A Forrester Total Economic Impact™ Study

Commissioned By

Cisco

Project Director:
Michelle S. Bishop

September 2016

The Total Economic Impact™ Of Cisco TrustSec

Simplified Security Engineering And Reduced Operations Costs Enabled By Cisco

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Executive Summary

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 TrustSec software-defined segmentation. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cisco on their organizations.

> **"TrustSec simplifies the security access model and allows for much less policy maintenance."**
>
> **— Enterprise architect, educational institution**

To better understand the benefits, costs, and risks associated with TrustSec, Forrester interviewed four customers that had deployed TrustSec. The TrustSec software-defined segmentation solution simplifies the provisioning and management of highly secure access to network services and applications. Unlike access control mechanisms that work on network topology, TrustSec policies use logical grouping. Highly secure access is consistently maintained even as resources are moved in mobile and virtualized networks. A more detailed description of TrustSec is available on the Cisco TrustSec Overview page in this document.

The customers interviewed had a range of goals for their TrustSec implementations which included risk mitigation and compliance as well as increased IT operations efficiency. These customers wanted to protect their applications in all their locations and control and limit access to approved assets. TrustSec use cases for the customers interviewed included managing mobile access for tablets and phones, managing network segmentation across the organization, restricting access to critical applications in the data center, and moving to an identity-based access model for all resources.

TRUSTSEC REDUCES OPERATIONAL COSTS, SIMPLIFIES SECURITY ENGINEERING, AND INCREASES AGILITY

Our interviews with four existing customers and subsequent financial analysis found that a composite organization based on these organizations experienced the risk-adjusted ROI, benefits, and costs shown in Figure 1.[1]

The composite organization analysis points to benefits of $3,989,498 versus implementation costs of $1,663,914, adding up to a net present value (NPV) of $2,325,584. TrustSec enabled the organizations interviewed to reduce operational costs, with the cost avoidance of an alternative traditional perimeter-based security solution; reduce additional IT operations headcount required; and improve network resilience with a lower risk of downtime.

Other benefits cited by the interviewed organizations include faster time-to-market for project rollout, consistent and effective network segmentation, simplified security engineering with simplification of the security policy, improved automated firewall rule management, improved agility,ability to scale security policy, improved security posture for the network, and improved regulatory compliance.

FIGURE 1

Financial Summary Showing Three-Year Risk-Adjusted Results

ROI: 140%

NPV: $2.33 million

IT Operational costs: ▼ as much as 80%

Time to implement network changes: ▼ 98%

Source: Forrester Research, Inc.

- **Benefits.** The composite organization experienced the following risk-adjusted present value benefits that represent those experienced by the interviewed companies:

- **Savings from cost avoidance of alternative traditional solution.** By using TrustSec instead of an alternative traditional segmentation solution such as VLANs and firewalls, the composite organization was able to save over $2.7 million over the three-year analysis.
- **Reduction in IT operations cost.** TrustSec reduces administration costs for access management, particularly when considering the administration effort required for more traditional solutions, such as VLANs and firewalls. Organizations interviewed reported a reduction in operational costs ranging from 25% to 80%. Without TrustSec, the composite organization would have had to hire an additional four network engineers; therefore, the composite organization saved $945,402.
- **Improved network resilience with lower risk of downtime.** TrustSec also improves the network resilience of an organization, leading to a lower risk of downtime. At 1 hour of downtime reduced per year for 4,000 users, the downtime reduction savings for the composite organization is quantified at $319,716.
- Other benefits experienced by the interviewed organizations include
    - **Faster time-to-market for project roll-out**
    - **Simplified and automated firewall rule management plus associated operational savings**
    - **Improved regulatory compliance**
    - **Consistent and effective network segmentation**
    - **Simplified security engineering with simplification of security policy**
    - **Improved agility and ability to scale security policy**
    - **Increased security posture for the network**

› **Costs.** Implementing traditional or TrustSec software-defined segmentation have associated costs. Traditional segmentation costs are considered in Table 1. The composite organization experienced the following risk-adjusted present value costs for TrustSec software-defined segmentation:

- **TrustSec infrastructure costs.** The composite organization spent $346,500 on TrustSec infrastructure. This includes the cost of the Cisco Identity Services Engine (ISE) appliance and associated licenses. This does not include network upgrades, as the composite organization timed its TrustSec implementation with its scheduled life-cycle replacement of network infrastructure.
- **Cisco Advanced Services costs.** The composite organization used Cisco Advanced Services for low-level and high-level design at a cost of $231,000. Not all customers interviewed used Cisco Advanced Services when they planned their TrustSec implementation.
- **Professional services fees.** The composite organization also incurred $404,250 in professional services fees for its implementation of TrustSec. Not all customers interviewed use professional services in their TrustSec implementation.
- **Internal labor for implementation and testing.** The composite organization spent $130,680 for its six-month implementation of TrustSec.
- **Ongoing administration and support costs.** The composite organization had two engineers for ongoing administration and testing of regular software updates for the network, resulting in $551,484 in costs over the three-year analysis.

Disclosures

The reader should be aware of the following:

- The 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 report to determine the appropriateness of an investment in TrustSec.

- 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.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering implementing Cisco TrustSec. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision, to help organizations understand how to take advantage of specific benefits, reduce costs, and improve the overall business goals of winning, serving, and retaining customers.

