A Forrester Total Economic Impact™
Study Commissioned By Cisco
January 2018

# The Total Economic Impact™ Of Cisco's Solution for Network Visibility and Segmentation

## Cost Savings And Business Benefits Enabled By Stealthwatch And ISE

FORRESTER®

# Table Of Contents




**Project Director:**
Sean Owens

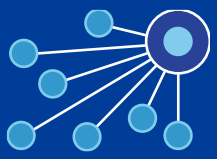

ABOUT FORRESTER CONSULTING

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®

## Benefits And Costs



Avoided network security remediation costs:
**$285,000**

Business impact savings of avoided security events:
**$1.6 million**

IT resource cost savings:
**$892,000**

Avoided hardware costs:
**$236,000**

Employee productivity:
**$1.4 million**

# Executive Summary

Cisco provides a Zero Trust security solution that helps its customers solve the problems of network visibility and access. 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 Stealthwatch and ISE. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Stealthwatch and Identity Services Engine (ISE) on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with years of experience using Stealthwatch and ISE. Cisco Stealthwatch delivers clear and actionable network visibility, and Cisco ISE provides alerts and automated policy management and enforcement. Together they deliver a solution that can pinpoint the source of an issue, automatically lock down the affected devices or accounts, and then ensure network compliance before bringing them back online.

Prior to using Stealthwatch and ISE, the customers used a variety of security and network management tools and solutions. However, network visibility was a clear pain point, meaning many issues were not stopped before requiring significant resource time — or even went undetected — before Stealthwatch and ISE.

## Key Findings

**Quantified benefits.** The following three-year, present-value, risk-adjusted benefits are representative of those experienced by the companies interviewed:

- **Network security remediation time reduced 200 hours for each major event and 3 hours for each minor issue.** Cisco ISE and Stealthwatch helps organizations identify and mitigate network security issues before they become events that can incur significant remediation time and cost. When you include the potential business cost of an attack — whether unusual network activity, an employee error, or industrial espionage — Stealthwatch and ISE can help protect networks and data, adding up to nearly $1.9 million in time savings for a composite organization.
- **IT employee productivity that allows the composite organization to avoid hiring six new employees over the three-year period.** IT network managers are more productive with Stealthwatch and ISE, and they can not only focus on more value-added tasks, but also keep pace with organizational growth and future needs without needing more resources. Avoiding the hiring of two network engineers each year over three years adds up to about $892,000 in time savings for the composite organization.
- **Branch office bandwidth issues are identified and resolved without requiring new hardware or services, saving $236,000.** Interviewed organizations highlighted several instances where limited bandwidth was impacted by individual users or devices (such as a user syncing a whole network share or email message history). For the composite organization, this means identifying and fixing the issue instead of spending unnecessary money on more bandwidth or network circuits.

**ROI**
**120%**

**Benefits PV**
**$4.4 million**

**NPV**
**$2.4 million**

› **Employee productivity improvements of $1.4 million.** Reduced security issues impact all employees when they can't get access to the information they need quickly — which can impact their ability to get work done, make sales, and complete tasks.

**Unquantified benefits.** The interviewed organizations experienced the following benefits, which are not quantified for this study:

› **Avoided additional business impact of major security issues.** A major issue can cause ripple effects in a business. An external data breach can mean a major public relations impact, as well as customer remediation costs. Even an internal breach can impact an organization's ability to make informed decisions in a timely manner.

› **Added benefits from Cisco TrustSec and NetFlow.**[1] Some interviewed organizations also leverage these Cisco technologies, leading to improved network visibility and management.

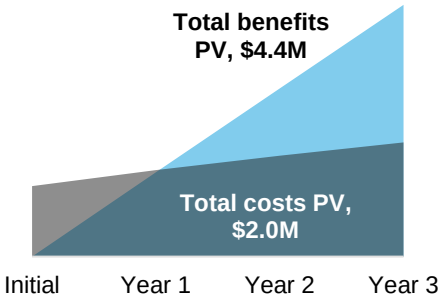
**Costs.** The interviewed organizations experienced the following risk-adjusted costs:

› **Ongoing maintenance, support, and resource costs of $757,000.** Annual costs include a team of IT professionals who are responsible for the management of Stealthwatch, ISE, and other support tasks, as well as the annual maintenance and support license fees to Cisco.

