The Total Economic Impact™ Of Cisco TrustSec
Simplifying Security Engineering With Effective Network Segmentation
### Table Of Contents

- Executive Summary ................................................................. 1
- Disclosures .............................................................................. 2
- TEI Framework And Methodology ............................................ 3
- Analysis .................................................................................. 4
- Financial Summary ................................................................. 13
- Cisco TrustSec: Overview ....................................................... 14
- Appendix A: Total Economic Impact™ Overview ..................... 16
- Appendix B: Glossary ............................................................... 17

---

**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.

---

© 2015, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com.
Executive Summary

In January 2015, Cisco commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment enterprises may realize by deploying Cisco TrustSec. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cisco TrustSec on their organizations.

The Cisco TrustSec solution simplifies the provisioning and management of highly secure access to network services and applications. Unlike access control mechanisms that work on network topology, Cisco TrustSec policies use logical grouping. Highly secure access is consistently maintained even as resources are moved in mobile and virtualized networks. For a more detailed overview of Cisco TrustSec and its components, please refer to page 14.

To better understand the benefits, costs, and risks associated with Cisco TrustSec, Forrester interviewed two companies. Company A is an organization that provides senior housing for over 22,000 residents in the US. This organization used Cisco TrustSec to provide highly secure segmented mobile network services to its residents. Company B is an international packaging and paper group company experiencing rapid growth. It used Cisco TrustSec as an innovative solution to quickly integrate the infrastructure of new acquisitions into its own and standardize security architecture across its wide area network (WAN) globally. While the case study will talk about the experiences of these two companies, the financial analysis focuses on the impact that Cisco TrustSec had on one organization.

CISCO TRUSTSEC INCREASES IT SECURITY AND LOWERS OPERATING COSTS

Our interviews with these two customers and subsequent financial analysis found that Cisco TrustSec had the financial impact shown in Figure 1.

The analysis points to risk-adjusted benefits of $2.48 million over three years versus costs of $492,000, adding up to a net present value of approximately $1.99 million. Cisco TrustSec contributed to a 5% reduction in operating costs for one of the organizations interviewed.

Cisco TrustSec enabled the organizations interviewed to reduce operational costs by avoiding additional IT headcount, deploy new environments faster, and implement consistent and effective network segmentation resulting in lower downtime.

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ROI:</strong></td>
<td><strong>405%</strong></td>
<td><strong>NPV:</strong></td>
<td><strong>$1.99 million</strong></td>
</tr>
<tr>
<td><strong>Payback:</strong></td>
<td><strong>4.7 months</strong></td>
<td><strong>Operating costs:</strong></td>
<td><strong>↓ 5%</strong></td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

*This represents the NPV of Company A, a relatively smaller organization (compared to Company B) with a 110-person IT department.*
Benefits. The Cisco TrustSec customers interviewed experienced the following key benefits:

- **Reduced operational costs with the cost avoidance of additional headcount.** Company A reported that by using Cisco TrustSec, it only needed to manage seven virtual local area networks (VLANs) instead of 32,000 VLANs in a more traditional infrastructure environment. It did not have to increase its network team by 350%, thus saving an additional 10.5 IT engineer headcount. These resource cost avoidance savings represent $1.05 million saved in the first year of implementation. At an overall annual IT operating budget of $20 million, Cisco TrustSec contributed to a 5% reduction in operating costs for Company A.

- **Faster time-to-market of projects.** Company B reported that it was also able to quickly integrate its acquisitions into its infrastructure as a result of TrustSec. With TrustSec, they were able to reduce their acquisition network integration time by 83%. Company B estimated it saved an average of five man-days per acquisition as a result.

- **Risk reduction resulting in downtime cost savings.** Company B reported that it was able to mitigate risk, as Cisco TrustSec allowed it to better manage the increasing complexity of its IT infrastructure. This risk reduction would conservatively result in $400,000 saved per downtime incident.

- **Other benefits experienced by the organizations interviewed include:**
  - Consistent and effective network segmentation.
  - Simplified security engineering with simplification of security policy.
  - Increased flexibility and scalability.
  - Improved user satisfaction.

Costs. The organizations we interviewed experienced the following costs that are directly related to their Cisco TrustSec deployment:

- **Cisco TrustSec infrastructure and implementation costs.** The organizations interviewed allocated the premium paid on top of standard networking technology for their network life-cycle replacement project to TrustSec. This cost category includes hardware such as the Cisco Identity Services Engine (ISE) and premium switches. Implementation costs include professional services as well as internal labor.