APPROACH AND METHODOLOGY

Forrester took a multistep approach to evaluate the impact that Cisco can have on an organization (see Figure 2). Specifically, we:

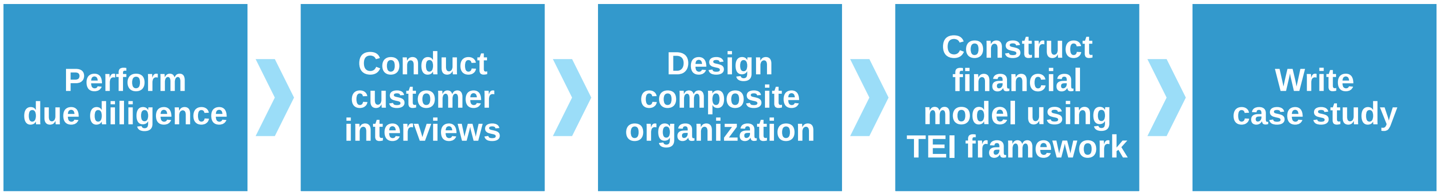
- Interviewed Cisco marketing, sales, and consulting personnel, along with Forrester analysts, to gather data relative to TrustSec and the network security market in general.
- Interviewed four organizations currently using TrustSec to obtain data with respect to costs, benefits, and risks.
- Designed a composite organization based on characteristics of the interviewed organizations (see Appendix A).
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews (as applied to the composite organization).
- Risk-adjusted the financial model based on issues and concerns the interviewed organizations highlighted in interviews. Risk adjustment is a key part of the TEI methodology. While interviewed organizations provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling TrustSec: benefits, costs, flexibility, and risks.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix B for additional information on the TEI methodology.

FIGURE 2

TEI Approach


Perform due diligence
Conduct customer interviews
Design composite organization
Construct financial model using TEI framework
Write case study

Source: Forrester Research, Inc.

Analysis

COMPOSITE ORGANIZATION

For this study, Forrester conducted interviews with representatives from the following four companies, which are Cisco customers:

- A corporate retail group with 1,350 stores. It has 20 office locations and two major data centers.
- An educational research institution with 80,000 wired ports spread over 74 buildings.
- A central and commercial bank with 20 locations, serving, with its subsidiaries, over 30 million customers.
- A retail and commercial bank with 2,700 sites and over 75,000 employees.

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization that Forrester synthesized from these results represents an organization with the following characteristics:

- It is a financial services organization with approximately 4,000 employees.
- It has 30,000 LAN ports with 250 switches and 50 routers.
- Its goal for network segmentation was to implement global traffic tiers, with different work groups for users, applications, and databases. It wanted to limit traffic between those groups, for example, where certain users could access particular application services but not database services.

INTERVIEW HIGHLIGHTS

Situation

The main drivers for the organizations interviewed for moving to TrustSec were risk mitigation and improved security operations efficiency. Highlights from discussions with the companies interviewed include:

- One of the companies interviewed noted its TrustSec implementation was part of an overall network security risk mitigation program. Given the size and scale of its network, the focus for this company was to: 1) restrict access to specific critical applications in the data center and 2) improve situational awareness of the network. With TrustSec, the company wanted to protect applications in the data center, headquarters, and branch offices by controlling and limiting access to approved assets and restricting access to resources and applications to authorized users.
- Organizations interviewed also highlighted their need to increase security operations efficiency in order to increase their ability to grow and scale security operations. One organization interviewed noted that it moved to TrustSec to gain better control of its access policy to its resources. It wanted to change from an “allowed machine”-based model to an “allowed user”-based model and move to identity networking. Another interviewee noted that pre-TrustSec, the organization achieved

> *“With TrustSec, you have no bandwidth restrictions versus the firewall approach. So we have less investment risk with TrustSec. And from an operational cost point of view, TrustSec is quite inexpensive.”*
>
> ~ Head of network services, interviewed organization

microsegmentation by having like users in the same VLANs, leading to significant costs for managing all these VLANs.

- Regulation was a driver for one company interviewed that used TrustSec to address segmentation, and limit network access to authorized users. This financial services organization wanted segmentation not just at the box but also at the access point. The goal for this organization was to pass network security audits administered by its industry regulators.

- The retail organization interviewed implemented TrustSec as part of its initiative to give mobile access from its employees' tablets and phones. Its goal was to create different groups of users with different access levels for their mobile devices in retail stores, all based on Active Directory. The organization noted that since it already had Cisco Adaptive Security Appliance (ASA) firewalls and ISE, it had the necessary components for this approach. It would be simple for it to assign security tags to different kinds of users. TrustSec would be a good way to differentiate users across mobile devices.

- One interviewed organization observed that its choice of TrustSec for label-based security was based on the nature of its network. It had a large traditional network with over 380,000 active devices, and it noted that other label-based approaches would not address the other 80% of its network.

> *"We looked at other options for label-based security, such as software-defined networking approaches. But with a big traditional network like ours, with traditional kits and mainframes, TrustSec was our choice. With the other options, we couldn't tackle 80% of our network."*
>
> ~ Chief network architect, network security, financial services organization

Solution

The composite organization evaluated different alternatives for implementing network segmentation with a view toward mitigating risk, creating an efficient IT operations model that would scale with the company's growth as well as address requirements of its regulatory environment. The scope for this segmentation project included its data center as well as all its bank locations. To meet financial regulatory requirements, the composite organization evaluated firewalls and TrustSec software-defined segmentation. VLAN-based segmentation was not considered sufficient to address the regulators' requirements. After evaluating the larger firewall investment over time, and considering that the bank already had TrustSec-capable network infrastructure, the composite organization chose to implement TrustSec.

