FORRESTER®

The Total Economic Impact™ Of Cisco Security Suites For Zero Trust

Cost Savings And Business Benefits Enabled By *Security Suites For Zero Trust*

A Forrester Total Economic Impact™ Study
Commissioned By Cisco, March 2025

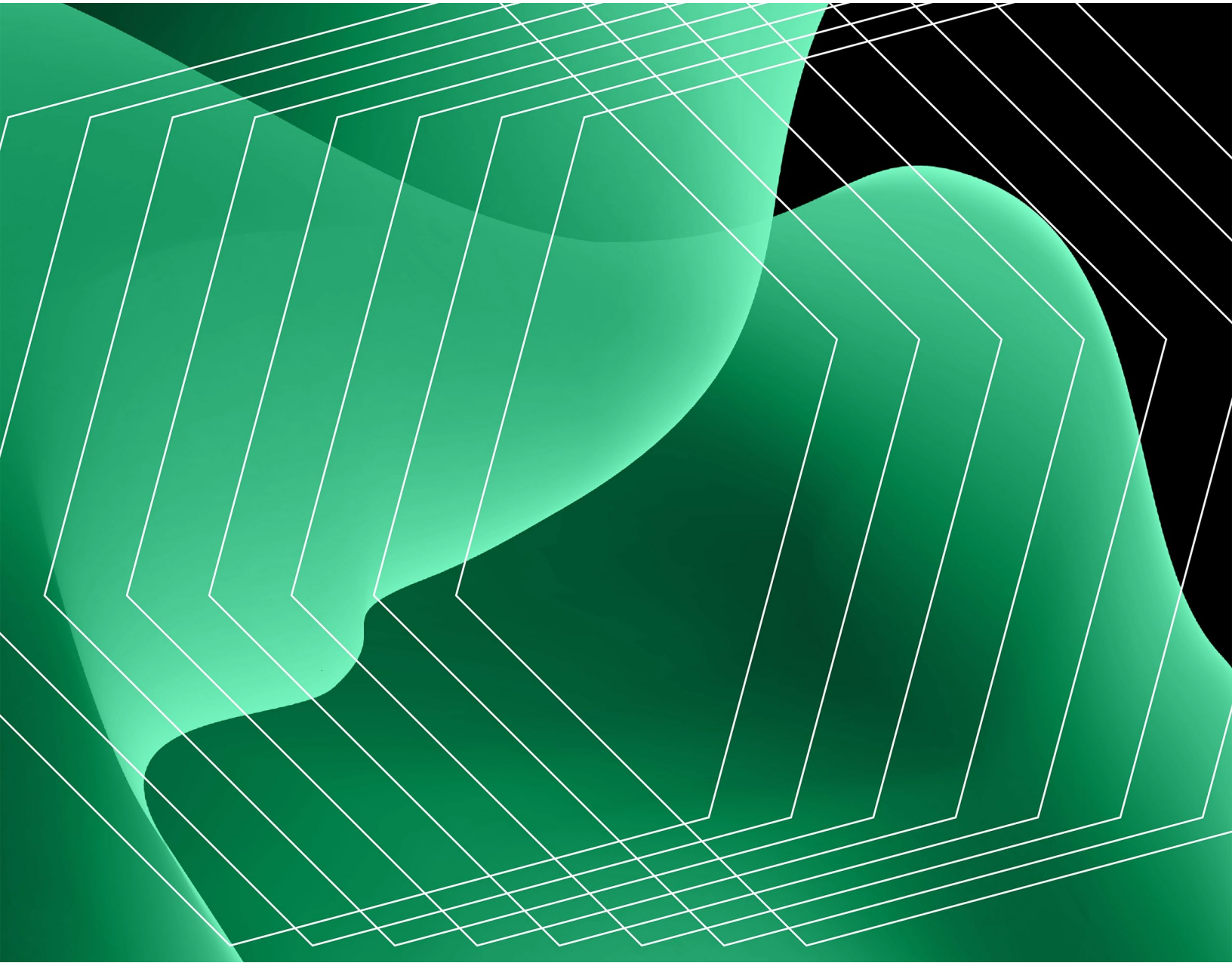


Table Of Contents

Consulting Team:

Courtenay O'Connor

ABOUT FORRESTER CONSULTING

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

Executive Summary

Today, 74% of global security decision-makers say their organizations are adopting Zero Trust.[1] Coined by Forrester Research in 2009, Zero Trust is a security strategy of explicit policy enforcing least-privilege access and inspecting and monitoring everything.[2] Investments in Zero Trust help organizations reduce the impacts of a material breach, transform technology architecture, and boost customer and employee experience for growth.[3]

Cisco Security solutions integrate to enable a Zero Trust architecture across users, devices, networks, cloud, endpoints, and email, including:

- The User Protection Suite, which facilitates secure users' access to applications, cloud services, and communication tools.
- The Breach Protection Suite, which empowers security teams to simplify operations and accelerate response across the most prominent attack vectors, including email, endpoints, network, and cloud.

Cisco commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Cisco Security Suites as part of their Zero Trust strategy.[4] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cisco Security Suites on their organizations.

Return on investment (ROI)
110%

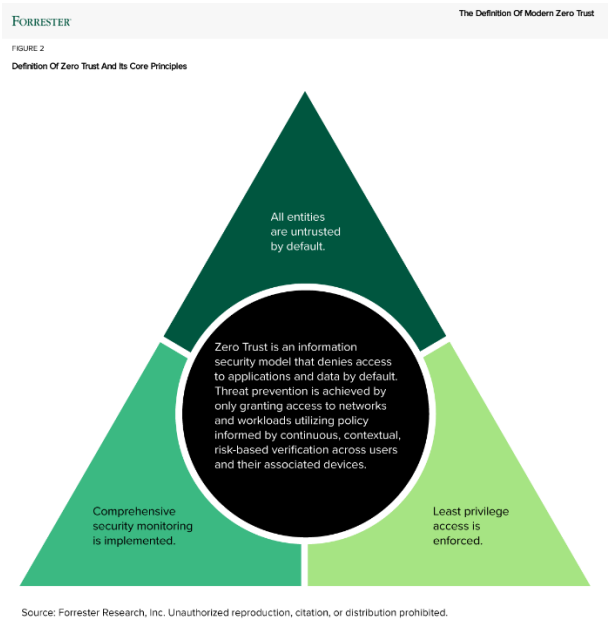
Net present value (NPV)
$2.34M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives with experience using Cisco Security Suites For Zero Trust. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization with 5,000 FTEs globally and revenue of $2 billion per year.

Interviewees said that prior to using Cisco Security Suites for Zero Trust, their organizations' environments had decentralized user management procedures. Siloed application access security and management efforts were completed by business resources as well as technology resources. The goal of securing user privileges often served as an entry point into their organizations' journey toward Zero Trust architecture.

After investing in Cisco Security and rebuilding their technology environment using the pillars of Zero Trust, the interviewees reported significant cost savings and technology optimizations, including centralizing and automating functions for identity security and management. Key results from the investment include more secure and efficient user access to corporate resources, reduced volume of security incidents, and optimized support and remediation efforts.

Definition Of Zero Trust And Its Core Principles



Forrester's Zero Trust definition combines the original three principles of Zero Trust with the operational domains of ZTX.

Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates three core principles: All entities are untrusted by default; least-privilege access is enforced; and comprehensive security monitoring is implemented.

KEY FINDINGS

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

- **A 15% reduction in legacy costs by transitioning to Zero Trust architecture with Cisco Security, with a reduction of more than 3,000 hours of internal vendor management.** The composite transforms its networking and security stack around the principles of Zero Trust using the Cisco Security User Protection Suite Advantage and Breach Protection Suite Premier. Several drivers act to consolidate networking and security spend, including licensing optimization, software or software-as-a-service (SaaS) license and subscription savings, and hardware decommissioning cost savings. The streamlined technology environment mitigates agent sprawl and requires fewer labor hours to administer. For the composite, incorporating Zero Trust principles into its consolidated networking and security infrastructure with the User and Breach Protection suites saves $527,000.
- **A 70% reduction in labor hours for identity security and access management with Cisco Security.** The composite eliminates the unnecessary replication of identity security and management efforts with business resources. Instead, it automates key workflows with the Cisco Security Suites, leveraging only technical resources. Consolidating identity security and management with Cisco Security Suites allows business resources to reallocate more than 21,000 hours to higher-value activities, resulting in $934,000 of avoided and redundant identity security and management labor costs.
- **An 80% productivity improvement for networking and infrastructure operations.** With its transition to a Zero Trust architecture with Cisco Security Suites, the composite centralizes and automates previously manual network and infrastructure management workflows. Enabling Zero Trust principles in its effort to consolidate networking and security infrastructure with Cisco Security saves the composite organization $427,000.

