrofit our existing infrastructure. This was an opportunity to buy some Zero Trust on the cheap."

> **"The biggest benefit in my opinion has been the amount of education and learning that everyone that's involved in this project has gained as a result of looking at the visibility data."**
>
> *Cybersecurity engineer, logistics*

- Illumio also helps organizations more efficiently implement and maintain segmentation. The director of infrastructure in the legal industry explained, “With traditional firewalls, we would need to add at least two to three network engineers because if we had to do everything with access control lists on switches, it would be a nightmare to manage and it would be a nightmare to document.”

Modeling and assumptions. For the financial model, Forrester assumes:

- A significant amount of labor is budgeted to segment its network using legacy strategy.
- Using Illumio for Zero Trust Segmentation, including microsegmentation, reduces the effort for infosec professionals to install and successfully manage the segmented network by 90%.
- The composite organization can only achieve 40% of the segmentation work with firewalls compared to what was possible with Illumio.
- Fully loaded hourly salary for infosec team is $68.15 per hour.

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

- Capabilities of existing technology to perform and manage segmentation.
- Salary for the infosec team.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.6 million.

Increased Operational Efficiency Gains For Infosec Teams

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Baseline time to do segmentation and maintain policies via traditional firewalls (hours)	Interviews and Forrester metrics	45,760	20,800	12,480
A2	Reduction in time using Illumio for segmentation implementation	Interviews	90%	90%	90%
A3	Likelihood of completing segmentation with traditional appliances	Interviews and Forrester metrics	40%	40%	40%
A4	Effort saved using Illumio for policy management and segmentation (hours)	A1*A2*A3	16,474	7,488	4,493
A5	Infosec and network engineer fully loaded hourly compensation	TEI standard	$68.15	$68.15	$68.15
At	Infosec efficiency gains	A4*A5	$1,122,676	$510,307	$306,184
	Risk adjustment	↓5%			
Atr	Infosec efficiency gains (risk-adjusted)		$1,066,542	$484,792	$290,875
	Three-year total: $1,842,209			**Three-year present value: $1,588,777**	

DECREASED OVERALL RISK EXPOSURE

Evidence and data. Interviewees had a "not if but when" mindset, recognizing that preventing a breach is no longer realistic. With that in mind, interviewees were confident that Illumio ZTS' visibility and segmentation capabilities significantly reduced their vulnerability and severely limited the impact of a potential breach by preventing lateral movement within their network.

- One interviewee felt comfortable hosting multiple, distinct businesses all in the same environment because they were able to use Illumio ZTS to segment each business. With this approach, the organization leverages only one tool (i.e., Illumio) and one network to host and protect over 60 different businesses.

  The IT technician in the manufacturing industry said, "Illumio has been a game changer for us and has allowed us to leverage our large environment to host many companies while still having granular controls over policies and network traffic."
- The head of cyber defense in the financial services industry discussed how Illumio ZTS works as a great deterrent as it forces bad actors out of their comfort zone: "Illumio provides us with a means to create and protect distinct islands in our network. If we have an adversary, it means the adversary has to work harder and has to make a decision as to whether they will continue to try and breach our network and potentially risk exposure because they will be going outside their normal operating procedures, or they just roll over and go, 'You know what? We're going to move on to the next one.'"

"One key benefit is Illumio's value in reducing the likelihood of internal compromises moving laterally and spreading out. It's been very effective in preventing lateral movement — it's a very effective control."

Head of security strategy, insurance

"We see Illumio's risk reduction impact during our investigation process. We can look at minor incidents and say they were minor because of the way that we have this environment kitted out with Illumio segmentation."

Senior executive, software

Modeling and assumptions. For the financial model, Forrester assumes:

- The average number of breaches experienced annually is two and a half, costing potentially $1.8 million for the incidents. These costs include: response and remediation costs, notification costs to affected parties, regulatory fines, customer compensation, customer lawsuits and punitive damages, audit and security compliance costs, lost revenue, cost to rebuild brand equity, and the cost to acquire new customers.
- With Illumio ZTS fully implemented, the blast radius of a breach is reduced by 66% through restricting lateral movement.
- The segmentation provided by Illumio is effective against 50% of attacks based on the most likely attack vectors leading to a breach. Forrester does not assume that a Zero Trust approach has

been taken across the entirety of the network so certain types of attacks may not be impacted by segmentation, such as lost or stolen credentials.

- Realizing the benefits of risk reduction requires input from people and updated processes which account for a portion of the financial benefits. Illumio is responsible for 75% of this benefit, with people and processes accounting for the other 25%.