Customers interviewed considered VLANs in addition to firewalls as segmentation solutions that were alternatives to TrustSec software-defined segmentation. However, there are other TrustSec use cases that organizations may use that add to its total value. These use cases include:

- Rapid threat containment to isolate attacks and vulnerable devices
- Restrict the lateral movement of threats with micro-segmentation
- Reduce the scope of compliance for regulations such as PCI
- Segment IoT devices
- Simplify extranet access controls for business partners and supplier connections
- Extend enterprise security policies to hybrid cloud and multi-cloud environments

Readers of this study should consider their own use case for TrustSec and the particular alternatives involved for their use case, when evaluating an investment in TrustSec.

Results

The interviews with TrustSec customers revealed the following benefits:

- **Savings from cost avoidance of alternative traditional network security solutions.** By implementing TrustSec, a number of interviewed organizations noted that they were able to avoid the cost of implementing and managing VLANs and firewalls, which are a more traditional perimeter-based model for network security. As one chief network architect observed: "It's quite costly to manage network security with firewalls. That soft center, hard outside model is an all-or-nothing approach. With TrustSec, we have a degree of control rather than security elements relying on the perimeter. TrustSec is attractive because it can be implemented, in theory, on existing network infrastructure by configuration. You don't have to implement expensive firewalls. It's not just the kit costs, but project rollout, definition, and testing." Another interviewee also observed that when making choices for network segmentation, "We took a look at prospective operation cost, network resilience, bandwidth restrictions, and firewall capacity, which can be a chokepoint. And with TrustSec, you have no bandwidth restrictions. So we have less investment risk with TrustSec versus a firewall. TrustSec is also less time consuming. From a mere operational point of view, TrustSec is quite inexpensive."

- **Increased operational efficiency, leading to avoidance of additional IT headcount.** A common theme among the organizations interviewed was their increased IT operational efficiency as a result of their TrustSec implementation. Without TrustSec, a number of these organizations would have had to hire additional IT network operations resources to achieve a similar level of functionality for access management in a more traditional deployment.

  > "Without TrustSec, we would have used ISE, but instead of security tagging, we would have used VLANs, and the network, and different policies. So we'd be working with six to eight different policies instead of just one. So with TrustSec, the network is a lot easier to maintain and administer. We've reduced operations costs and saved a quarter of an employee."
  > *— IT network architect, corporate retailing group*

> *"If we had to do this with firewalls instead of TrustSec, I estimate that we would have had to hire 10 more FTEs."*
>
> ~ Chief network architect, voice and domain networks, financial services organization

- **Improved network resilience with lower risk of downtime.** By using TrustSec instead of a more traditional perimeter-based approach, organizations were also able to lower risk, reduce complexity, and reduce downtime.

  > "If we didn't use TrustSec, I'd have to compare it with the next best alternative. If I used a firewall-approach, I'd have to coordinate two engineering groups, network engineers and security engineers, when solving problems. Firewall segmentation just adds a layer of complexity. We've increased the resilience of the network overall."
  > *— Head of network services, interviewed organization*

- **Faster time-to-market for project rollout by as much as 98% as compared to a VLAN-based segmentation approach.** Interviewed organizations also gained improved agility with their TrustSec deployment. They found that they could get to market faster for projects such as bring your own device (BYOD). The interviewees also noted that security policy and other network access changes could be implemented faster. As one financial services organization noted, "When you use firewalls, it can be quite onerous to get changes made to the infrastructure from a security point of view." Due to the risk-averse nature of its industry, a routine change to a traditional firewall environment would take over four to six weeks, while an emergency change would still take several days.

  One retail organization that used TrustSec to manage mobile access from tablets and phones for over 5,500 access points found that the time to implement changes was reduced by as much as 98%. In 30 minutes, the organization was able to implement a change of policy that allows mobile users on the corporate office network to use the store network, which is on a different wireless network. The organization estimated that without TrustSec, implementing this change would have taken between one to two days.

> “We can do changes a lot faster and simpler without having to rebuild by using TrustSec.”
> *— IT network architect, corporate retailing group*

- **Simplified and automated firewall rule management, with associated operational savings.** With TrustSec, the interviewed organizations gained improved and automated firewall rule management. Automation of firewall rules and access control list (ACL) administration also led to reduced costs for these companies.

- **Regulatory compliance.** For a number of these companies, the regulatory compliance was one of the leading benefits of their TrustSec implementation. One bank noted that its regulators were “happy with the solutions.” Regulators approved of the user rights management approach of the bank, as it linked network security to the user and application role using TrustSec.

> “TrustSec lets us design user models for every application type and business process, and then write the user rights according to that user model. With that user role, network communications roles are defined. It’s just one click. If they have a new role, access changes instantaneously. Auditors were happy with this approach that did not end in the application environment, which would then have to go up two layers of communication to get approved.”
> *— Head of network services, interviewed organization*

> “This cyberthreat program that TrustSec is a part of is about delivering risk mitigation for an acceptable price. We want to mitigate financial and reputational risk. There are devastating business effects if a regulator publicly names and shames us. It’s an arms race and we need to anticipate problems based on emerging trends.”
> *— Chief network architect, network security, financial services organization*

- **Consistent and effective network segmentation.** All interviewed organizations reported that they were able to benefit from consistent and effective network segmentation with TrustSec. These organizations noted that TrustSec was more cost effective, as it enabled them to control access based on defined user roles and Active Directory. This automated access management meant they did not have to expend much manual effort on network segmentation.