- **A 50% reduction in resources needed to optimize for effective Zero Trust security management.** To meet the full needs of a Zero Trust environment with Cisco Security Suites, the composite automates key security workflows; adds layers of protection for users, devices, and apps; and improves visibility and adds bidirectional integrations with Cisco Security Suites and other vendor tools. These enhanced capabilities and time savings with Cisco Security Suites lead to security operations optimizations saving the organization $667,000.
- **A 60% reduction in the likelihood of a severe data breach, reducing the costs of a material breach.** The composite organization has a 91% likelihood of experiencing one or more serious data breaches per year in which the organization's sensitive data is potentially compromised, at an average potential cost of $4.1 million. With Cisco Security Suites deployed in alignment with Zero Trust principles, the composite reduces the likelihood of a severe data breach caused by an external attack by 60%. For the composite, enabling Zero Trust principles with Cisco Security helps the organization avoid $1.5 million in costs associated with a material breach.
- **More than 12,000 end-user hours recaptured from improved remote access workflows.** In the prior environment, the composite organization's 2,500 remote end users wasted four minutes per day due to friction in accessing services remotely. With Cisco Security Suites in alignment with Zero Trust best practices, the composite reduces the time it takes end users to access services remotely by 75%, with 25% of that recaptured time reallocated toward productive use. For the composite, enabling Zero Trust principles with Cisco Security regains $353,000 worth of productive hours for end users.
- **More than 11,250 IT tickets avoided with help desk optimization.** In the prior environment, the composite processed 7,500 IT support tickets, each of which took 10 minutes on average to resolve. With Cisco Security Suites and Zero Trust, the composite reduces related IT support ticket volume by 50%. For the composite, enabling Zero Trust principles with Cisco Security Suites saves the organization $27,000 in IT administration and help desk costs.

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

- More efficient mergers and acquisitions (M&A) activities.
- Reduced technical debt.
- Improved standing with cybersecurity insurance providers.

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

- **Cisco Security Enterprise Agreement.** The composite organization deploys the Cisco Security Breach Protection Suite Premier and User Protection Suite Advantage in a phased implementation alongside the introduction of Zero Trust best practices. By the end of the three-year period, the composite organization completes 70% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. Total Cisco Enterprise Agreement costs in this timeframe come to $1.7 million.
- **Implementation and training.** Over the multiyear transition, the composite dedicates internal technology resources to standing up and training in the new Cisco Security architecture to align with Zero Trust principles. It also relies on technical implementation support from Cisco's Software Support Service, included in the Security Suite. Three-year implementation and training costs for change management efforts related to Cisco Security and Zero Trust total $287,000.
- **Platform administration.** The composite organization partially dedicates technology resources to maintaining the Cisco Security architecture. These resources are further supported by Cisco's Software Support Service. For the composite, platform administration costs are $130,000.

The representative interviews and financial analysis found that a composite organization experiences benefits of $4.47 million over three years versus costs of $2.12 million, adding up to a net present value (NPV) of $2.34 million and an ROI of 110%.

80%

Percentage reduction in siloed network and infrastructure management labor with Cisco Security automations

"The big value [of Cisco Security Suites] is the huge time savings and actually having products that work together in an ecosystem where we understand them. They all have the same look and feel, even though they do different things, with the ability to natively integrate them all. The biggest return is the time it saves us from dealing with a lot of different point products to get the answers that we need."

VP OF IT SERVICES, CONSTRUCTION

Return on investment (ROI)

110%

Benefits PV

$4.47M

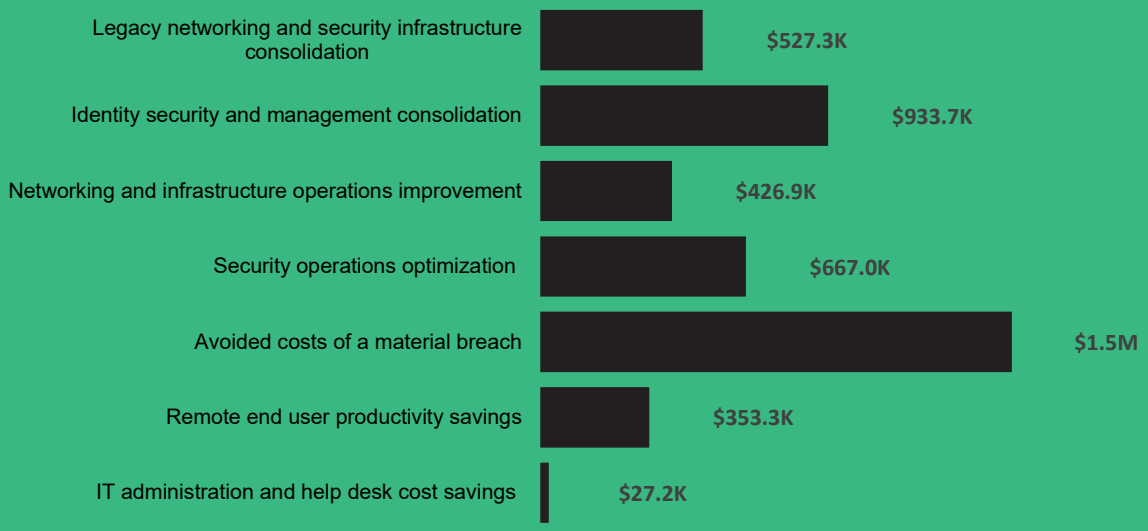
Net present value (NPV)

$2.34M

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 Cisco Security Suites.

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 Cisco Security Suites can have on an organization.

DISCLOSURES
Readers should be aware of the following:

This study is commissioned by Cisco and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Cisco Security Suites. For the interactive functionality using Configure Data/Custom Data, the intent is for the questions to solicit inputs specific to a prospect's business. Forrester believes that this analysis is representative of what companies may achieve with Cisco Security Suites based on the inputs provided and any assumptions made. Forrester does not endorse Cisco or its offerings. Although great care has been taken to ensure the accuracy and completeness of this model, Cisco and Forrester Research are unable to accept any legal responsibility for any actions taken on the basis of the information contained herein. The interactive tool is provided "as is," and Forrester and Cisco make no warranties of any kind.

Cisco reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

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

1. Due Diligence
Interviewed Cisco stakeholders and Forrester analysts to gather data relative to Cisco Security Suites for Zero Trust.

2. Interviews
Interviewed six people at organizations using Cisco Security Suites to obtain data about costs, benefits, and risks.

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

4. Financial Model Framework
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

5. Case Study
Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the Total Economic Impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Cisco Security Suites For Zero Trust Customer Journey

Drivers leading to the Cisco Security Suites For Zero Trust investment

Interviews			
Role	**Industry**	**Region**	**Total Users**
Senior IT infrastructure architect	IT services	Europe	500 to 999
Network enterprise architect	Oil and gas	Asia Pacific	5,000 to 9,999
Cybersecurity manager	B2C commerce	North America	5,000 to 9,999
Vice president, IT services	Construction	North America	5,000 to 9,999
Vice president, information technology	Real estate	North America	Fewer than 500
CIO	Legal services	North America	Fewer than 500

KEY CHALLENGES

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

- **Disjointed legacy software and infrastructure, leading to cost and labor inefficiencies.** Interviewees noted that their organizations' prior environments were not structured properly to help meet business goals or even to meet minimum security requirements. This required multiple and sometimes redundant point solutions and agents from many vendors and resulted in increased costs. The complexity inherent in these environments required excess labor to manage vendor relationships.
    - The senior IT infrastructure architect in the IT services industry pointed to the growing complexity of their organization's prior technology systems: "I think not only the traffic has grown, but the complexity has grown. I think in the last five to

six years, the complexity has at least doubled because of work granularity, systems, and fast implementation."

- The network enterprise architect in the oil and gas industry indicated that, in the prior environment, one of their organization's subsidiary companies, which was located in a smaller country, did not even have a VPN in place. When the COVID-19 pandemic hit in 2020, the interviewee pointed out that their organization was in need of a secure way to quickly and remotely connect users to corporate resources.