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

- The frequency and cost of a data breach.
- The specific characteristics and security posture prior to deploying Illumio.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.8 million.

Decreased Overall Risk Exposure

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Likely number of breaches annually	Forrester internal metrics	2.5	2.5	2.5
B2	Cost of a material breach (specific costs listed in write-up)	Forrester internal metrics	$1,815,822	$1,815,822	$1,815,822
B3	Reduced blast radius of a breach with Illumio	Interviews	30%	50%	66%
B4	Percentage of data breaches impacted by microsegmentation	Forrester internal metrics	50%	50%	50%
B5	Illumio attribution	Interviews and Forrester metrics	75%	75%	75%
Bt	Decreased risk exposure	B1*B2*B3*B4*B5	$510,700	$851,167	$1,123,540
	Risk adjustment	↓10%			
Btr	Decreased risk exposure (risk-adjusted)		$459,630	$766,050	$1,011,186
	Three-year total: $2,236,866			**Three-year present value: $1,810,663**	

REDUCED COST AND IMPACT OF DOWNTIME

Evidence and data. With Illumio ZTS, organizations are better protected against downtime related to breaches and experience significantly less unexpected downtime related to manual errors.

- One organization experienced first-hand how effective Illumio ZTS is at preventing a significant breach and keeping their business up and running. The director of infrastructure in the legal industry explained: “When we experienced our breach, Illumio allowed us to shut off access to our network completely after applying a single policy to the affected systems. This immediately ended the attack.”

“If we experienced this same event without Illumio, at least two to three times more systems would have been impacted, creating a much more significant issue.”

Director of infrastructure, legal

- The senior executive in the software industry explained: “The automation of that environment with Illumio has led to an enormous, almost complete reduction in outages caused by manual error. We’re not doing all the policy deployment workaround with human beings who are prone to errors, so we are not going to eat the cost associated with human-induced outages anymore. Illumio helped solve a big problem for us.”
- The head of cyber defense in the financial services industry described how Illumio helped prevent frequent and disruptive downtime during segmentation work: “With the traditional approach, we were seeing massive interruptions to systems when we went to do the segmentation work. It was a very slow process. You can burn through a lot of money in a short period of time and not see a lot of value for it.”

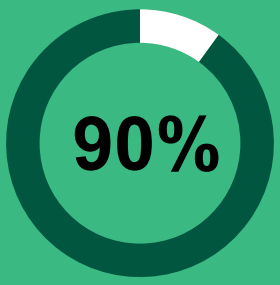
“Our MSSP told us they had never seen any of their other clients shut down an attack in that short a period of time and as efficiently, which was one of the main reasons there was no exfiltration of any data from the firm.”

Director of infrastructure, legal

Modeling and assumptions. For the financial model, Forrester assumes:

- The composite organization reduced the impact of a data breach by 66%, as outlined in the previous benefit.
- Each breach impacts 10% of internal users, causing 3.6 hours of downtime per user.
- The average fully loaded hourly salary is $40 per hour.
- An hour of outage costs the business $240,000.
- There was a monthly unplanned outage lasting an average of 72-minutes prior to adopting Illumio ZTS.
- With Illumio ZTS, the frequency of these unplanned outages is reduced by 50% in Year 1, increasing to 90% in Year 3 when the full network is mapped and segmented.
- Fifty percent of the outage reduction is attributed to Illumio ZTS and the other 50% to the people and processes put in place around Illumio ZTS to prevent outages.

Reduced unplanned outages from segmentation work, migration, and other IT activities.



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

- The specific deployment characteristics impacting the reduction in data breach impact.
- The percentage of impacted employees and average downtime associated with a breach.
- The amount of lost revenue per hour of downtime.
- The frequency and duration of unplanned outages.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $3.8 million.