- **Ongoing administration.** Company A incurred ongoing costs to maintain its wireless network enabled by TrustSec and allocated a percentage of this annual maintenance and administration cost to Cisco TrustSec in its 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 financial results 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 Cisco 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 deploying Cisco TrustSec. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision.

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

› Interviewed Cisco marketing and sales personnel, along with Forrester analysts, to gather data relative to Cisco TrustSec and the network security market in general.
› Interviewed two organizations currently using Cisco TrustSec to obtain data with respect to costs, benefits, and risks.
› 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 one 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 Cisco TrustSec: benefits, costs, flexibility, and risks.

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

FIGURE 2
TEI Approach

Perform due diligence ➔ Conduct customer interviews ➔ Construct financial model using TEI framework ➔ Write case study

Source: Forrester Research, Inc.
Analysis

INTERVIEWED ORGANIZATIONS

For this study, we interviewed representatives from the following companies:

› Company A is a leading provider in senior housing. It has over 22,000 residents in 18 communities in the US, 14,000 staff members, and annual revenue of $1 billion.

› Company B is an international packaging and paper group company. It employs over 24,000 people in more than 30 countries and has approximately $6.5 billion in annual revenue.

INTERVIEW HIGHLIGHTS

Situation

Company A wanted to roll out highly secure segmented mobile network services to its residents. It initially investigated setting up SSIDs for individual residents, but hardware and device limitations resulted in issues for these residents. The company needed a solution to provide secure wireless service across its residents and staff that was easy to manage and control. Company B, meanwhile, was undertaking a life-cycle replacement project for its Cisco wired and wireless networks. It was looking for a network security solution that would address future business challenges such as hyperconvergence, the Internet of Things, and increasing workforce mobility. Its business was also driven by aggressive growth through acquisition, as a lot of consolidation was happening within the industry.

Solution

Company A worked with Cisco lab engineers to use TrustSec as a VLAN automation tool. It established a Cisco 802.11ac wireless network and used Cisco TrustSec and the Identity Services Engine to create, secure, and manage individual networks for residents. It also used this network for staff laptops for core medical applications and wall-mounted displays. Company B implemented Cisco TrustSec with its network life-cycle replacement project for its headquarters and satellite operations, establishing a bring-your-own-device (BYOD) environment serving over 12,000 users.

Results

The interviews revealed that the organizations experienced the following benefits:

› Reduced operational cost with fewer resource requirements. Company A noted that without Cisco TrustSec, it would have had to hire additional network resources to manage the number of VLANs needed in a more traditional deployment.

"With TrustSec, we aren’t managing 32,000 VLANs; we’re managing seven. When we calculated the benefits enterprise wide, we would have had to increase our network team by 350%.”

~ VP, IT operations and customer support, senior housing company

› Faster time-to-market for project deployment. Cisco TrustSec simplified the security engineering process for the interviewed organizations. As a result, the companies interviewed saw that they were able to roll out IT projects at a faster pace when compared with their previous environment.

› Lower risk resulting in downtime reduction. With Cisco TrustSec, organizations could mitigate their risks in an increasingly complex environment.

› Consistent and effective network segmentation. Organizations interviewed noted that Cisco TrustSec enabled more consistent and effective network segmentation. As one organization observed, “We wanted to try something that was very innovative.” It noted that with Cisco TrustSec, its security architecture would remain intact even with changes to its network
infrastructure. These organizations also noted Cisco TrustSec gave them an effective method of segmentation to provide security to groups of devices and people that would ensure their assets were protected. They greatly valued this consistent approach to managing their environment.

“TrustSec is a new way for network segmentation. We can virtualize network segmentation and security from the infrastructure. You need to look at security holistically.”

~ Head of infrastructure, international packaging and paper company

Simplified security engineering with simplification of security policy. Company B noted that Cisco TrustSec enabled it to quickly translate business security policy requirements into a network security policy. With Cisco TrustSec, organizations could enact security group tagging with policy rules instead of relying on long lists of IP addresses. This gave the companies interviewed a more flexible, automated model that was easier to manage.