- **Identity security and access management cost inefficiencies and security gaps.** Identity security efforts were redundantly managed both by the business resources and technology resources. Business resources were responsible for identity security and access management related to core business apps, and technology resources were also involved in troubleshooting user problems and remediating user-driven security incidents, such as account takeovers. The cybersecurity manager in the B2C commerce industry told Forrester: "When COVID hit, the [number of] cloud apps just exploded. Everybody could [buy them with] corporate credit cards, and people were just all doing their own things. [We had to issue] a corporate mandate saying, 'You do not want to manage people's identities.'"
- **Siloed and manual efforts to manage outdated infrastructure, which slowed time to value and drained critical resources.** In the prior environment, interviewees indicated that their organizations' workflows to manage devices, manage infrastructure, and secure access to corporate resources and other cyber assets were manual, labor intensive, and prone to error. The cybersecurity manager in the B2C commerce industry highlighted the challenge for technical resources to have consistent capabilities across their infrastructure because of variability in security policies and functionality of legacy tools: "One of the biggest challenges we see with these point products is the policies aren't always consistent. And when they're not consistent, that means that you can do something over here that you can't do over there."
- **Ineffective security management.** Interviewees highlighted a lack of visibility into critical technology estates due to poorly configured environments. As a result, they had to manage their siloed infrastructure with insufficient, error-prone manual processes. The senior IT infrastructure architect in the IT services industry shared that the prior

environment was not really manageable because the things [our legacy vendor] provided were not really good for [what we needed], so you had to invent something to do it."

- **Material breaches and evolving threats that caused cascading costs to organizations.** Interviewees pointed out how their organizations' risk landscape had evolved and increased over time, as did their costs associated with security events. Commonly cited breach- and incident-causing vectors included ransomware, malware, and social engineering attacks. The senior IT infrastructure architect in the IT services industry shared: "Ransomware is top of the list [of threats to our organization] because it's omnipresent. This threshold is changing over time. Seven years ago, ransomware was relevant, but not like today. We have to adapt our thresholds regarding emerging threats."
- **Impediments to remote end-user productivity.** Interviewees' organizations had varying capabilities for secure remote work in their prior environments, although most lamented that the systems in place (if any) were often riddled with multiple steps that led to friction. The CIO at the legal services company shared: "Before the Zero Trust initiative, the company shut down [in the event of a breach or disaster]. There was no one there to do any work. People would go home but couldn't work from home because there was no mechanism by which that would work. They couldn't reliably try to use a VPN for the telephony system because it was messed up. There were deep technical issues that [meant] we were wholly unprepared for disaster."
- **IT administration and help desk cost inefficiencies due to excess issues from vectors listed above.** Legacy networking and security workflows caused errors and redundancies for IT administrators, networking and security resources, and end users alike. This inflated IT help desk ticket volumes with numerous issues. The CIO at the legal services company noted that their firm experienced difficulty with the prior VPN and antivirus security solutions from a legacy vendor: "It was an unmitigated disaster — just fly by the seat of their pants, running WMI scripts to try to do inventory. It was really bad because they were coming out of working with an MSP [managed service provider] that wasn't centralized. Tickets were handled [with no real standard operating procedures]."

> "Before the journey [toward Zero Trust with] Cisco Security, our biggest issue was that we had no single pane of glass to see what was happening in the network. We didn't know. [Our legacy solution] was good in what it did, but, again, we didn't have the visibility in the sense that you are flying a plane blind."
>
> NETWORK ENTERPRISE ARCHITECT, OIL AND GAS

> "[Ransomware threats] will quadruple over the next couple of years, definitely."
>
> SENIOR IT INFRASTRUCTURE ARCHITECT, IT SERVICES

INVESTMENT OBJECTIVES FOR THE CUSTOMER JOURNEY TOWARD ZERO TRUST ARCHITECTURE ENABLED BY CISCO SECURITY SUITES

The interviewees' organizations searched for a solution that could address their growing concerns regarding shadow IT, which became more prevalent as the organizations shifted applications to the cloud. Interviewees noted that a primary entry point on their Zero Trust journeys was their organizational goals to secure user access to critical corporate resources. Other goals for this digital transformation included to:

- **Leverage the range of essential tools that Cisco Security Suites offers to secure the pillars of Zero Trust.** Interviewees shared that their organizations sought advanced protection for identity, devices, network, and data. The network enterprise architect in the oil and gas industry reported that their organization's Zero Trust journey with Cisco Security began in earnest after a device was compromised: "One retail manager had a

laptop infected with a virus, and we didn't have anything in between retail and corporate. That could have infected all our stores, so we had to deploy something very quickly, and that's when we got in touch with Cisco and signed an Enterprise Agreement. I actually convinced the business that we needed Cisco's identity security engine because that is where we know we need to look at the device posture."

- **Keep pace with organizational growth while consolidating the security infrastructure.** Interviewees lamented that prior solutions were not able to withstand the level of complexity and transaction volume that their organizations were reaching. The cybersecurity manager in the B2C commerce industry shared that their prior solution was not equipped to scale alongside their organization. They said, "We were using [a legacy two-factor authentication solution], which worked fairly well for years for an extremely limited number of users."
- **Positively impact the end-user experience while securing the brand.** Whether it was the internal technology resource at the keyboard, the internal end user or developer, or the external customer, interviewees noted that any impacts to these constituencies' experience had to be positive and serve their business objectives.
    - The cybersecurity manager in the B2C commerce industry shared: "Anytime we make a policy change, we're enforcing something on the end user, it has to make the user's life easier, or we're not going to do it — unless there's like a really, really good reason. But we have to make the user's life easier. It has to be faster, more convenient, etc."
    - The network enterprise architect in the oil and gas industry described the costly impacts of business disruption during a severe security event: "I'm glad [our organization hasn't been] on the 6 o'clock news [due to a data security breach]. This is all in the back of my mind in the sense that if one store gets caught out of thousands of stores, and we take one store offline, we would lose millions."

> "Zero Trust is one of our top priorities. It's one of the core things we have to do, especially to win the trust of our customers, and so they don't lose [confidence in us]. They have to know their money is safe with us."
>
> SENIOR IT INFRASTRUCTURE ARCHITECT, IT SERVICES

> "Before Cisco Security Suites, nothing was done until something happened, and we can't work like that anymore. Given the [onslaught of] threats at the moment, we have to be proactive. As times are moving, there's a lot happening, so we're looking to see who can give us a holistic approach, and in the retail space, Cisco fits [that need] perfectly."
>
> NETWORK ENTERPRISE ARCHITECT, OIL AND GAS

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. The composite is a globally distributed organization generating $2 billion in annual revenue. It is supported by 5,000 FTEs worldwide, with 30 FTEs dedicated to technology infrastructure, networking, and security operations as well as troubleshooting and incident response. Early in its security maturity journey, the composite organization's legacy

approach to cyber defense followed a traditional one in which its network represented its main perimeter.

The composite has 50 enterprise applications as a result of growing sprawl in its technology estate. In the past, applications were often unsupported by the technology organization, with identity management functions decentralized among business units, resulting in redundant identity management and security operations and troubleshooting.

Deployment characteristics. The composite organization is undergoing a digital transformation to align cyber defense strategies with business growth objectives. It seeks to limit the sprawl of its technology estate while centralizing and streamlining activities for identity security and management. As part of this technology consolidation, the composite organization is also shifting to a hybrid work model in which half of the FTEs will work remotely part time.

To stay competitive and secure its brand, the composite organization sets out on a multiyear journey toward Zero Trust intermediate maturity. To facilitate this transformation, the composite organization transitions its users to a Cisco Security environment featuring:

- Extended detection and response (XDR) functionality.
- Advanced capabilities for security policy management, multifactor authentication (MFA), and single sign-on (SSO).
- Protection for email, endpoints, and devices.
- A modernized, cloud-delivered, security service edge network that consolidates multiple security capabilities, including a secure web gateway, cloud access security broker, and Zero Trust network access.

The composite organization's change management effort includes a multiyear transition to mainstream Zero Trust principles in the Cisco Security environment. It deploys Cisco Security's User Protection Suite and Breach Protection Suite to 25% of all users in Year 1. This increases to 55% of all users in year 2, with 70% of users supported by the Cisco Security environment by the end of Year 3.

KEY ASSUMPTIONS

$2 billion annual revenue

5,000 total FTEs, 50% remote/hybrid

30 security, network, infrastructure and other FTEs dedicated to Zero Trust architecture enabled by Cisco Security Suites

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	Legacy networking and security infrastructure consolidation	$109,148	$240,126	$305,615	$654,889	$527,289
Btr	Identity security and management consolidation	$193,284	$425,225	$541,195	$1,159,704	$933,746
Ctr	Networking and infrastructure operations improvement	$88,358	$194,388	$247,404	$530,150	$426,855
Dtr	Security operations optimization	$138,060	$303,732	$386,568	$828,360	$666,962
Etr	Avoided costs of a material breach	$316,691	$696,720	$886,734	$1,900,145	$1,529,919
Ftr	Remote end-user productivity savings	$73,124	$160,874	$204,748	$438,746	$353,261
Gtr	IT administration and help desk cost savings	$5,616	$12,384	$15,768	$33,768	$27,187
	Total benefits (risk-adjusted)	$924,281	$2,033,449	$2,588,032	$5,545,763	$4,465,219

LEGACY NETWORKING AND SECURITY INFRASTRUCTURE CONSOLIDATION

Evidence and data. In general, customers reported a consolidated spend related to several factors, including Cisco licensing optimization, software or SaaS license and subscription savings, and legacy hardware decommissioning cost savings. The optimized and consolidated technology environment required fewer resource hours to manage additional solutions from multiple vendors, providing additional technology management labor optimization.