- **Simplified security engineering with simplification of security policy.** Organizations also consistently cited simplified security engineering with a simplified security policy as a direct benefit of their TrustSec implementation. The ability to set security policy based on identity and not on IP address was a key part of this simplification.

> “Security policies are easier to understand, shorter, and easier to read. We’ve increased security with TrustSec”
> *— IT network architect, corporate retailing group*

- **Improved agility and ability to scale security policy.** By using TrustSec versus the more traditional firewall-based approach, companies were also able to increase their agility and improve their ability to scale security policy. One organization noted that firewall changes are seen as a major challenge for starting new projects. With TrustSec, new changes can now be implemented faster. This simplifies requirements for future projects. Another interviewed organization also noted that with TrustSec, it could scale its security policy and implement new projects faster. “We’re a little bit more agile with zoning [segmentation],” the head of network services remarked. “We don’t have to calculate

> *“We committed to the regulators to mitigate risks with appropriate and demonstrable controls. TrustSec is the most cost-effective way to deliver this commitment because of the sheer complexity of trying to put firewalls everywhere.”*
>
> ~ Chief network architect, network security, financial services organization

if the additional load can be handled by the firewall.” This also made projects more predictable and saved some project time.

- **Improved security posture for the network.** The organizations interviewed also cited improved security as a benefit of their TrustSec implementation. These organizations saw an improved security posture for the network, increased visibility, and, for some, improved cyber threat defense and improved data center security.

> “It’s all about having access rules based on what type of user you are and not the IP address, so we have a deeper knowledge about who is doing what. We can then correlate a security breach to a particular account. TrustSec gives us visibility. It’s who versus where.”
>
> *— IT network architect, corporate retailing group*

BENEFITS

The composite organization experienced a number of quantified benefits in this case study.

- Savings from cost avoidance of an alternative perimeter-based solution.
- IT operations cost savings.
- Improved network resilience with lower risk of downtime.

Cost Avoidance of Alternative Traditional Perimeter-Based Solutions

Organizations interviewed stated that TrustSec was the lower cost choice when considering other alternative solutions. One retail organization would have had to implement a VDI (virtual desktop infrastructure) solution to provide differentiated access levels for mobile users at the store level without TrustSec and incur the associated costs. With TrustSec, it has one pool of users allocated to one resource. One IT network architect noted that without TrustSec, “We would have different pools for different users and waste a lot of hardware. We would need extra space — five different pools for VDIs and space at the top of the pools.”

Organizations that evaluated more traditional perimeter-based solutions such as firewalls instead of TrustSec also noted the higher cost of this alternative. One organization estimated that to implement a firewall configuration that would meet its high-capacity and high-resilience network requirements would cost a total of $330,000. To replicate the functionality of a TrustSec implementation, it would have to implement an additional 400 firewalls, making this alternative cost-prohibitive. Another organization noted that while it had made a large initial investment in TrustSec, it had no annual maintenance costs compared with an alternative solution. In addition to these annual savings, the organization had lower investment risk compared with a firewall implementation, with one interviewee noting: “As volume rises over the firewall, there is a need for heavy reinvestment in firewall equipment. You don’t have to do that with TrustSec.”

By using TrustSec instead of an alternative traditional perimeter-based solution, the composite organization was able to avoid an initial infrastructure investment of $1.65 million and $550,000 in annual ongoing maintenance for this traditional solution. The total savings to the organization is $3.3 million over three years.

The interviewed organizations had varying use cases for their TrustSec implementations. These cost avoidance savings varied per organization and, to account for this variability, this benefit was risk-adjusted and reduced by 5%. The risk-adjusted total benefit resulting from cost avoidance of a traditional perimeter-based solution was $3,135,000. Details of this calculation are shown in Table 1 below. See the section on Risks for more detail.

TABLE 1

Cost Avoidance of Alternative Solution

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total	Present Value
A1	Initial infrastructure investment		$1,650,000				
A2	Ongoing maintenance		$550,000	$550,000	$550,000		
At	Cost avoidance of alternative traditional perimeter-based security solution	A1+A2	$2,200,000	$550,000	$550,000	$3,300,000	$2,867,769
	Risk adjustment	↓5%					
Atr	**Cost avoidance of alternative traditional perimeter-based security solution (risk-adjusted)**		**$2,090,000**	**$522,500**	**$522,500**	**$3,135,000**	**$2,724,380**

Source: Forrester Research, Inc.

Operational Cost Savings

The organizations interviewed also cited operational cost savings as a benefit of their TrustSec implementations. The “ease of management” of TrustSec compared with other solutions fed into these savings. One organization estimated that TrustSec brought an 80% reduction in time spent by network and security engineers on access management. This would include time spent on the implementation of role changes and the approval process. As another company stated, “We would have needed more people, not for the day-to-day work but for when we do changes, implement new roles, or when a new person has access.” Interviewees noted that without TrustSec, they would need to hire additional IT operations personnel. Savings from avoiding the cost of hiring this additional headcount ranged from one to 10 FTE’s (full-time equivalent) for the companies interviewed. These savings represent a reduction in IT operational costs from 25% to 80% for the companies interviewed.

Without TrustSec, the composite organization would have had to hire an additional four network engineers. At an average annual fully loaded cost of $105,600 per engineer this translates to IT operations cost avoidance savings of $422,400 per year.