Company A noted that without the simplified security engineering enabled by Cisco TrustSec, it would have abandoned the project. As one VP of IT observed: “We wouldn’t have been able to support it in a traditional way with SSIDs. There are 1,500 individual residents in one community. The Apple device limits separate SSIDs to 60, and that limit causes a lot of issues for the residents.” The Cisco TrustSec solution enabled Company A to use fewer than five SSIDs instead of thousands and eliminated co-channel interference from a multiplicity of wireless routers from different service providers in its pre-TrustSec environment.

Increased flexibility and scalability. One organization identified Cisco TrustSec’s “compatibility with change” as a major benefit of the solution. Hyperconvergence and the Internet of Things was a theme in discussions with both organizations interviewed. Company B’s estimates predicted very aggressive growth in these types of devices, so it needed to change behaviors and processes to cope with this future growth. Otherwise, it would have to increase its spending if it stuck to its traditional way of doing things. This organization also has a very fast-moving business environment and noted that by detaching security from the infrastructure with Cisco TrustSec, it now had a better ability to scale. “That scalability is very important with our manufacturing environment, and I can’t imagine how much more important in a financial environment,” one IT executive added.

Improved user satisfaction. Company A noted that with the mobile network services project enabled by Cisco TrustSec, it was able to provide a “higher level of security with a lower level of technical know-how from an end user perspective.” It was able to provide a simplified wireless network environment for its residents and make it simple to provision new users. Residents could now easily connect their own devices to the wireless environment, as Cisco TrustSec assigned these residents to security groups using simple plain language names. This company saw user satisfaction improve with instant service provisioning.

“We had a very specific use case that TrustSec allowed us to take care of and knock out of the park. We are just using a fraction of [TrustSec] capabilities, and the extensibility of the platform is appealing to us.”

~VP of IT, national senior housing provider

“The most valuable feature of our TrustSec project has been the ease of use from an end user perspective. We have a lot of residents with Kindles, iPads, and Nooks, and they set them up themselves. They click on the resident SSID and click passwords; it’s done and they never have to touch it again. It’s incredibly simple.”

~ VP of IT, national senior housing provider
BENEFITS

The financial analysis quantifies the benefits to Company A, which used Cisco TrustSec to simplify segmentation and policy-based access control as the organization rolled out mobile network services for its senior housing residents and staff.

While benefits that Company B experienced are also discussed in this section, these quantified benefits are not included in the final financial analysis.

Reduced Operational Costs — Additional IT Headcount

Both organizations interviewed noted that their Cisco TrustSec implementations resulted in operational cost savings. Company B observed, “If we had gone the more traditional route, we would have had to spend more resources on manpower to cope with additional requirements or hire professional services.” Company A’s goal was to provide secure and segmented mobile network services to its residents and staff. If it had used a more traditional approach, it would have needed to manage approximately 32,000 VLANs. Instead, it is only managing seven VLANs enterprise-wide. The organization estimated that without Cisco TrustSec, it would have had to increase its network team by 350%. They also noted that since their five-person network team had two voice engineers, this 350% increase applies to the three engineer resources on their team. Cisco TrustSec has saved the organization an additional 10.5 headcount. At an annual loaded compensation of $100,000 per full-time equivalent (FTE), the organization was able to reduce operational costs by $1.05 million per year in engineering resource savings.

To account for risk and uncertainty in these estimates, this number is risk-adjusted down by 5%, resulting in $997,500 in annual savings over the three-year analysis.

<table>
<thead>
<tr>
<th>TABLE 1</th>
<th>Cost Avoidance Of Additional Headcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref.</td>
<td>Metric</td>
</tr>
<tr>
<td>A1</td>
<td>Number of network FTEs (saved)</td>
</tr>
<tr>
<td>A2</td>
<td>Annual rate per FTE</td>
</tr>
<tr>
<td>At</td>
<td>Cost avoidance of additional IT headcount</td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
</tr>
<tr>
<td>Atr</td>
<td>Cost avoidance of additional IT headcount (risk-adjusted)</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

With an overall IT budget of $20 million per year, Cisco TrustSec contributed to a 4.99% reduction in the organization’s operating costs through resource cost avoidance savings from its mobile network services project.