- The VP of IT at the real estate company reported on significant savings by optimizing licensing for various other point solutions because they use Cisco Security Suites: “Normally, we would buy the advanced tier, which includes extra protections … but [now we are] running all of our traffic through the secure web gateway, included in Secure Access. With Cisco Security Suites, there’s not much of a need for those [higher-cost licenses] anymore, so it reduces our costs. In fact, it’ll eventually reduce the cost so much, it just pays for itself.”

- The VP of IT services at the construction company estimated that their organization paid twice as much in the prior environment to cover what Cisco Security Suites accomplished when configured into a Zero Trust architecture. These excess costs would include seven to eight point solutions with four FTEs to manage them. They also discussed the added savings from discounts conferred by the Enterprise Agreement: "There'd probably be an additional seven or eight point products [additional agents] that we would have to deploy in the environment. And then there would be something to tie that all together, whether it's something to bring in logs and something to correlate all the data through those applications. We would have all these different things, and we would need more people to do it. But the big benefit [of going with Cisco Security Suites is] not only locking in that cost for a five-year term, but also, it's cheaper than a la carte. There's a significant discount with an Enterprise Agreement, and if you add multiple years to it, the math gets even better."
- The cybersecurity manager in the B2C commerce industry shared how the consolidated Enterprise Agreement saved dozens of hours related to annual budgeting and purchasing decisions. The manager also noted that the agreement structure made it easier to achieve executive buy-in for the large-scale, multitool, multiyear investment in both the tools and change management labor efforts related to securing an organization according to Zero Trust principles. They said, "Talking to the executive board, presenting [the Enterprise Agreement] as a cohesive solution, a one-time thing, made it a whole lot easier not only to get in place but also to budget with predictable costs."

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

- Total licensing costs for networking and security tools in the prior environment were $2,432,000.
- The composite organization experiences a 15% reduction in legacy costs with security tool consolidation in a transition to Zero Trust architecture, enabled by Cisco Security. This is a result of a combination of cost optimizations related to legacy software license and SaaS and subscription savings, plus legacy hardware decommissioning cost savings.

- In Year 1, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.
- The composite organization also avoids internal labor costs to maintain legacy infrastructure. In the prior environment, the composite organization dedicates 2,912 hours of internal labor to maintain the legacy infrastructure and security stack. This also includes technology management labor savings related to consolidating multiple vendors to one vendor and switching to a five-year agreement.
- With Zero Trust infrastructure enabled by Cisco Security, the composite experienced a 70% reduction in the total hours of internal labor to maintain legacy infrastructure per year.
- The blended, fully burdened hourly rate of a technology resource is $59.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The functionality, license level, and quantity of legacy vendor solutions decommissioned.
- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles.
- Network and security operations FTE salaries and the skill sets available.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $527,000.

15%

Percentage reduction in legacy costs with transition to Zero Trust architecture with Cisco Security Suites

> "We can remove the need to purchase advanced licenses [for our firewalls] because now all that traffic is going through the Cisco Secure firewall web gateway anyway, in the cloud."
>
> VP OF IT, REAL ESTATE

Legacy Networking And Security Infrastructure Consolidation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Total cost of legacy systems consolidated or decommissioned with Zero Trust and Cisco Security	Composite	$2,432,250	$2,432,250	$2,432,250
A2	Percentage reduction in legacy costs with transition to Zero Trust architecture with Cisco Security	Interviews	15%	15%	15%
A3	Percentage of transition to Zero Trust architecture with Cisco Security	Interviews	25%	55%	70%
A4	Subtotal: legacy infrastructure cost consolidation with Cisco Security	A1*A2*A3	$91,209	$200,661	$255,386
A5	Hours of internal labor to maintain legacy infrastructure in prior environment	Interviews	2,912	2,912	2,912
A6	Percentage reduction in hours of internal labor to maintain legacy infrastructure	Interviews	70%	70%	70%
A7	Blended fully burdened hourly rate of a technology resource	Composite	$59	$59	$59
A8	Subtotal: avoided internal labor costs to maintain legacy infrastructure	A3*A5*A6*A7	$30,066	$66,146	$84,186
At	Legacy networking and security infrastructure consolidation	A4+A8	$121,275	$266,807	$339,572
	Risk adjustment	↓10%			
Atr	Legacy networking and security infrastructure consolidation (risk-adjusted)		$109,148	$240,126	$305,615
	Three-year total: $654,889			**Three-year present value: $527,289**	

IDENTITY SECURITY AND MANAGEMENT CONSOLIDATION

Evidence and data. In the interviewees' prior environment, identity management responsibility was atomized across the organizations, leading to labor inefficiencies and increasing the risk of misconfigurations, security gaps, and the potential for threat actors to gain access, resulting in

lateral movement inside of the network. Day-to-day identity management effort was taken on by business resources, while incident management and troubleshooting also required help desk and technology resources.

With their transition to Zero Trust architecture with Cisco Security Suites, interviewees discussed how their organizations were able to consolidate identity security and management within the Cisco Security platform. This eliminated business resources' role both in the redundant, manual management efforts and in identity security remediation efforts such as account takeovers and investigations, thus allowing these resources to focus on higher-value activities. The transition to the Cisco Security environment also conferred efficiencies in identity security and management benefits for technical resources, which are reflected in the Security Operations Optimization benefit as well as the IT Administration And Help Desk Cost Savings benefit.

Interviewees noted several specific value drivers for their organizations, which varied in how they managed identities prior to Cisco Security Suites:

- The VP of IT services at the construction company indicated that their organization's use of Cisco Duo and MFA improved both the administration and end-user side of the authentication experience. They shared: "We have users who do bad things … and the machine learning within Duo can look at anomalies and login requests, where people are, and all those different things, [including] push breaks attacks, and then it can automatically, without us doing anything, move into a step-up multifactor authentication. That machine learning capability definitely makes me happy. It's an extra layer of security for our users when they are doing bad things. I think people like the single sign-on capabilities and not having to remember a password."
- The cybersecurity manager in the B2C commerce industry reported that their organization experienced a surge in business applications managed outside of the technology organization in the years since the COVID-19 pandemic. The interviewee pointed out that this decentralized approach would impede resources from achieving their own core business objectives: "COVID hit, and people were just all doing their own things and [soon enough, we had] 28 applications. For each one of those 28 applications, a quarter of [a business resource's] job was just managing those identities. I said to these resources, 'You do not want to manage people's identities. You've got another job. Do what's important to you. We have this whole platform that will do this. All

you have to do is plug in.' So we mitigated seven full-time employees from not having to do that."

- The VP of IT at the real estate company discussed how their organization was able to centralize identity security and management with a Zero Trust network access (ZTNA) approach using Cisco Security Suites. Their organization's prior environment required repetitive, manual processes for securely managing user identities across all of its properties and their devices, which included security systems and cameras. They shared, "It was very cumbersome to manage, mainly because it had to be managed individually per building. And when you're managing 30 buildings, it's much easier to do it in ZTNA [with Cisco Security Suites] because the user can be added just to 30 buildings at a time, instead of going building network by building network and provisioning them."

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

- The composite seeks to limit agent sprawl over the investment period. While the number fluctuates, it maintains an average of 50 enterprise applications at any given time.
- In the prior environment, each enterprise application and its identity and security management workflows were routed and managed through the respective business units that own the applications. Each application required an average of 416 labor hours for identity security and management annually.
- In Year 1 of the investment period, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.
- In the Cisco Security environment, the composite organization reduces the total number of hours required for identity security and management labor by 70%.
- The blended, fully burdened hourly rate of a technology resource is $59.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The total number of enterprise applications and any anticipated growth.

- The functionality and quantity of decommissioned legacy vendor solutions related to identity security and management.
- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles.
- An organization's identity security and management policies prior to Cisco Security Suites. Organizations that previously centralized identity management and security may not experience this benefit.
- Related FTE salaries and the skill sets available.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $934,000.

15%

Percentage reduction in legacy costs with transition to Zero Trust architecture with Cisco Security Suites

"By hooking into our systems like this, your life is easier. You don't have to have a full-time employee just managing identities [for our HR app], for [my company]."