Reduced Cost And Impact Of Downtime					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Total number of employees	Composite	30,000	30,000	30,000
C2	Breaches per year	B1	2.5	2.5	2.5
C3	Percentage of internal users impacted by each breach (of 30,000 FTE)	Forrester internal metrics	10%	10%	10%
C4	Average fully burdened hourly rate of general employee	TEI standard	$40	$40	$40
C5	Downtime induced by breaches, in hours	Forrester internal metrics	3.6	3.6	3.6
C6	Subtotal: Cost of breach-related employee downtime annually	C1*C2*C3*C4*C5*B3*B4*B5	$121,500	$202,500	$267,300
C7	Revenue lost per hour of outage	Interviews	$240,000	$240,000	$240,000
C8	Subtotal: Cost of breach-related production downtime	C2*C5*C7*B3*B4*B5	$243,000	$405,000	$534,600
C9	Frequency of unplanned outages linked to segmentation or trust policies in legacy environment (annually)	Composite	12.0	12.0	12.0
C10	Average length of unplanned outage (hours)	Composite	1.2	1.2	1.2
C11	Reduction in unplanned outages with Illumio	Composite	50%	75%	90%
C12	Attribution to Illumio	Composite	50%	50%	50%
C13	Subtotal: Cost of unplanned outages with legacy environment	C7*C9*C10*C11*C12	$864,000	$1,296,000	$1,555,200
Ct	Reduced cost and impact of downtime	C6+C8+C13	$1,228,500	$1,903,500	$2,357,100
	Risk adjustment	↓15%			
Ctr	Reduced cost and impact of downtime (risk-adjusted)		$1,044,225	$1,617,975	$2,003,535
	Three-year total: $4,665,735			**Three-year present value: $3,791,750**	

TOOL CONSOLIDATION AND REDUCED FIREWALL COSTS

Evidence and data. Illumio ZTS is infrastructure-agnostic, allowing organizations to take advantage of existing infrastructure and repurpose some of their legacy technology to support the new, Zero Trust architecture enabled by Illumio.

- All interviewees were looking for a Zero Trust solution that could be used with existing technologies and avoid a large, multimillion-dollar capital expenditure project to update their network architecture.

The IT technician in the manufacturing industry shared: “A big benefit of Illumio is that we can deploy it fast using our existing infrastructure. We used our built-in firewalls on each workload to achieve Zero Trust Segmentation in the server network. This was the fastest, most cost-effective way to achieve Zero Trust with the fewest amount of labor hours.”

- The head of cyber defense in the financial services industry explained: "We deployed our initial use cases wherever we had legacy infrastructure that we couldn't remediate in a short period of time. Effectively, the first thing we did was wrap Illumio around and microsegment that heritage and legacy infrastructure to provide those assets with much better levels of protection."
- Illumio also helped organizations avoid additional expenditure. The cybersecurity engineer in the logistics industry explained, "We avoided having to purchase a bunch of firewalls because we're using Illumio as that compensating control."
- One interviewee estimated a $31 million dollar capital expenditure if their organization did not use Illumio for Zero Trust Segmentation — and even at that cost, they would not get the same visibility and segmentation capabilities that Illumio provides.

Modeling and assumptions. For the financial model, Forrester assumes:

- The composite organization can repurpose $1.5 million worth of their legacy firewall deployment and associated maintenance costs, and recapture $1.2 million in Zero Trust Segmentation labor in Year 1.

> **"Without Illumio, we would have had to spend $31 million in new hardware to secure our environment. From a cost and logistics point of view, that was untenable. A firewall is not a set-and-forget type of device, either. It requires care and feeding to properly function and has ongoing support costs."**
>
> *Head of cyber defense, financial services*

- In Years 2 and 3, the amount of recaptured labor declines as Illumio adds net-new capabilities.

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

- Legacy technology and legacy architecture.
- Skillset and knowledge base of existing IT team.
- Level of maturity of Zero Trust architecture prior to deployment.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $3 million.

Tool Consolidation And Reduced Firewall Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Firewall investment repurposed	Interviews	$1,500,000	$150,000	$150,000
D2	Repurposed Zero Trust and segmentation work	A1*A3*A5	$1,247,418	$567,008	$340,205
D3	Repurposed maintenance costs of firewalls	20% of hardware	$300,000	$30,000	$30,000
Dt	Tool consolidation and reduced firewall costs	D1+D2+D3	$3,047,418	$747,008	$520,205
	Risk adjustment	↓20%			
Dtr	Tool consolidation and reduced firewall costs (risk-adjusted)		$2,437,934	$597,606	$416,164
	Three-year total: $3,451,704			**Three-year present value: $3,022,863**	