Forrester risk-adjusted this calculation by 10% to account for variability to an annual benefit of $380,160. Over three years the total operational cost savings to the composite organization were $1.14 million. The details of this calculation are shown in Table 2. See the section on Risks for more detail.

TABLE 2
Operational Cost Savings

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total	Present Value
B1	Number of additional network engineers (saved)		4	4	4		
B2	Yearly rate per person		$105,600	$105,600	$105,600		
Bt	Operational cost savings — additional FTE	B1*B2	$422,400	$422,400	$422,400	$1,267,200	$1,050,446
	Risk adjustment	↓10%					
Btr	**Operational cost savings — additional FTE (risk-adjusted)**		**$380,160**	**$380,160**	**$380,160**	**$1,140,480**	**$945,402**

Source: Forrester Research, Inc.

Improved Network Resilience — Lower Downtime Risk

Improved network resilience was also a benefit of a TrustSec implementation. A more traditional network solution such as a firewall would add a layer of complexity and require more coordination among different groups during issue resolution.

The head of network services also noted that business losses as a result of downtime could run into the millions for a financial services organization, particularly if this downtime affected the trading floor.

By using TrustSec, the composite organization was able to lower incident time-to-resolution and improve network resilience. This resulted in lower downtime risk for the organization and is quantified at 1 hour of downtime avoided per major incident. At a major incident rate of one a year, TrustSec has saved the organization from revenue impact loss as a result of downtime and also employee time loss. To be conservative, in this analysis Forrester quantifies lower downtime risk in terms of employee time saved. The downtime cost per user per hour is calculated as a function of average hourly employee compensation. Readers of this study can also choose to consider the business impact of downtime to their organizations in their own evaluations.

With 4,000 users and an hourly downtime cost per user of $37.81, the total quantified savings due to improved network resilience with lower risk of downtime is $151,250 per year. To account for the wide variation in downtime cost per company this benefit was risk-adjusted by 15%. The risk-adjusted total benefit resulting from lower downtime per year was $128,563. Over three years, this saved the organization $385,688. Details of this calculation are shown in Table 3 below. See the section on Risks for more detail.

TABLE 3

Improved Network Resilience With Lower Risk of Downtime

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total	Present Value
C1	Number of users		4,000	4,000	4,000		
C2	Number of incidents a year		1	1	1		
C3	Downtime cost per user		$37.81	$37.81	$37.81		
Ct	Improved network resilience with lower risk of downtime	C1*C2*C3	$151,250	$151,250	$151,250	$453,750	$376,136
	Risk adjustment	↓15%					
Ctr	**Improved network resilience with lower risk of downtime (risk-adjusted)**		**$128,563**	**$128,563**	**$128,563**	**$385,688**	**$319,716**

Source: Forrester Research, Inc.

Total Benefits

Table 4 shows the total of the benefits listed above, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of approximately $4 million.

TABLE 4

Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Year 1	Year 2	Year 3	Total	Present Value
Atr	Cost avoidance of alternative traditional perimeter-based security solution	$2,090,000	$522,500	$522,500	$3,135,000	$2,724,380
Btr	Operational cost savings	$380,160	$380,160	$380,160	$1,140,480	$945,402
Ctr	Improved network resilience with lower risk of downtime	$128,563	$128,563	$128,563	$385,688	$319,716
	Total benefits (risk-adjusted)	**$2,598,723**	**$1,031,223**	**$1,031,223**	**$4,661,169**	**$3,989,498**

Source: Forrester Research, Inc.

COSTS

The composite organization experienced a number of costs associated with TrustSec:

- TrustSec infrastructure costs.
- Cisco Advanced Services — TrustSec design fees.
- Professional services fees.
- Internal labor for implementation and testing.
- Ongoing administration and support.

These represent the mix of internal and external costs experienced by the composite organization for initial planning, implementation, and ongoing maintenance associated with the solution.

TrustSec Infrastructure Costs

Organizations interviewed emphasized the importance of planning and ensuring that their network infrastructure was compatible with TrustSec. One interviewee noted that certain device categories would not be "TrustSec capable," but their organization was able to avoid any additional network infrastructure cost because it already had "upper class" equipment from the Cisco 3800 and 4000 series. Readers should also note that TrustSec can operate in mixed device (TrustSec-compliant and non-compliant networks). Forrester recommends consulting with Cisco on network infrastructure requirements for TrustSec for your particular use case.

The composite organization timed its TrustSec implementation after its network life-cycle replacement was scheduled. This ensured that it would not have to incur any additional infrastructure costs for TrustSec. It invested $330,000 in a Cisco ISE appliance and associated licenses. To account for variability in the estimates, we risk-adjusted these fees up by 5%, for a total of $346,500 over the three-year analysis.

As costs will differ per organization based on the use cases implemented for TrustSec, the infrastructure costs for a TrustSec implementation may vary widely, especially in cases where TrustSec is implemented outside a typical network life-cycle refresh. Forrester urges readers to take into consideration their own environment and use case for TrustSec and consult with Cisco to estimate their own TrustSec infrastructure costs.

Cisco Advanced Services — TrustSec Design Fees

The composite organization paid Cisco $220,000 in fees for high-level and low-level design services for its TrustSec implementation. These fees for Cisco Advanced Services came to $220,000. After a risk adjustment up by 5%, this brings the total to $231,000.

Professional Services Fees

The composite organization also paid $385,000 in professional services for its TrustSec implementation. The use of professional services for a TrustSec implementation was typically dependent on an organization's appetite for partnering with outside consultants for IT projects. Half of the organizations interviewed used professional services. We risk-adjusted these fees up by 5%, for a total of $404,250 over the three-year analysis.