CYBERSECURITY MANAGER, B2C COMMERCE

Identity Security And Management Consolidation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Total applications	Composite	50	50	50
B2	Hours of decentralized identity security and management labor per application in the prior environment	Interviews	416	416	416
B3	Total hours of identity and access management labor in the prior environment	B1*B2	20,800	20,800	20,800
B4	Percentage reduction in hours of identity and access management labor with Cisco Security	Interviews	70%	70%	70%
B5	Percentage of transition to Zero Trust architecture with Cisco Security	A3	25%	55%	70%
B6	Blended fully burdened hourly rate of a technology resource	Composite	$59	$59	$59
Bt	Identity security and management consolidation	B3*B4*B5*B6	$214,760	$472,472	$601,328
	Risk adjustment	↓10%			
Btr	Identity security and management consolidation (risk-adjusted)		$193,284	$425,225	$541,195
	Three-year total: $1,159,704			**Three-year present value: $933,746**	

NETWORKING AND INFRASTRUCTURE OPERATIONS IMPROVEMENT

Evidence and data. As they centralized networking and security functions with Cisco Security Suites, interviewees shared how their organizations leveraged infrastructure automation and orchestration of the provisioning lifecycle for virtual and physical devices for operational efficiencies. By automating major tenets of Zero Trust into the provisioning lifecycle, interviewees shared how their teams were able to increase their deployment capacity and reduce service-level agreement (SLA) timeframes and related labor effort. At the same time, they discussed how their teams reduced manual errors and related labor to correct errors, and how they mitigated the risk of misconfiguration that could lead to cost overruns and risky security gaps.

- The network enterprise architect in the oil and gas industry discussed how Cisco Security Suites' help their infrastructure teams automate and improve workflows across the provisioning lifecycle, leading to major time savings. They indicated that onboarding devices was streamlined as the process leveraged the existing Cisco security stack, cutting down on time spent on manual provisioning in the prior environment: "On the

infrastructure side, in the past we had a team of seven to eight people just doing new builds for a device, a firewall, anything. But now, with the automation that we're building in… it is just plug and play. [Previously] it took hours and hours to do simple things. Now with automation, we're just doing it in minutes."

- In addition to reducing the volume of repetitive workflows with automation, as noted above in the Identity Security And Management Consolidation benefit, the VP of IT at the real estate company reported further time savings for technical resources. The interviewee discussed the time savings when provisioning devices and deploying infrastructure in a Zero Trust environment built on Cisco Security Suites: "[Now, users] automatically get removed from the ZTNA access, whereas before, we would have to manually remove their VPN access for all the different systems. That's one whole hour [of work down] to 10 seconds."
- The CIO at the legal services company noted that their organization found particular value in Duo's trusted endpoint configuration and management capability. They said, "This is the first organization that I've been able to deploy 100% trusted endpoint requirements on."

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

- In the prior environment, the composite dedicated four resources to siloed network and infrastructure management.
- By transitioning to a Zero Trust architecture with Cisco Security Suites, the composite centralizes and automates network and infrastructure management workflows, reducing manual labor by 80%.
- In Year 1, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.
- The blended, fully burdened annual salary of a technology resource is $122,720.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles.
- The functionality and quantity of decommissioned legacy vendor solutions related to identity security and management.
- Network and infrastructure FTE salaries, the skill sets available, and the extent to which their workflows were manually conducted in the prior environment. Some activities noted in this section may be completed by security resources in some organizations, which would impact the distribution of both this benefit and the Security Operations Optimization benefit.

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

Networking And Infrastructure Operations Improvement					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Resources dedicated to siloed network and infrastructure management in the prior environment	Composite	4	4	4
C2	Percentage reduction in siloed network and infrastructure management labor with Cisco Security automations	Interviews	80%	80%	80%
C3	Percentage of transition to Zero Trust architecture with Cisco Security	A3	25%	55%	70%
C4	Blended fully burdened annual salary of a technology resource	Composite	$122,720	$122,720	$122,720
Ct	Networking and infrastructure operations improvement	C1*C2*C3*C4	$98,176	$215,987	$274,893
	Risk adjustment	↓10%			
Ctr	Networking and infrastructure operations improvement (risk-adjusted)		$88,358	$194,388	$247,404
	Three-year total: $530,150			**Three-year present value: $426,855**	

80%

Percentage reduction in siloed network and infrastructure management labor with Cisco Security automations

> "Now, with Cisco Security automation, we're just doing [what used to take hours] in minutes. Every day, we're heavily focusing on automation, especially in my space in the security and infrastructure side. Since this journey began three years ago, we have [automated] hundreds to thousands of workloads."
>
> NETWORK ENTERPRISE ARCHITECT, OIL AND GAS

SECURITY OPERATIONS OPTIMIZATION

Evidence and data. Interviewees discussed how the activation of Zero Trust principles served to guide the transition toward Cisco Security solutions, and how the integration of these new technologies and processes assisted their security teams in their day-to-day, proactive cyber defense efforts.

This benefit examines the business value of avoided manual cyber defense workflows intended to prevent threats from materializing into a serious material breach, or to prevent unauthorized disclosure of critical data. See Avoided Costs Of A Material Breach, Benefit E, for analysis on the business value that may occur once a threat is realized.

- The VP of IT services at the construction company described how the Cisco Security Suites integrated with other vendor tools to augment controls over their organization's Zero Trust environment: "We can enrich all the data that we're receiving in from all the different Cisco components. All those products talk to each other, and then we tie that together with XDR. So it's like a single pane of glass to see everything about the

environment so our SOAR [security orchestration, automation, and response] capabilities are far greater than anything we've ever had."

- The cybersecurity manager in the B2C commerce industry shared how their organization's Zero Trust architecture enabled by Cisco Security Suites integrated well to identify and block threat actors from entering the organization through web-based attacks and malware. As a result, they reported, "For our organization's size, we should have 10 people on my team, not including myself, and I can do my job with a managed security provider, one SOC [security operations center] analyst, me, and [some] help from the operations team."
- The network enterprise architect in the oil and gas industry discussed how Cisco Security Suites helped their organization reduce the labor effort associated with managing policies for the thousands of firewalls protecting operations at critical retail and refining locations. They shared how Cisco's integration of AI into the workflow added insight into prioritization of issues and helped with policy optimization to clean up shadow, redundant rules or dead rules: "We have thousands [of firewall rulesets] in the sense, we have that many Cisco firewalls that it has become tedious every day to manage these firewalls in terms of the rule sets. There're duplicate rules, rules to clean up, etc. We have about a dozen [FTEs managing them and] we can turn that down to six, so the other six can focus on the bigger things."
- The CIO at the legal services company noted that their organization was able to finely tune their security policies much more easily in the Cisco Security Suites environment: "The ability to have highly technical, highly tuned policies per application while also supporting group policies for exceptions for application has been remarkable. You can't log on to [your email] unless you do it from a trusted endpoint. You can't log on the VPN unless it's on a trusted endpoint device, as stipulated by combination of the Duo Desktop application or an enrolled mobile device, and what enables that is the Duo. And without the ability to quickly and easily manage the exceptions that will inevitably pop up, we wouldn't be able to do that."

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

- In the prior environment, 10 technology resources were partially dedicated security operations related to Zero Trust. To meet the full needs of a Zero Trust environment

without Cisco Security Suites, the composite would need to fully dedicate all 10 of these resources.

- By investing in Cisco Security Suites to enable its Zero Trust architecture:
    - The composite organization improves visibility and adds bidirectional integrations with Cisco and other vendor tools. The consolidated network and security environment aligning with Zero Trust best practices augments the range and quality of data that security resources access used to perform day-to-day tasks and to troubleshoot and remediate.
    - Further, the optimized Zero Trust environment enabled by Cisco Security Suites automates critical workflows that were previously conducted manually by security resources, such as account takeovers and aspects of incident detection and response.
- Taken together, these enhanced capabilities and time savings lead to a 50% reduction in resources needed to optimize for effective Zero Trust security management. This also frees up internal security resources to focus on higher-value security operations activities.
- In Year 1, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.
- The blended, fully burdened annual salary of a technology resource is $122,720.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The percentage of total users supported by Cisco Security architecture and an organization’s adoption ramp.
- An organization’s security maturity and its progress toward Zero Trust principles.
- The functionality and quantity of decommissioned legacy vendor solutions related to security operations.
- The nature, frequency, and volume of threats particular to an organization.
- Security operations FTE salaries and the skill sets available.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $667,000.