Faster Time-To-Market Of Projects

Company A noted that it was now “so simple to provision new users” with Cisco TrustSec. This simplicity meant it could now provide wireless services to its users at a faster pace. Company B has a fast-paced changing business environment. It is buying companies for consolidation every year, and it needs to quickly integrate these acquisitions into its environment. As
one executive noted, “It usually takes a couple of man-days of work to understand a local environment, put in a firewall, test, and other tasks. And with TrustSec we can avoid that right now. We have certain security groups that are standardized across the network. We can simply attach a new community to the network and start from that.” They added that TrustSec was a very efficient way to have a model for network security that was independent from local infrastructure.

Company B estimated that it saved an average of five man-days per acquisition as a result of Cisco TrustSec, and it typically acquires five companies per year. These tasks are usually outsourced to external suppliers at an average cost of $1,140 per man-day. Table 2 below provides a sample calculation of how organizations can value the benefit of faster time-to-market as a result of their Cisco TrustSec implementation. This calculation captures this benefit value in terms of the time saved on the project and the cost of this time. Company B’s Cisco TrustSec deployment has resulted in a faster time-to-market benefit of $28,500 in non-risk-adjusted savings per year.

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Metric</th>
<th>Calculation</th>
<th>Year 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>Time saved per acquisition (days)</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>B2</td>
<td>Cost per day</td>
<td></td>
<td>$1,140</td>
</tr>
<tr>
<td>B3</td>
<td>Number of acquisitions</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Bt</td>
<td>Faster time-to-market — new environment rollout</td>
<td>B1<em>B2</em>B3</td>
<td>$28,500</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

**Downtime Reduction Savings Due To Risk Mitigation**

For Company B, one of the main benefits of its deployment of Cisco TrustSec was the ability to mitigate risks in an increasingly complex environment. As the organization’s head of infrastructure noted, “The more IT complexity we deploy, the risks get higher.” With the simplicity TrustSec brings to managing network security, the company was able to avoid errors and the related cost of these errors. As it’s a manufacturing company operating with central information systems, IT incidents could trigger downtime in machine operations. By lowering the risk of downtime incidents, Cisco TrustSec saved the company the cost of downtime.

Table 3 illustrates how the cost of downtime can be calculated for Company B. The average length of downtime for one paper machine due to a network security issue/error is estimated at 4 hours, based on historical incidents. The cost of downtime for one machine is $100,000 per hour, as this affects downstream processes such as printing and warehousing for finished goods. Downtime reduction savings due to lowered risk with TrustSec is quantified as $400,000 per incident.


**TABLE 3**  
Downtime Reduction Savings

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Metric</th>
<th>Calculation</th>
<th>Year 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Number of incidents</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>C2</td>
<td>Length of downtime (hours)</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>C3</td>
<td>Cost of downtime per hour</td>
<td>C1<em>C2</em>C3</td>
<td>$100,000</td>
</tr>
<tr>
<td>Ct</td>
<td>Downtime reduction savings</td>
<td></td>
<td>$400,000</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

Company B stated that incidents of this scale had happened once every three years, but as its IT environment becomes more complicated, risk also increases, and the rate of these downtime incidents for its 60 machines would also climb if it did not manage these risks.

**Total Benefits**

Table 4 shows the quantified benefit for Company A listed above, as well as present values (PVs) discounted at 10%. Over the three-year analysis, the benefits have a total risk-adjusted present value of approximately $2.48 million.

**TABLE 4**  
Total Benefits (Risk-Adjusted)

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Initial</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Total</th>
<th>Present Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced operational costs</td>
<td>$0</td>
<td>$997,500</td>
<td>$997,500</td>
<td>$997,500</td>
<td>$2,992,500</td>
<td>$2,480,635</td>
</tr>
<tr>
<td>Total benefits</td>
<td>$0</td>
<td>$997,500</td>
<td>$997,500</td>
<td>$997,500</td>
<td>$2,992,500</td>
<td>$2,480,635</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.
COSTS

This section describes and lists the incremental costs that are directly related to the deployment and maintenance of Cisco TrustSec for Company A.

Cisco TrustSec Deployment

Company A budgeted $8.8 million for setup and installation of mobile network services across all its communities. This budget includes electric installation, cabling to access points, and staff augmentation, among others. The organization estimated that $300,000 out of this budget is allocated to TrustSec-related costs. This portion includes ISE hardware, the premium paid on standard switches and networking technology, professional services, and internal labor for deployment. As implementation can be variable, this benefit is risk-adjusted up 25%, resulting in a $345,000 net present value in costs.