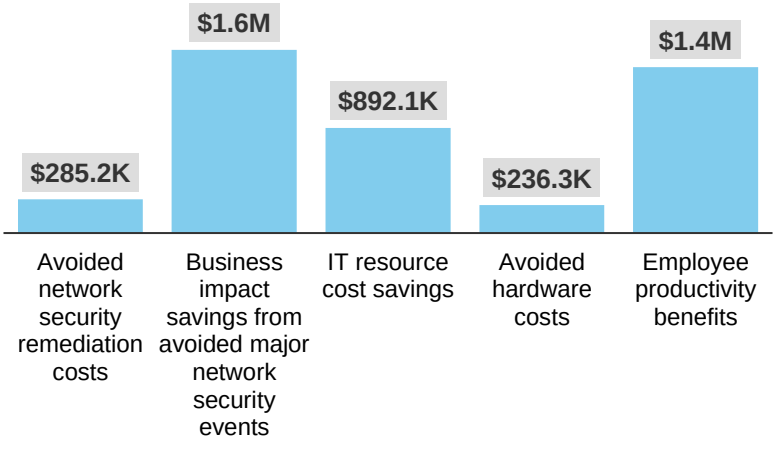
› **Implementation labor costs of $480,000 and software, hardware, and services costs of $746,000.** Upfront costs include software licensing costs, employee time to plan and implement deployment, and some hardware costs needed for new routers and switches that needed immediate replacement ahead of the normal refresh schedule. These added up to $1.2 million in costs.

Forrester's interviews with three existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of almost $4.4 million over three years versus costs of nearly $2.0 million, adding up to a net present value (NPV) of $2.4 million, a payback of 12 months, and an ROI of 120%.

**Financial Summary**




**Benefits (Three-Year)**






FORRESTER®

## TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Cisco Stealthwatch and ISE.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Cisco Stealthwatch and ISE can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

**DUE DILIGENCE**
Interviewed Cisco stakeholders and Forrester analysts to gather data relative to Stealthwatch and ISE.

**CUSTOMER INTERVIEWS**
Interviewed three organizations using Stealthwatch and ISE to obtain data with respect to costs, benefits, and risks.

**COMPOSITE ORGANIZATION**
Designed a composite organization based on characteristics of the interviewed organizations.

**FINANCIAL MODEL FRAMEWORK**
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

**CASE STUDY**
Employed four fundamental elements of TEI in modeling Cisco Stealthwatch and ISE's impact: 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 A for additional information on the TEI methodology.

# The Cisco Customer Journey

**BEFORE AND AFTER THE STEALTHWATCH AND ISE INVESTMENT**

## Interviewed Organizations

For this study, Forrester conducted three interviews with Cisco Stealthwatch and Identity Services Engine (ISE) customers. Interviewed customers include the following:

| INDUSTRY | REGION | INTERVIEWEE | ORGANIZATIONAL DETAILS |
|---|---|---|---|
| Banking | Europe | • Manager, network security team | • 70,000 employees at corporate offices spread out across 2,000 branches, primarily in Europe.<br>• It also deployed Cisco TrustSec-enabled devices to their network around the same time.[2] |
| Healthcare insurance | United States | • Director, information security | • 50,000 employees across 5 main campuses and more than 100 clinics and hospitals. |
| Banking | Europe, Asia, and Africa | • CIO/network architect | • 40,000 employees spread out across 1,500 branches, across several countries in Europe, Africa, and Asia.<br>• It had deployed many Cisco TrustSec network devices already. |

## Key Challenges

Interviewed organizations struggled to keep up with security needs with issues such as:

- **Little or no network visibility.** Network and security managers were not able to respond quickly to issues or plan current and future network needs when they had little or no view into how network resources were used or where to find and fix bandwidth chokepoints. The CIO of a worldwide bank reported that, "We needed more visibility and we needed to understand what's actually happening in the network."
- **Rapid identification and remediation of minor and major network security issues.** Potential threats such as spam, malware, distributed denial-of-service (DDoS) attacks, viruses, malicious behavior, or even internal mistakes were all hard to identify, diagnose, and resolve before they spread to affect more machines and data sources. The network security team manager at a European bank reported that, "We had incidents in the past where people in branches were being coerced by people to connect devices into servers and workstations in branches."
- **IT and employee inefficiencies.** Bandwidth issues, viruses, or major network attacks all can slow down the network and make it inaccessible. Each slowdown, delay, or missed connection can lead to significant lost time and rework. The director of information security for a US healthcare insurance firm reported that, "We were only looking at router and switch logs, but they have showed the point-to-point, IP to IP traffic, so it was hard to identify what traffic was causing latency or an outage."

> "We needed more visibility and we needed to understand what's actually happening in the network."
>
> *CIO/network architect, worldwide bank*

> "We were only looking at router and switch logs, but they have showed the point-to-point, IP to IP traffic, so it was hard to identify what traffic was causing latency or an outage."
>
> *Director of information security, healthcare insurance firm*

## Solution Requirements

The interviewed organizations searched for a solution that could:

- Deliver clear and convenient information about network usage; including location, data transferred, and even user account information (if applicable).
- Set network access policies.
- Automate network tasks to provide convenient access when appropriate, and lock down a device when necessary.
- Deliver better network and information security without sacrificing employee productivity.
- Meet future growth and planned technologies, particularly software defined networking and cloud capabilities.

All interviewed organizations were already Cisco customers, but chose Stealthwatch and ISE not only because it was the best option for their infrastructure investment, but found it to be the most comprehensive network visibility and security solution. Deployment included:

- One organization has taken a phased approach, rolling out Stealthwatch and ISE over the past three years by office and department.
- Another started with ISE a few years ago, also rolling out the solution across their network in phases, and over the past year they have added Stealthwatch.
- And the third organization rolled out Stealthwatch in three months.

> "We had incidents in the past where people in branches were being coerced by people to connect devices into servers and workstations in branches."
>
> *Network security team manager, European bank*

## Key Results

The interviews revealed that key results from the Stealthwatch and ISE investment include:

- Visibility into network configuration to identify bandwidth chokepoints, resolve them, and avoid overspending on bandwidth access. With Stealthwatch and ISE, organizations can track network flow and identify specific IP addresses and user accounts taking up bandwidth to resolve issues without having to purchase more networking hardware or services.
- **Reduction in major and minor security issues to reduce costs and avoid serious business risks**. With Stealthwatch and ISE, organizations can track network flow, identify issues, and mitigate security issues before they become major events needing remediation.
- **Improve IT productivity.** IT network engineers can spend less time on network management and security tasks and more time focused on network health and other more valuable tasks. Organizations can keep up with network administration needs (and even add more) without having to add more resources.
- **Improve employee productivity.** Whether a teller is working with a customer or an insurance adjuster is analyzing data and building out reports, anyone who works with customers, a team, and/or data know that slow or offline networks can significantly impact work by reducing productivity, leading to errors, rework, and an adverse effect on customer satisfaction. Stealthwatch and ISE help avoid or reduce the time of these events, helping everyone stay focused.

## Composite Organization

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 is representative of the three companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

## “Pinnacle” Composite Organization

**Description of composite.** The organization is a US-based financial services company with 30,000 employees. It has 2,000 branches as well as a significant online and phone-based customer contact and support system. Corporate employees primarily work at one of two office locations, with the rest working at branches. Branches have dedicated Internet connections, and use VPN connections for corporate access. However, branch bandwidth and network quality can vary.

**Deployment characteristics.** The organization deployed ISE over a year period, with Stealthwatch deployed soon after over several months. The organization has had both ISE and Stealthwatch in place as integrated solutions for the past year. During deployment five IT employees were focused on Stealthwatch and ISE implementation, along with a few dozen managers and business department employees. After deployment, three IT network management employees have come to support and manage the Stealthwatch and ISE solutions for Pinnacle.