Security Operations Optimization					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Total resources required to optimize for effective Zero Trust security management	Composite	10	10	10
D2	Percentage reduction in new resources needed to optimize for effective Zero Trust security management attributed to Cisco Security	Interviews	50%	50%	50%
D3	Percentage of transition to Zero Trust architecture with Cisco Security	A3	25%	55%	70%
D4	Blended fully burdened annual salary of a technology resource	Composite	$122,720	$122,720	$122,720
Dt	Security operations optimization	D1*D2*D3*D4	$153,400	$337,480	$429,520
	Risk adjustment	↓10%			
Dtr	Security operations optimization (risk-adjusted)		$138,060	$303,732	$386,568
	Three-year total: $828,360			**Three-year present value: $666,962**	

50%

Percentage reduction in new resources needed to optimize for effective Zero Trust security management attributed to Cisco Security Suites

> "[Our organization values] the ease of access to critical information about our network and data traversing it and the endpoints on it. The visibility is fantastic. We can see everything now. And not only can we see it, we can pivot to other applications within that Cisco Security stack from a single location."
>
> VP OF IT SERVICES, CONSTRUCTION

AVOIDED COSTS OF A MATERIAL BREACH

Evidence and data. As a result of the optimized security environment and improved security management workflows described above, interviewees further articulated business benefits related to reduced costs of a potential material breach. Interviewees noted how their Cisco Security Suites, sometimes in combination with other vendor tools and aligning with Zero Trust principles, effectively blocked and remediated attacks, reallocating that amount of reactive team effort to higher-value security activities.

This benefit examines the business value of avoided costs that may occur once a threat is realized. See Security Operations Optimization, Benefit D, for analysis on the business value of avoided manual, proactive cyber defense workflows.

- The VP of IT at the real estate company discussed how the shift to a Zero Trust network access environment with Cisco Security Suites significantly increased their organization's cyber defenses compared to their prior, perimeter- and password-based environment: "Because we can leverage our own IDP [(identity provider) using Cisco Security Suites], now we can add all sorts of conditional access policies and security measures on top of users' login info. You're moving from an old password-based system to these modern, secure authentication methods. So the environment is maybe 90% more secure after you do one building on [ZTNA with Cisco Security]."
- Compared to their organization's prior environment, the VP of IT services at the construction company shared that their organization was avoiding significant security incidents with Cisco Security Suites as well as the wide-ranging, costly impacts that

breaches cause: “We can’t grow a business if we’re down [due to a security incident]. Having proper security, proper tools, to keep the business rolling without disruption, that’s the way that I’m looking at it. The Cisco Security tools are doing their job. We’re getting people connected to things that they need to connect to. We’re not having major incidents where we’re having to isolate PCs or take things offline.”

- The cybersecurity manager in the B2C commerce industry reported that Cisco Security Suites combined with a Zero Trust approach greatly increased their organization’s security posture compared to the prior environment: “Secure Internet Access [from Cisco Security] has saved me more times than I can count. There was a malware called WannaCry that came out a week [after we installed Umbrella]. We got hit pretty hard; about nine of our systems got hit simultaneously, and Umbrella blocked it all.”
- The CIO at the legal services company shared that their configuration of Zero Trust principles in their Cisco Security Suites greatly increased their organization’s defenses against credential theft: “I can give you my credentials right now and sit and wait for you to log on and accept the Duo Push for you to log on, and you still couldn’t log on. That has all been obviated, even the concern for phishing attacks, because no one can log on [without the proper trusted endpoints].”

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

- The composite organization has a 91% likelihood of experiencing one or more serious data breach per year in which the organization’s sensitive data is potentially compromised; this is held flat year over year for the purpose of this analysis.[5]Forrester estimates that 70% of breaches are addressable with Cisco Security User Protection Suite and Breach Protection Suite when implemented in alignment with Zero Trust principles.[6] These include external attacks targeting the organization or an employee’s remote work environment as well as most internal incidents within the organization.[7]
- The mean cumulative cost of data breaches in the prior environment is $4.1 million. For the composite, these combined factors yield $2,639,000 of annualized risk exposure addressable with Cisco Security Suites and Zero Trust.[8]
- In Year 1, 25% of the composite organization’s users are supported by Cisco Security Suites built upon Zero Trust principles; that rises to 75% in Year 2 and 90% in Year 3.

- With Cisco Security Suites deployed in alignment with Zero Trust principles, the composite reduces the likelihood of a severe data breach caused by an external attack by 60%.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles.
- The functionality and quantity of decommissioned legacy vendor solutions related to external breach protection.
- Security operations FTE salaries and the skill sets available.
- The likelihood and associated costs of security breaches each year.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.5 million.

Avoided Costs Of A Material Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Likelihood of experiencing one or more breaches per year	Forrester research	91%	91%	91%
E2	Mean cumulative cost of breaches	Interviews	$4,143,000	$4,143,000	$4,143,000
E3	Percentage of breaches originating from external attacks and addressable with Zero Trust architecture and Cisco Security	Forrester research	70%	70%	70%
E4	Annual risk exposure addressable with Cisco Security	E1*E2*E3	$2,639,091	$2,639,091	$2,639,091
E5	Reduced risk of breaches attributed to Cisco Security and from leveraging Zero Trust principles	Interviews	60%	60%	60%
E6	Percentage of transition to Zero Trust architecture with Cisco Security	A3	25%	55%	70%
Et	Avoided costs of a material breach	E5*E4*E6	$395,864	$870,900	$1,108,418
	Risk adjustment	↓20%			
Etr	Avoided costs of a material breach (risk-adjusted)		$316,691	$696,720	$886,734
	Three-year total: $1,900,146			**Three-year present value: $1,529,919**	

70%

Reduced risk of breaches attributed to Cisco Security Suites and from leveraging Zero Trust principles

"People have [still] been successfully phished, but there has been no successful breach, The phisher couldn't do anything with the credentials because we [use Duo and] also have geoblocking."

CIO, LEGAL SERVICES

REMOTE END-USER PRODUCTIVITY SAVINGS

Evidence and data. Interviewees shared how the transition to Zero Trust approaches with Cisco Security Suites helped streamline the overall technology environment and reduce the amount of friction an end user faced when accessing the network remotely. By shifting to URL-based access linked to their organization's identity provider, they can reduce keystrokes associated with the legacy authentication process.

- The VP of IT at the real estate company described how this shift to Zero Trust with Cisco Security Suites looked at their organization: "[Prior], you were going to connect to the VPN, and then once you're connected, then you would go to the resource you need [and log in again]. With Cisco Security Suites, you're moving from [having to connect to the VPN] to just clicking a link, so your reduction [in time spent on authentication processes] would probably be from a couple minutes down to 10 seconds."
- The VP of IT at the real estate company further noted that improvements and optimizations in identity, networking, and infrastructure management reduced end users' SLAs, thus increasing the time they could spend productively using corporate resources. They said, "We just will label groups based on [our criteria], and then they can just add them to the groups and then they automatically have access with the same username and password and security they already have on their user accounts for their computer."
- The VP of IT services at the construction company also indicated that the deployment of Duo SSO qualitatively and quantitatively improved their end user's remote experience by removing friction: "People are definitely happier with single sign-on, not having to remember a password. It probably shaves 30 seconds [off every login]. I'm happier that people are using it because that's tied into Duo … with machine learning capability."

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

- The composite organization has 2,500 end users accessing services remotely.
- On average, each remote end user wasted 4 minutes per day due to friction in accessing services in the prior environment.
- With Cisco Security Suites in alignment with Zero Trust best practices, the composite reduces the time it takes end users to access services remotely by 75%.

- End users are able to recapture 25% of the hours that would have otherwise been lost to lengthy remote end-user bootup procedures.
- In Year 1, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.
- The fully burdened hourly rate for an end user is $40.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles.
- The functionality and quantity of decommissioned legacy vendor solutions related to remote access.
- The level of friction present in the end user's prior environment and the extent to which that is mitigated with Cisco Security Suites.
- End-user FTE salaries and the rate at which resources can recapture lost productivity.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $353,000.

Remote End-User Productivity Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
F1	End users accessing services remotely	Composite	2,500	2,500	2,500
F2	Total minutes per end user to access services remotely, per day	Interviews	4	4	4
F3	Total hours end users spend accessing services remotely per year in prior environment	F1*F2/60*260	43,333	43,333	43,333
F4	Reduction in time for end users to access services remotely with Cisco	Interviews	75%	75%	75%
F5	End-user productivity capture	Composite	25%	25%	25%
F6	Fully burdened hourly rate for an end user (average)	Composite	$40	$40	$40
F7	Percentage of transition to Zero Trust architecture with Cisco Security	A3	25%	55%	70%
Ft	Remote end-user productivity savings	F3*F4*F5*F6*F7	$81,249	$178,749	$227,498
	Risk adjustment	↓10%			
Ftr	Remote end-user productivity savings (risk-adjusted)		$73,124	$160,874	$204,748
	Three-year total: $438,746			**Three-year present value: $353,261**	

4.9 hours per end user per year

Previously wasted time saved with Cisco Security Suite's improved remote end-user environment

"The [remote end-user] experience is way different [with Cisco Security Suites]. There's no need for end users to fuss about connecting to VPNs or seeing if they're disconnected. It just works."