Both organizations emphasized the importance of working closely with Cisco engineers on the deployment of their Cisco TrustSec solutions. One VP of IT noted: “A big success factor was getting involved with the right folks at Cisco who understood the business case. We tried it in the labs a couple of time and eventually hit on using TrustSec as a VLAN automation tool.”

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Calculation</th>
<th>Initial</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>Cisco TrustSec implementation — ISE, premium on standard networking technology, professional services, internal labor, etc.</td>
<td>$300,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dt</td>
<td>Cisco TrustSec deployment</td>
<td>D1</td>
<td>$300,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td></td>
<td>↑ 25%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dtr</td>
<td>Cisco TrustSec deployment (risk-adjusted)</td>
<td></td>
<td></td>
<td></td>
<td>$375,000</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

Annual Operating Costs

Company A pegged operating costs for its mobile network services project at $815,000 per year. This includes phone service connectivity, administration, maintenance contracts, and equipment replacement, among others. We conservatively estimate that 5% of those annual operating costs are allocated to ongoing administration and operating costs of the Cisco TrustSec solution. Total annual operating costs attributed to TrustSec are quantified at $40,750 per year. This value is risk-adjusted up by 15%, resulting in $46,863 in annual costs or a net present value of $116,540 over a three-year analysis.
TABLE 6
Annual Operating Costs

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Metric</th>
<th>Calculation</th>
<th>Initial</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Project operating costs</td>
<td></td>
<td>$815,000</td>
<td>$815,000</td>
<td>$815,000</td>
<td></td>
</tr>
<tr>
<td>E2</td>
<td>Percentage allocated to Cisco TrustSec</td>
<td></td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Et</td>
<td>Annual operating costs</td>
<td>E1 * E2</td>
<td>$40,750</td>
<td>$40,750</td>
<td>$40,750</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>↑ 15%</td>
</tr>
<tr>
<td>Etr</td>
<td>Annual operating costs (risk-adjusted)</td>
<td></td>
<td>$46,863</td>
<td>$46,863</td>
<td>$46,863</td>
<td></td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

Total Costs
Table 7 shows the total of the costs that are directly related to the Cisco TrustSec deployment, as well as associated present values, discounted at 10%. Over three years, the Company A incurred estimated costs that have a net present value of $491,540.

TABLE 7
Total Costs (Risk-Adjusted)

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Initial</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Total</th>
<th>Present Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco TrustSec deployment</td>
<td>$375,000</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$375,000</td>
<td>$375,000</td>
</tr>
<tr>
<td>Annual operating costs</td>
<td>$0</td>
<td>$46,863</td>
<td>$46,863</td>
<td>$46,863</td>
<td>$140,588</td>
<td>$116,540</td>
</tr>
<tr>
<td>Total costs</td>
<td>$375,000</td>
<td>$46,863</td>
<td>$46,863</td>
<td>$46,863</td>
<td>$515,588</td>
<td>$491,540</td>
</tr>
</tbody>
</table>

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 use Cisco 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).

Areas of flexibility identified by the organizations interviewed include hyperconvergence, with Cisco TrustSec enabling simpler security management should these organizations choose to integrate compute, storage, virtualization resources, networking, and other technologies into a single managed system. These organizations could also see additional operational cost savings as they add more devices onto the network. In this dynamic environment, as Cisco TrustSec adds features and functionality, organizations would also see additional benefits and improved productivity. As an example, one organization noted that in the latest release of TrustSec, Cisco has implemented an interface that enables networking inspection layers to find abnormal network activities. The organization can receive information from these inspection tools and create network rules using security groups. One executive noted, “We could dynamically create policies for certain areas that would give us more flexibility and functionality in the future.” Another area of flexibility identified was around traffic intelligence. Using TrustSec, organizations could eventually route traffic on different networks with differentiating security technology on a network packet. These features, along with other additional functionality in the pipeline, could bring additional operational cost savings and risk mitigation benefits to organizations as a result of their TrustSec implementation.