UNQUANTIFIED BENEFITS

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

- **Improved institutional knowledge.** The cybersecurity engineer in the logistics industry explained: "For me, the biggest benefit is the body of knowledge that Illumio has been able to provide to not only the infosec team but to the infrastructure and app development teams as well. Our app owners now have an idea of where and how their applications communicate and can address potential vulnerabilities."
- **Satisfies cybersecurity insurance requirements.** Interviewees felt that current cyber insurance providers were not looking deep enough at organizations' segmentation and were confident that Illumio exceeded any requirements from insurance providers. The IT technician in the manufacturing industry said: "The insurance companies do not yet understand the importance of microsegmentation and the vulnerabilities that exist between unsegmented systems. They just don't quite understand the detailed picture yet."
- **Regulatory compliance benefits.** Security regulations are getting stricter as governments and other regulating bodies try to keep up with the evolving threat landscape. Interviewees felt that Illumio will help them comply with any regulations around segmentation and make it easier to prove that they are compliant. The head of cyber defense in the financial services industry said, "We can use Illumio to help certify to a regulator that, when we did our disaster recovery (DR) test, or our pen-test, our controls were actually working as intended."
- **Improved accuracy of CMDB.** With Illumio providing visibility and fidelity into all network traffic, the data that Illumio generates can be used to audit and continuously update the CMDB to ensure that it has an accurate catalog of all network assets.

FLEXIBILITY

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

- **Extremely granular segmentation controls down to each individual computer.** The IT technician in the manufacturing industry noted: "To gain even more use of Illumio, we are thinking about implementing Illumio on every computer. Right now, we only have it on servers. But we are thinking about implementing on end users' computers. That will give us Zero Trust Segmentation between different computers as well as the servers in various environments."
- **Ability to identify critical assets in the network.** The head of cyber defense in the financial services industry said, "We have integrated vulnerability scanning data in with Illumio's vulnerability maps and the network's information flow that Illumio provides so we can now get criticality assessments of our workloads…based on network flows that we can see."
- **Being cloud-agnostic.** The director of infrastructure in the legal industry said: "One of the things I like about Illumio is it was really cloud-agonistic to a large degree. While today I primarily use one public cloud, down the road I may have some workloads in a different one. It's nice to have that future flexibility."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Illumio licensing and service contracts	$1,516,008	$0	$1,705,509	$1,895,010	$5,116,528	$4,349,269
Ftr	Implementation and ongoing costs	$86,161	$154,973	$164,275	$164,275	$569,684	$486,232
	Total costs (risk-adjusted)	$1,602,169	$154,973	$1,869,784	$2,059,285	$5,686,211	$4,835,501

ILLUMIO LICENSING AND SERVICE CONTRACTS

Evidence and data. Illumio breaks costs into two buckets, base licensing costs for Illumio and a service contract.

- Interviewees noted how their organization's boards and executives typically viewed Illumio as a necessary cost to secure their networks and prevent a significant breach, and paid for itself by preventing lateral movement within the network.
- Some organizations had experienced data breaches with and without Illumio. They knew first-hand how effective it was at preventing loss and limiting blast radius, which justified cost factors.
- Most organizations provided frequent updates to their board on the Illumio deployment, highlighting new visibility capabilities, percentage of segmented estate, among other metrics.
- Organizations typically started with Illumio in visibility mode and then deliberately built out enforcement based on where critical data and applications were located. This approach increases costs over time while also increasing the level of security and protection.

Modeling and assumptions. For the financial model, Forrester assumes:

- The composite organization starts with everything in visibility mode during the initial deployment and slowly adds enforcement as they segment and lock down high-value assets.
- The composite organization leverages Illumio's support services while they map, segment, and enforce security policies across the network.

Risks. This cost may vary due to:

- The specific technology stack deployed in the legacy network environment.
- The level of service and strategic planning required.

Results. To account for these risks, Forrester adjusted this cost upward by 8%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.3 million.

Illumio Licensing And Service Contracts						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Cost of base Illumio license	Vendor	$1,087,876	$0	$1,263,340	$1,438,804
E2	Support contract	Vendor	$315,835	$0	$315,835	$315,835
Et	Illumio licensing and service contracts	E1+E2	$1,403,711	$0	$1,579,175	$1,754,639
	Risk adjustment	↑8%				
Etr	Et (risk-adjusted)		$1,516,008	$0	$1,705,509	$1,895,010
	Three-year total: $5,116,528			**Three-year present value: $4,349,269**		

IMPLEMENTATION AND ONGOING COSTS

Evidence and data. By all accounts, deploying Illumio ZTS is extremely fast, easy, and does not require extra bandwidth or impact network performance.

- One organization deployed Illumio across their network without notifying anyone, and none of the application owners ever noticed until the IT team shared the newly created application dependency map.
- All interviewees said that deploying Illumio was significantly cheaper, faster, and less complicated than deploying an alternative solution using hardware.
- Visibility, Zero Trust, and segmentation are critical projects for the interviewees. Their businesses also expected and budgeted for headcount in order to deploy Illumio and secure their critical assets.
- Illumio improves institutional knowledge about how the network operates and how individual applications work, benefiting individual application owners and network and security teams.