VP OF IT, REAL ESTATE

IT ADMINISTRATION AND HELP DESK COST SAVINGS

Evidence and data. By shifting to a technology environment that upholds Zero Trust principles using Cisco Security Suites, interviewees reported that their organizations were able to reduce the volume of issues related to user access.

- The VP of IT at the real estate company said that the transition to Cisco Security Suites and Zero Trust helped to eliminate the number of tickets that resulted from manual errors made during the provisioning process: “Usually an error would just be forgetting to provision someone in a certain building or something. [The combination of Zero Trust architecture and Cisco Security] reduces errors. Fewer moving parts means fewer errors, which would manifest as [fewer] tickets.”
- The VP of IT services at the construction company also stated that their organization faced fewer provisioning issues: “We usually have little to no tickets about any provisioning [with Cisco Security Suites]. We’re doing a lot more now, and we barely have any issues.”

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

- In the prior environment, the composite processed an average of 7,500 IT support tickets related to user access and device and infrastructure management troubleshooting. Each ticket took 10 minutes on average to resolve.
- With Cisco Security Suites and the Zero Trust environment it facilitates, the composite reduces related IT support ticket volume by 50%.
- In Year 1, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.
- The fully burdened hourly rate for an IT support technician is $40.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this benefit:

- The extent to which an organization achieves other benefit areas impacting the support function, such as remote end-user productivity.

- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles.
- The number of related help desk tickets filed annually.
- The nature and severity of network and security issues fielded by the IT help desk in the prior environment, and how much time it took to resolve them.
- IT support technician FTE salaries and the skill sets available.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $27,000.

IT Administration And Help Desk Cost Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
G1	Total IT support tickets related to user accounts and access in the prior environment	Composite	7,500	7,500	7,500
G2	Average minutes to resolve IT support tickets related to user accounts and access in the prior environment	Composite	10	10	10
G3	Total hours to resolve IT support tickets related to user accounts and access in the prior environment	G1*G2/60	1,250	1,250	1,250
G4	Percentage reduction in related IT support tickets with Cisco Security	Interviews	50%	50%	50%
G5	Percentage of transition to Zero Trust architecture with Cisco Security	A3	25%	55%	70%
G6	Hours of avoided IT support due to reduced ticket volume with Cisco Security	G3*G4*G5	156	344	438
G7	Fully burdened hourly rate for an IT support technician	Composite	$40	$40	$40
Gt	IT administration and help desk cost savings	G6*G7	$6,240	$13,760	$17,520
	Risk adjustment	↓10%			
Gtr	IT administration and help desk cost savings (risk-adjusted)		$5,616	$12,384	$15,768
	Three-year total: $33,768		**Three-year present value: $27,187**		

50%

Percentage reduction in networking, security, and remote end-user-related IT support tickets with Cisco Security

"Once the ZTNA tunnels are up and have been tested that they're working properly, we basically eliminated any VPN tickets we get from that group of people."

VP OF IT, REAL ESTATE

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not quantified for this study:

- **More efficient M&A activities.** Interviewees whose organizations had a high volume of mergers and acquisitions noted that their teams were able to normalize operations for newly merged companies much faster and more effectively than in the prior environment. The senior IT infrastructure architect in the IT services industry noted that Cisco helped them standardize security when merging new companies: "We definitely improved on the timeline to implement [the merger] because we ramped it up a lot. Previously, there were a lot of legacy processes, a lot of approvals, and we streamlined this also with the product, with visibility and so on."
- **Reduced technical debt.** Interviewees noted that Cisco Security Suites, in alignment with Zero Trust principles, helped them eliminate much of the technical debt caused by efforts to maintain business continuity despite the complexity present in the prior environment. The senior IT infrastructure architect in the IT services industry shared: "We've always looked to reduce complexity and automate things when possible. We try

to reduce technical debt, but a lot of old technical debt couldn't be identified. Now we know [about] it, and now we can address these risks and move forward in an agile way."

- **Improved standing with cybersecurity insurance providers.** Interviewees noted that their organizations were able to improve their cyber defenses. As a result, they were able to gain cyber insurance coverage where they were unable to before or received discounts on annual premiums.

> "Up until recently, we haven't been able to get cybersecurity insurance — we weren't even eligible. We became eligible last month because of Duo."
>
> CYBERSECURITY MANAGER, B2C COMMERCE

FLEXIBILITY

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

- **Digital transformation.** Interviewees discussed how their Cisco Security Suites, coupled with the implementation of Zero Trust principles, helped them lay the groundwork for several other digital transformation business objectives. The network enterprise architect in the oil and gas industry shared how their configuration of Cisco Security Suites permitted their organization to invest in IoT enablement at their retail outlets. This facilitated more efficient fuel inventory management, better maintenance and upkeep of their fleet of vehicles, and optimization of solar energy used in their operations.
- **Less time spent on auditing.** Interviewees shared how the improved visibility and unified policy management in the Zero Trust environment with Cisco Security Suites reduced the time that resources needed to spend on audits. The CIO at the legal

services company indicated that in the prior environment, two out of 30 resources were dedicated to coordinating manual reporting. With the Zero Trust environment with Cisco Security Suites, their organization was able to reattribute those reporting resources to higher-value activities.

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

> "[With Cisco Security ISE and Secure Firewall], we don't have holes that we don't know about, because it's all one policy at that point. Again, this leads to less staff having to do audits and things like that."
>
> **CYBERSECURITY MANAGER, B2C COMMERCE**

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**
Htr	Cisco Security Enterprise Agreement	$0	$353,194	$777,026	$988,943	$2,119,163	$1,706,263
Itr	Implementation and training	$179,630	$78,959	$35,409	$8,142	$302,140	$286,791
Jtr	Platform administration	$0	$26,998	$59,397	$75,595	$161,990	$130,428
	Total costs (risk-adjusted)	$179,630	$459,151	$871,832	$1,072,680	$2,583,292	$2,123,482

CISCO SECURITY ENTERPRISE AGREEMENT

Evidence and data. Interviewees discussed the components of their organization's Enterprise Agreements for Cisco Security Suites. They noted several aspects of the agreement that allowed their organizations the flexibility to grow without limiting their security coverage in between agreement cycles.

- The cybersecurity manager in the B2C commerce industry shared how they leveraged Cisco's Enterprise Agreement while negotiating and budgeting for the many needed solutions in the cybersecurity stack: "What Cisco allows me to do as a practitioner, especially with the enterprise license agreement, is say, 'We're getting all of these things,' to the board, and that becomes a much easier sell because that includes the majority of the Cisco Suite. So that would be Secure Internet Access, ISE, Firewall Solutions, and Secure Endpoint, [etc.]."
- The network enterprise architect in the oil and gas industry pointed out how the Enterprise Agreement made it easier to secure approval for a more comprehensive approach to endpoint security. They shared, "Now, because we own the Enterprise Agreement bucket, the licensing part is super easy, which is why we decided to deploy Secure Internet Access to every laptop out there in the retail space."

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

- Over three years, the composite organization deploys the following Cisco Security solutions in a phased implementation alongside the introduction of Zero Trust:
    - Breach Protection Suite Premier: XDR Premier; Email Threat Defense; Endpoint Premier; and Secure Network Analytics.
    - User Protection Suite Advantage: Duo Advantage; Secure Access Advantage; and ISE Premier.
- In Year 1, the composite organization completes 25% of its multiyear transition to Zero Trust architecture enabled by Cisco Security. This increases to 55% in Year 2 and 70% in Year 3.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this cost:

- The functionality, license level, and quantity of legacy vendor solutions decommissioned.
- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles prior to Cisco Security Suites.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.7 million.

> "What's really important to me is the entire integration piece, so [all of the Cisco Security solutions] can talk to each other. The whole is more than the sum."
>
> **CYBERSECURITY MANAGER, B2C COMMERCE**

Cisco Security Enterprise Agreement						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Cisco Security Enterprise Agreement for Breach Premier and User Advantage	Interviews	$0	$336,375	$740,025	$941,850
Ht	Cisco Security Enterprise Agreement	H1	$0	$336,375	$740,025	$941,850
	Risk adjustment	↑5%				
Htr	Cisco Security Enterprise Agreement (risk-adjusted)		$0	$353,194	$777,026	$988,943
	Three-year total: $2,119,163			**Three-year present value: $1,706,263**		

IMPLEMENTATION AND TRAINING

Evidence and data. Most interviewees' organizations already had some Cisco networking or security products incorporated into their technology environment before beginning their journey to facilitate a Zero Trust approach to their security architecture. Several interviewees highlighted the value of Cisco Security Suite's technical support during the implementation and integration process.