The value of flexibility is unique for 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 Cisco 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 Cisco TrustSec, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

<table>
<thead>
<tr>
<th>TABLE 8</th>
<th>Benefit And Cost Risk Adjustments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benefits</strong></td>
<td><strong>Adjustment</strong></td>
</tr>
<tr>
<td>Resource cost savings</td>
<td>↓ 5%</td>
</tr>
<tr>
<td><strong>Costs</strong></td>
<td><strong>Adjustment</strong></td>
</tr>
<tr>
<td>TrustSec deployment costs</td>
<td>↑ 25%</td>
</tr>
<tr>
<td>Annual operating costs</td>
<td>↓ 15%</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

Quantitatively capturing investment 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 risk that affects benefits is identified as part of the analysis:

› Headcount and productivity savings are based on averages and estimations by the interviewed organizations. To be conservative, the estimated productivity gains and headcount savings have been risk-adjusted down.

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

› The deployment and ongoing administration costs are based on the average estimated efforts, but it might take more time and effort than initially foreseen. These costs have therefore been risk-adjusted up.

Table 8 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates. 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 organization's investment in Cisco 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)

TABLE 9
Cash Flow (Risk-Adjusted)

<table>
<thead>
<tr>
<th>Initial</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Total</th>
<th>Present value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs</td>
<td>($375,000)</td>
<td>($46,863)</td>
<td>($46,863)</td>
<td>($46,863)</td>
<td>($515,588)</td>
</tr>
<tr>
<td>Benefits</td>
<td>$0</td>
<td>$997,500</td>
<td>$997,500</td>
<td>$997,500</td>
<td>$2,992,500</td>
</tr>
<tr>
<td>Net benefits</td>
<td>($375,000)</td>
<td>$950,638</td>
<td>$950,638</td>
<td>$950,638</td>
<td>$2,476,913</td>
</tr>
</tbody>
</table>

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 technology protects assets such as data, applications, and mobile devices from unauthorized access. It simplifies the provisioning and management of network access, accelerates security operations, and consistently enforces policy anywhere in the network.

Introducing Cisco TrustSec®

Software-Defined Segmentation based on business policy

Cisco TrustSec Policy-Defined Segmentation

Unlike access control mechanisms based on network topology, Cisco TrustSec controls are defined using logical policy groupings, so resource segmentation and highly secure access are consistently maintained even as resources move in mobile and virtualized networks.

Taking Complexity out of Network Security

Instead of complicated VLAN, access control lists (ACLs), and firewall-rule engineering and administration, a Cisco TrustSec system uses plain-language policies. These policies are managed in a simple matrix that segments the network and controls access to critical assets by assigning business roles.

Cisco TrustSec policies are enforced in wired and wireless networks and VPN devices from the network edge right to applications in the data center. This capability makes it easy to understand and enforce security policies as well as manage operations and comply with regulatory requirements.
The Cisco TrustSec solution simplifies the provisioning and management of highly secure access to network services and applications. Unlike access control mechanisms that are based on network topology, Cisco TrustSec policies use logical groupings. Highly secure access is consistently maintained even as resources are moved in mobile and virtualized networks. Decoupling access entitlements from IP addresses and VLANs simplifies security policy maintenance tasks, lowers operational costs, and allows common access policies to be consistently applied to wired, wireless, and VPN access. Cisco TrustSec classification and policy enforcement functions are embedded in Cisco switching, routing, wireless LAN, and firewall products. By classifying traffic according to the contextual identity of the endpoint instead of its IP address, the Cisco TrustSec solution enables more flexible access controls for dynamic networking environments and data centers.

The ultimate goal of Cisco TrustSec technology is to assign a tag (known as a Security Group Tag, or SGT) to the user’s or device’s traffic at ingress (inbound into the network), and then enforce the access policy based on the tag elsewhere in the infrastructure (in the data center, for example). This SGT is used by switches, routers, and firewalls to make forwarding decisions.

Data Center Segmentation
Secure enclaves and server separation

Main site – [Cisco TrustSec](#)

- At-a-Glance
- Solution Overviews
- Case Studies
- White Papers:
  - [Cisco TrustSec for PCI Scope Reduction – Verizon Assessment and Validation](#)
  - [Securing BYOD with Cisco TrustSec Security Group Firewalling](#)
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.

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 enterprisewide 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 applies a probability density function known as “triangular distribution” to the values entered. At a minimum, three values are calculated to estimate the underlying range 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 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>
<thead>
<tr>
<th>Ref.</th>
<th>Metric</th>
<th>Calculation</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
</table>

Source: Forrester Research, Inc.