**Key assumptions**

- 30,000 employees
- 50,000 nodes
- 2,000 branches
- 1,000 minor and 3 major security events each year
- 200 total IT employees (5 network engineers focused on this solution)
- Network visibility at or near zero

# Financial Analysis

**QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE**

## Total Benefits

| REF. | BENEFIT | YEAR 1 | YEAR 2 | YEAR 3 | TOTAL | PRESENT VALUE |
|---|---|---|---|---|---|---|
| Atr | Avoided network security remediation costs | $114,685 | $114,685 | $114,685 | $344,055 | $285,204 |
| Btr | Business impact savings from avoided major network | $624,000 | $624,000 | $624,000 | $1,872,000 | $1,551,796 |
| Ctr | IT resource cost savings | $207,000 | $369,000 | $531,000 | $1,107,000 | $892,089 |
| Dtr | Avoided hardware costs | $95,000 | $95,000 | $95,000 | $285,000 | $236,251 |
| Etr | Employee productivity benefits | $565,279 | $565,279 | $565,279 | $1,695,838 | $1,405,766 |
| | Total benefits (risk-adjusted) | $1,605,964 | $1,767,964 | $1,929,964 | $5,303,893 | $4,371,106 |

The table above shows the total of all benefits across the areas listed below, 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 nearly $4.4 million.

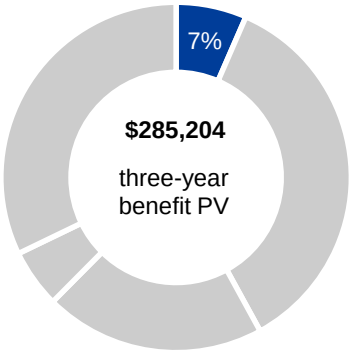
### Avoided Remediation Costs And Business Impact Savings

With improved network monitoring and management comes the ability to identify and handle network security issues more quickly, as well as identify and correct network weak points before anything happens. The implementation of Stealthwatch and ISE enabled:

- **Better network visibility to allow for infrastructure improvements and a more secure network.** The CIO of a worldwide bank reported that, “With Stealthwatch, we’re seeing the whole network.” Pinnacle was able to see how data moved between systems, allowing it to harden security at important points and turn off accounts, ports, and devices that were no longer in use. The CIO continued with an example, “We shut down business in a region, but we still had firewalls and a server that was in place, and both were forgotten until Stealthwatch identified the network connections to completely shut everything off.”
- **Better network management with ISE to help Pinnacle set and automatically enforce network policies.** The organization can set policies by device, location, role, application, user, and other parameters so that access from an unauthorized device or user, or other situations, can be blocked. “Road warrior” employee laptops that haven’t been updated with the latest patches can be kept from accessing the network until patches are installed. Devices infected with serious malware can be quarantined until IT reviews the situation.
- **Network security monitoring and management to stop unusual network activity that might be fraudulent or inadvertent.** The network security team manager reported that, “Stealthwatch provides an early warning against DDoS attacks as well. We’ve got it right where we can see any latency issues.” With Stealthwatch and ISE (as well as an infrastructure with many Cisco TrustSec-compliant network devices), Pinnacle can track unusual activity — data transmissions from a printer network connection, user access to unusual locations at unusual times, and other unusual activity, creating an event alert,

“Stealthwatch provides an early warning against DDoS attacks.”

*Network security team manager, European bank*




Avoided remediation costs



FORRESTER®

sending the user a warning, and/or completely blocking the access. One organization reported that fraudsters and thieves would identify targets and threaten physical violence. Forced access at unusual times could be identified more easily and investigated. The CIO of a worldwide bank highlighted another example: "Our organization alone sees around 400,000 attempted security intrusions or issues a month; external issues happen quite a lot. Unfortunately, it's the internal mistakes that were hard to find, such as an employee introducing a USB with malware. ISE and Stealthwatch help to end and mitigate those threats."