Internal Labor for Implementation And Testing

A number of interviewees noted that they invested a fair amount of internal resources in testing versus just operating the TrustSec solution. "We have a lot of investment in testing switches compared to before," one head of network services observed. The composite organization had two senior IT operations staff members spend six months full time on the TrustSec implementation. At an annual rate per person of $118,800, the internal labor cost of a TrustSec implementation for the composite organization is $118,800. Given the variability in implementation, we risk-adjusted this internal labor cost up by 10%, for a total of $130,680.

We should note that the use case for TrustSec has a significant effect on project duration for the implementation phase. One customer interviewed had granular requirements for access that initially did not fit into Cisco’s binary architecture for TrustSec. As a result, the organization experienced a delay in the implementation process, as it had to wait for Cisco to add this technical feature to the product.

TABLE 5
Internal Labor — Implementation And Testing

Ref.	Metric	Calculation	Initial	Year 2	Year 3	Total	Present Value
G1	Number of engineers required for initial implementation		2				
G2	Length of implementation time (months)		6				
G3	Yearly rate per person		$118,800				
Gt	Internal labor — implementation and testing	(G1*G2)+G3	$118,800			$118,800	$118,800
	Risk adjustment	↑10%					
Gtr	**Internal labor — implementation and testing(risk-adjusted)**		**$130,680**			**$130,680**	**$130,680**

Source: Forrester Research, Inc.

Ongoing Administration and Support Costs

While recognizing the more time-consuming work of testing new releases for TrustSec, one interviewed organization noted that this cost would not grow as it expanded its network, in sharp contrast to a more traditional solution. “It’s a fixed value. It doesn’t rise as the network grows. If it’s 1,000 switches or 50 switches it’s the same effort. But if you add 50 more firewalls we would have to add 10 more people.”

The composite organization also allocated two IT operations engineers for ongoing testing for regular software updates in the network and administration of the solution. This administration would also include troubleshooting, the evaluation of features, and other nonoperational efforts on TrustSec. At a fully loaded compensation of $105,600 per IT operations engineer, the ongoing administration and testing costs to the composite organization are $211,200 per year. To account for variability in the resources needed for ongoing administration and testing for TrustSec, we risk-adjusted this total up by 5%, leading to a total cost of $221,760 per year.

TABLE 6
Administration And Testing Costs

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total	Present Value
H1	Number of people		2	2	2		
H2	Yearly rate per person		$105,600	$105,600	$105,600		
Ht	Administrative and testing costs	H1*H2	$211,200	$211,200	$211,200	$633,600	$525,223
	Risk adjustment	↑5%					
Htr	**Administrative and testing costs (risk-adjusted)**		**$221,760**	**$221,760**	**$221,760**	**$665,280**	**$551,484**

Source: Forrester Research, Inc.

Total Costs

Table 7 shows the total of all costs as well as associated present values, discounted at 10%. Over three years, the composite organization expects costs to total a net present value of approximately $1.66 million.

TABLE 7
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	TrustSec infrastructure costs	$346,500	$0	$0	$0	$346,500	$346,500
Etr	Cisco Advanced Services — TrustSec design fees	$231,000	$0	$0	$0	$231,000	$231,000
Ftr	Professional services — implementation	$404,250	$0	$0	$0	$404,250	$404,250
Gtr	Internal labor — implementation and training	$130,680	$0	$0	$0	$130,680	$130,680
Htr	Administrative and testing costs	$0	$221,760	$221,760	$221,760	$665,280	$551,484
	Total costs (risk-adjusted)	**$1,112,430**	**$221,760**	**$221,760**	**$221,760**	**$1,777,710**	**$1,663,914**

Source: Forrester Research, Inc.

FLEXIBILITY

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the “right” or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement TrustSec and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> “We did a lot of work with Cisco to develop this vision of a security environment, to allow third-party providers to interact with TrustSec. We now have a multivendor ecosystem with TrustSec.”
>
> *— Chief network architect, network security, financial services organization*

Organizations could see additional benefits as they implement more projects that would require network segmentation. For example, one interviewee implemented a new eBusiness environment with TrustSec and estimated that using a firewall would have added a couple of weeks to the projects and likely resulted in additional hardware costs. Cost avoidance savings and project implementation time saved are benefits that these companies may get with every future project they add to the network. Network expansion, such as mergers and acquisitions, would also bring additional benefits to these organizations. A number of organizations did note that as Cisco expanded and added features to their product set, they could gain more benefits from TrustSec. These companies could now get better value out of their existing software and other vendor products through the Cisco Platform Exchange Grid (pxGrid). And as Cisco adds new control and more analytics capabilities to the TrustSec product set, organizations could gain more benefits around security decision-making.

The value of flexibility is unique to each organization, and the willingness to measure its value varies from company to company.

RISKS

Forrester defines two types of risk associated with this analysis: “implementation risk” and “impact risk.” Implementation risk is the risk that a proposed investment in TrustSec may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in TrustSec, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 8
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Cost avoidance of alternative traditional perimeter-based security solution	↓ 5%
Operational cost savings	↓ 10%
Improved network resilience with lower risk of downtime	↓ 15%
Costs	**Adjustment**
Internal labor — implementation and training	↑ 10%
All other TrustSec costs	↑ 5%

Source: Forrester Research, Inc.

Quantitatively capturing implementation risk and impact risk by directly adjusting the financial estimates results provides more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as “realistic” expectations since they represent the expected values considering risk.