Modeling and assumptions. For the financial model, Forrester assumes:

- The initial implementation and deployment of Illumio took just under 350 hours to achieve greater visibility and to secure high-value assets with ZTS policies.
- The average fully loaded hourly salary for the implementation team is $68.15 per hour.
- There are 750 application owners, each holding responsibility for the various connections associated with their applications across the network.
- Application and services owners were needed to adhere to the new policies, which occasionally included reworking slight codes and process adjustments.
- Overall, the time spent initially is expected to be near 1,100 hours, with administration hours to be the equivalent of one FTE in ensuing years.

Risks. This cost may vary due to:

- Geographical footprint of the organization and the accompanying infrastructure.
- Network architecture, where cloud, multicloud, and hybrid environments come into play.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $486,000.

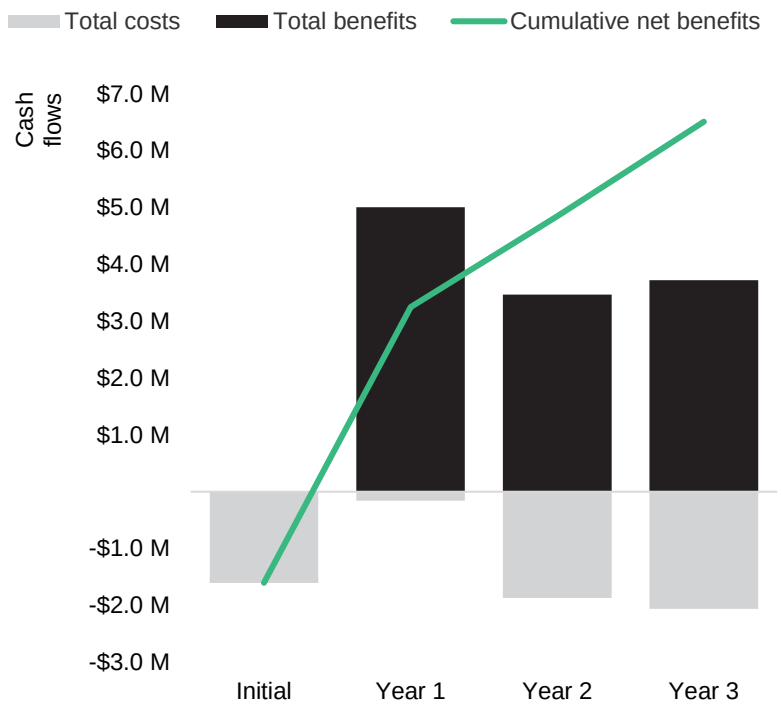
Implementation And Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Internal implementation labor hours	Interviews	347	0	130	130
F2	Ongoing maintenance and administration efforts, in hours	Interviews	0	2,080	2,080	2,080
F3	Internal labor cost per hour for infrastructure engineers and infosec analysts	TEI Standard	$68.15	$68.15	$68.15	$68.15
F4	Internal training cost per hour for service or app owners	Interviews	750	75	75	75
F5	Service owner cost per hour	Interviews	$77.88	$77.88	$77.88	$77.88
Ft	Implementation and ongoing costs	F1+F2)*F3+(F4*F5)	$82,058	$147,593	$156,453	$156,453
	Risk adjustment	↑5%				
Ftr	Implementation and ongoing costs (risk-adjusted)		$86,161	$154,973	$164,275	$164,275
	Three-year total: $569,684			**Three-year present value: $486,232**		

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	($1,602,169)	($154,973)	($1,869,784)	($2,059,285)	($5,686,211)	($4,835,501)
Total benefits	$0	$5,008,331	$3,466,423	$3,721,760	$12,196,514	$10,214,053
Net benefits	($1,602,169)	$4,853,358	$1,596,639	$1,662,474	$6,510,303	$5,378,552
ROI						111%
Payback period (months)						6 months

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.

Appendix B: Supplemental Material

Related Forrester Research

“Best Practices For Zero Trust Microsegmentation,” Forrester Research, Inc., June 27, 2022.

“The Forrester New Wave™: Microsegmentation, Q1 2022,” Forrester Research, Inc., March 10, 2022.

“The Forrester Tech Tide™: Zero Trust Threat Prevention, Q4 2022,” Forrester Research, Inc., October 21, 2022.

“Mitigating Ransomware With Zero Trust,” Forrester Research, Inc., August 20, 2021.

Appendix C: 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.


FORRESTER®