- The senior IT infrastructure architect in the IT services industry underscored the value of Cisco's technical expertise provided early on: "During the implementation phase, Cisco's Software Support Service helped us to introduce the product [and provided] a lot of knowledge transfer. That was very crucial for us."
- The network enterprise architect in the oil and gas industry described how their organization gained efficiencies while deploying solutions in their Cisco Security Suite over a multiyear period: "It took us three to four months from the start because we had to get all the policies within the Secure Internet Access set up. But once we did the packet, we just replicated that in pilot, and then from pilot we went full throttle into it. I think we picked like 50 stores in [a major city], and then we just rolled it across to everyone else."
- The cybersecurity manager in the B2C commerce industry shared how their organization enhanced its deployment of Cisco's Security Suite solutions by leveraging Cisco's Software Support Service. They noted that it could take upward of a month for an organization like theirs to deploy their configuration at once: "If somebody were doing the entire suite from nothing and they were starting [solution by solution], they should probably allow themselves a solid month … to do everything. That's not only going to be

your installation. That's going to be your policy generation, your test and tuning, and your production release as well."

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

- In the initial period of the multiyear transition, the composite dedicates half of the technology resources to standing up the new Cisco Security architecture to align with Zero Trust principles. Each resource dedicates 104 hours to deployment during this period, 60% of a resource's time for a three-month period. This decreases by 50% YoY because of efficiencies gained in the earlier stages. It also relies on technical implementation support from Cisco's Software Support Service included in the Security Suite.
- In Year 1, the composite dedicates 10 technology resources to standing up additional portions of the new Cisco Security architecture. Each resource dedicates 52 hours to deployment during this period, during which the composite completes 25% of its transition to Zero Trust architecture with Cisco Security.
- The composite organization completes 55% of its transition to Zero Trust architecture with Cisco Security by the end of Year 2. This requires five technology FTEs to dedicate 26 hours each to these implementation efforts.
- As new resources are ramped into the Cisco Security environment, they undergo 16 hours of training. In the initial period, there are 15 new trainees. In Year 1, 10 new resources are trained, and in Year 2, the remaining five technology resources receive training.
- The fully burdened hourly rate of an administrator is $59.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this cost:

- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles prior to Cisco Security Suites.

- The extent to which an organization engages Cisco's Software Support Service for implementation and training support.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $287,000.

> "Having Cisco's ISE and Secure Firewall [with Cisco Security Suites] has allowed us to have consistent policies, which means that we don't have to train users on how to do things over and over and over. The learning curve is basically flat … because it's the same thing."
>
> CYBERSECURITY MANAGER, B2C COMMERCE

Implementation And Training						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
I1	Total resources dedicated to the implementation effort	Interviews	15	10	5	0
I2	Average hours of implementation effort per resource	Interviews	104	52	26	0
I3	Blended fully burdened hourly rate for an implementation resource	Composite	$59	$59	$59	$59
I4	**Subtotal: internal implementation costs**	**I1*I2*I3**	**$92,040**	**$30,680**	**$7,670**	**$0**
I5	**Subtotal: external implementation costs**	**Interviews**	**$50,000**	**$25,000**	**$12,500**	**$0**
I6	New trainees	I1	15	10	5	0
I7	Hours of new user training, per trainee	Interviews	16	16	16	16
I8	Ongoing trainees	$I6_{PY}$+I6	0	15	25	30
I9	Annual ongoing training for existing users	Interviews	4	4	4	4
I10	**Subtotal: training costs**	**I3*((I6*I7)+(I8*I9))**	**$14,160**	**$12,980**	**$10,620**	**$7,080**
It	Implementation and training	I4+I5+I10	$156,200	$68,660	$30,790	$7,080
	Risk adjustment	↑15%				
Itr	Implementation and training (risk-adjusted)		$179,630	$78,959	$35,409	$8,142
	Three-year total: $302,140			**Three-year present value: $286,791**		

PLATFORM ADMINISTRATION

Evidence and data. As with implementation, interviewees underscored the value of Cisco Security Suites' technical support and operational guidance, Cisco's Software Support Service. They noted that this combination of internal and vendor-supplied efforts added to the efficiency of their Zero Trust architecture with Cisco products.

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

- As the composite stands up the Zero Trust environment with Cisco Security Suites, it partially dedicates technology resources to maintaining the Cisco Security architecture. These resources are further supported by Cisco's Software Support Service.

- At full deployment, platform administration requires the labor equivalent of 20% of two FTEs, or 1,664 hours. Over the investment period, the composite:
    - Completes 25% of its transition to Zero Trust architecture enabled by Cisco Security and requires 416 hours of platform administration in Year 1.
    - Completes 55% of its transition to Zero Trust architecture enabled by Cisco Security and requires 915 hours of platform administration in Year 2.
    - Completes 70% of its transition to Zero Trust architecture enabled by Cisco Security and requires 1,165 hours of platform administration in Year 3.
- The fully burdened hourly rate of an administrator is $59.

Risks. Forrester recognizes that these results may not be representative of all experiences. The following factors may impact this cost:

- The percentage of total users supported by Cisco Security architecture and an organization's adoption ramp.
- An organization's security maturity and its progress toward Zero Trust principles prior to Cisco Security Suites.
- The extent to which an organization engages Cisco's Software Support Service for platform administration support.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $130,000.

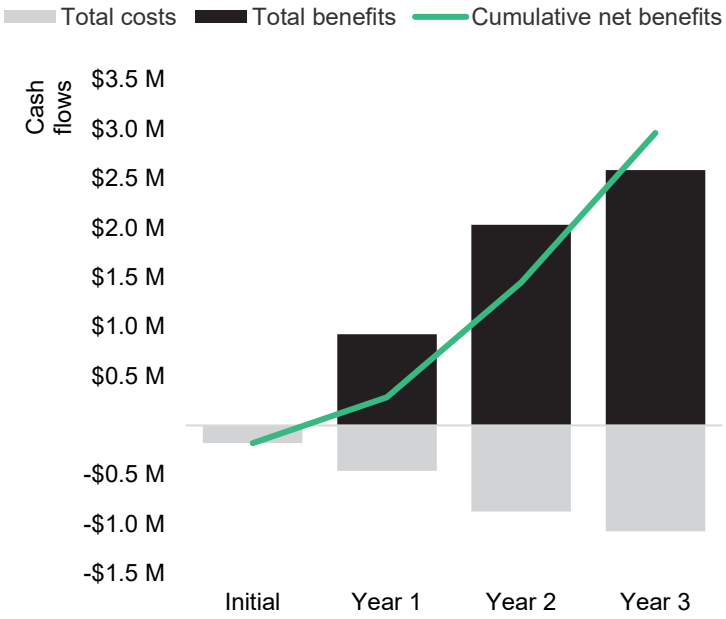
> "When you have a [Cisco Security Suite] care team to help handle [implementation and support], it just takes you to levels that you didn't even know you could go to."
>
> CYBERSECURITY MANAGER, B2C COMMERCE

Platform Administration						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
J1	Total hours dedicated to maintaining Cisco Security environment	Interviews	0	1,664	1,664	1,664
J2	Percentage reduction in legacy costs with transition to Zero Trust architecture with Cisco Security	A3	0%	25%	55%	70%
J3	Fully burdened hourly rate of an administrator	Composite	$59	$59	$59	$59
Jt	Platform administration	J1*J2*J3	$0	$24,544	$53,997	$68,723
	Risk adjustment	↑10%				
Jtr	Platform administration (risk-adjusted)		$0	$26,998	$59,397	$75,595
	Three-year total: $161,990			**Three-year present value: $130,428**		

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	($179,630)	($459,151)	($871,832)	($1,072,680)	($2,583,292)	($2,123,482)
Total benefits	$0	$924,281	$2,033,449	$2,588,032	$5,545,763	$4,465,219
Net benefits	($179,630)	$465,130	$1,161,618	$1,515,353	$2,962,471	$2,341,737
ROI						110%
Payback						<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."

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

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

APPENDIX B: ENDNOTES

[1] Source: Zero Trust Everywhere Is The Security Model Of The Future, Forrester Research, Inc., September 5, 2024.

[2] Source: The Definition Of Modern Zero Trust, Forrester Research, Inc., April 22, 2024.

[3] Source: The Business Of Zero Trust Security, Forrester Research, Inc., July 11, 2023. A material breach is defined as a the compromise of an organization's sensitive data is or in the past 12 months per year. A data breach can be defined as the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information. Source: The National Association of Attorneys General.

[4] 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.

[5] Source: Forrester's Security Survey, 2023. Base: 830 security decision-makers with network, data center, app security, or security ops responsibilities at companies with $10 million in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[6] Ibid.

[7] Note: Data-center-to-data-center workloads are excluded from this analysis.

[8] Source: Forrester's Security Survey, 2023. Base: 830 security decision-makers with network, data center, app security, or security ops responsibilities at companies with $10 million in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

FORRESTER®