The following impact risks that affect benefits are identified as part of the analysis:

- Customer benefits could vary depending on the environment, number of users, and particular use cases for TrustSec.
- Cost of downtime will vary per customer and how the benefit of improved network resilience is evaluated.

The following implementation risks that affect costs are identified as part of this analysis:

- Costs to implement TrustSec will vary greatly, depending on the customers’ current network environment and size of the implementation. Costs will increase should a customer also need to upgrade its network equipment to TrustSec-compatible devices outside of a regularly scheduled network infrastructure refresh.
- Organizations will have variable requirements for their TrustSec implementation of Cisco depending on the current structure of their network operations and security teams.

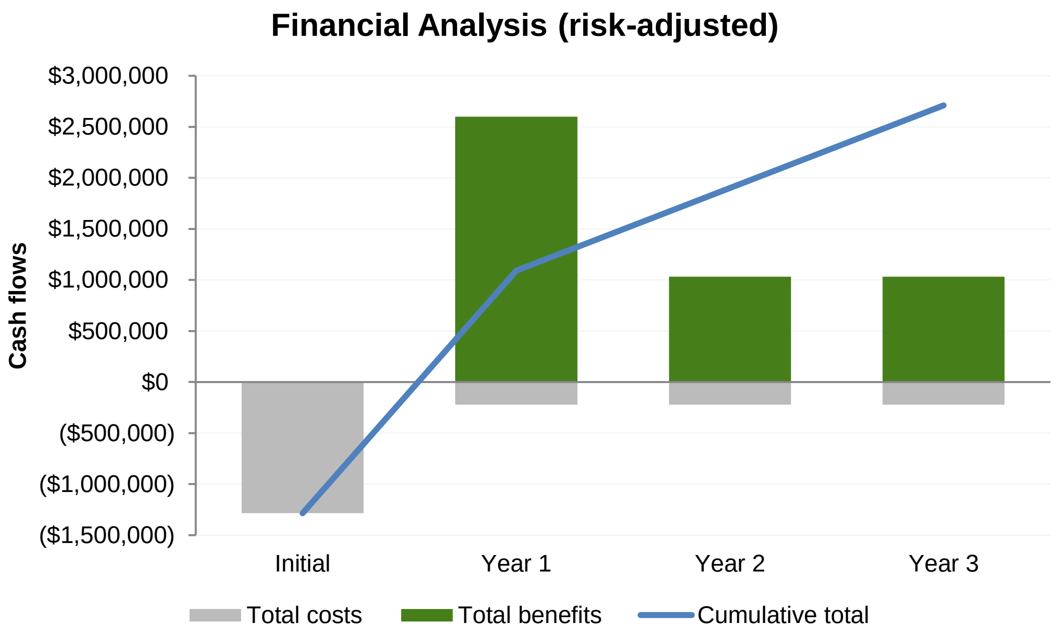
Table 8 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the composite organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

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 in TrustSec.

Table 9 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 8 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 3
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 9
Cash Flow (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	($1,112,430)	($221,760)	($221,760)	($221,760)	($1,777,710)	($1,663,914)
Benefits	$0	$2,598,723	$1,031,223	$1,031,223	$4,661,169	$3,989,498
Net benefits	**($1,112,430)**	**$2,376,963**	**$809,463**	**$809,463**	**$2,883,459**	**$2,325,584**
ROI						**140%**
Payback period						**5.6 months**

Source: Forrester Research, Inc.

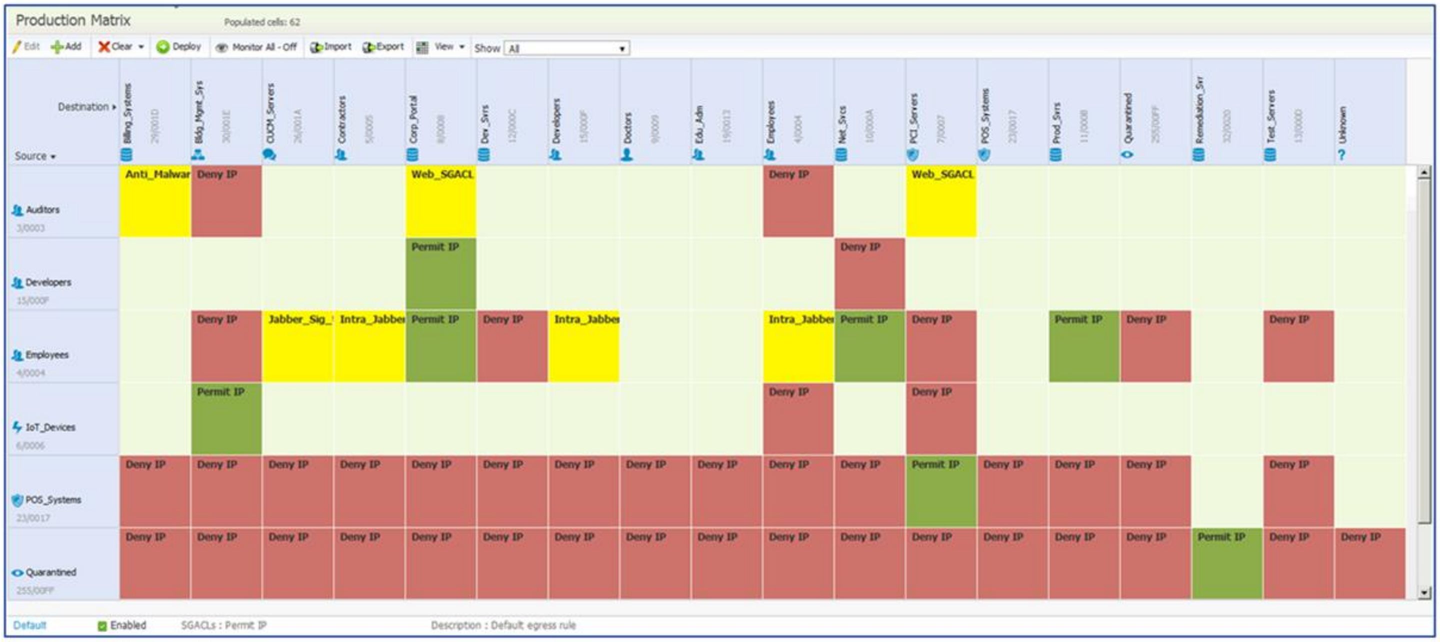
Cisco TrustSec: Overview

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

Cisco TrustSec is a scalable and agile software-defined segmentation (or micro-segmentation) technology implemented in hardware and software on Cisco platforms and protects assets such as data, applications, and mobile devices from unauthorized access.   Unlike conventional access control mechanisms which are based on network topology, TrustSec controls are defined using logical policy groupings, so resource segmentation and highly secure access are consistently enforced even as resources move within mobile and virtualized networks. TrustSec includes hardware based inline tagging technology allowing user traffic to be identified or “tagged” without a performance impact as its traverses the network.

TrustSec uses the Identity Services Engine (ISE) as the controller for identity and policy for all access and egress control. Policy is easily visible and manageable from the TrustSec Policy Matrix in ISE.

TrustSec Matrix in ISE: Egress Policy Example



Production Matrix   Populated cells: 62

Destination ▸ Source ▾	Billing_Systems 29/001D	Bldg_Mgmt_Sys 30/001E	CUCM_Servers 26/001A	Contractors 5/0005	Corp_Portal 8/0008	Dev_Svrs 12/000C	Developers 15/000F	Doctors 9/0009	Edu_Adm 19/0013	Employees 4/0004	Net_Svcs 10/000A	PCI_Servers 7/0007	POS_Systems 23/0017	Prod_Svrs 11/000B	Quarantined 255/00FF	Remediation_Svr 32/0020	Test_Servers 13/000D	Unknown
Auditors 3/0003	Anti_Malwar	Deny IP			Web_SGACL					Deny IP		Web_SGACL						
Developers 15/000F					Permit IP						Deny IP							
Employees 4/0004		Deny IP	Jabber_Sig_	Intra_Jabber	Permit IP	Deny IP	Intra_Jabber			Intra_Jabber	Permit IP	Deny IP		Permit IP	Deny IP		Deny IP	
IoT_Devices 6/0006		Permit IP								Deny IP		Deny IP						
POS_Systems 23/0017	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	Deny IP	Deny IP		Deny IP	
Quarantined 255/00FF	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	Deny IP

Default   ☑ Enabled   SGACLs : Permit IP   Description : Default egress rule

TrustSec is currently embedded in over 40 different Cisco product families and other vendor’s products and is now being used by customers to:

- Enforce rapid threat containment and isolate attacks
- Restrict the lateral movement of threats using segmentation (micro-segmentation)
- Segment campus, branch and data center networks
- Enable scalable BYOD and mobility access controls
- Reduce the scope of compliance for regulations such as PCI compliance
- Control access to regulated applications in finance and healthcare organizations
- Segment IoT devices
- Simplify extranet access controls for business partners and supplier connections
- Extend enterprise security policies to hybrid cloud and multi-cloud environments consistently
- Simplify policy management to reduce demands on IT staff

Make firewalls and traffic monitoring tools aware of endpoint roles

Cisco TrustSec key benefits include:

- **Reduced Complexity** - it removes complexity associated with topology based access control lists using plain-language policies.
- **Simplified Security Operations** – bring servers onboard faster and speed up moves, adds, and changes. Branch and campus level micro-segmentation can be managed centrally using ISE
- **Automation** – automate firewall rules and ACL administration.
- **Secure Mobility** – enables and enforces mobile policies from the branch, campus and data center networks.
- **Compliance** – maintains policy compliance automatically where ever users access data from the network.

TrustSec is an open technology as Cisco has submitted both SXP and inline tagging frame formats to the IETF to enable third party implementations. Open source SXP software is now available for other vendors and customers to use to directly integrate TrustSec group-based policies into their own products. In addition, the OpenDaylight open-source SDN Controller supports SXP in its Lithium release

Appendix A: Total Economic Impact™ Overview

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. TEI assists technology vendors in winning, serving, and retaining customers.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

BENEFITS

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place 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. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

COSTS

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

FLEXIBILITY

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprise wide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections and 2) the likelihood that the estimates will be measured and tracked over time. TEI risk factors are based on a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the risk factor around each cost and benefit.

Appendix B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

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.

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.

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.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A NOTE ON CASH FLOW TABLES

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at “time 0” or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until 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.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.

FRAMEWORK ASSUMPTIONS

The discount rate used in the PV and NPV calculations is 10%, and the time horizon used for the financial modeling is three years. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their respective company's finance department to determine the most appropriate discount rate to use within their own organizations.

Appendix C: Endnotes

[1] Forrester risk-adjusts the summary financial metrics to take into account the potential uncertainty of the cost and benefit estimates. For more information, see the section on Risks.