> "Without Stealthwatch and ISE, it [a malware outbreak] could have been hundreds of hours."
>
> *CIO/network architect, worldwide bank*

- **Automatic network enforcement reduces the scope of security issues.** With ISE, Pinnacle has not only seen fewer network security issues reduced, but events that do happen have much less impact than they might have. One organization was attacked with the "WannaCry" ransomware, but the event was contained within a few dozen desktop computers across bank branches, and was cleaned up within a day or two through quick antimalware integrated with ISE that immediately quarantined the machines. "Without Stealthwatch and ISE, it could have been hundreds of hours," continued the CIO of a worldwide bank.

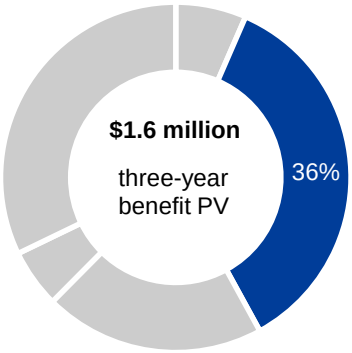
**Avoided Remediation Costs: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| A1 | Reduction in major network security related events requiring remediation each year with Stealthwatch and ISE | | 2 | 2 | 2 |
| A2 | Network admins involved in remediating a major event | | 6 | 6 | 6 |
| A3 | Reduction in time to resolve major issues with Stealthwatch and ISE (hours) | | 200 | 200 | 200 |
| A4 | Reduction in minor network security related events requiring remediation, each year with Stealthwatch and ISE (hours) | | 750 | 750 | 750 |
| A5 | Reduction in time for 1 FTE to resolve minor issues with Stealthwatch and ISE (hours) | | 3 | 3 | 3 |
| A6 | IT network administrator annual salary, fully burdened | | $90,000 | $90,000 | $90,000 |
| A7 | Percentage of network security improvements enabled by Stealthwatch and ISE | | 60% | 60% | 60% |
| At | Avoided network security remediation costs | A6/2080* (A1*A2*A3 + A4*A5) * A7 | $120,721 | $120,721 | $120,721 |
| | Risk adjustment | ↓5% | | | |
| Atr | Avoided network security remediation costs (risk-adjusted) | | $114,685 | $114,685 | $114,685 |

For Pinnacle, the reduction of events and remediation time can measure these improvements to resolve both major security breaches, as well as the more frequent minor attempted attacks, user mistakes, and other issues. The avoided negative business consequences of a security breach are also included. Pinnacle has experienced:

- Most major security breaches are blocked, but major issues requiring remediation have reduced by two per year.

- More significantly, the time to resolve major issues still takes the same six people, but the completion time has reduced by 200 hours for each issue.
- Minor issues have reduced by about two per day.
- Minor issue resolution time has reduced by three hours each.
- Also, the added costs from major security issues — such as lost sales from negative customer reaction, remediation costs, notification costs, customer monitoring costs (such as free credit monitoring subscriptions), regulatory costs, and potential litigation costs — are all greatly reduced or avoided. The average annual cost of remediating a network security event before Stealthwatch and ISE is estimated to be $1.3 million per year, though this will vary greatly from organization to organization.
- The number of events and time required to remediate may be overestimated or underestimated and are thus adjusted by a small risk factor. The added security issue business costs are extremely varied and are thus adjusted at a higher factor.
- To account for these risks, Forrester adjusted these benefits downward by 5% and 20%, yielding three-year risk-adjusted total present values (PVs) of $285,000 for avoided security remediation time and $1.6 million in avoided business costs from security issues adding up to a PV of nearly $1.9 million.




Business impact savings

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

**Business Impact Savings From Avoided Major Network Security Events: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| B1 | Additional major network security event avoided costs related to avoided data breaches, customer relationships, bad press, etc. | | $1,300,000 | 1,300,000 | 1,300,000 |
| B2 | Percentage of network security improvements enabled by Stealthwatch and ISE | | 60% | 60% | 60% |
| Bt | Business impact savings from avoided major network security events | B1*B2 | $780,000 | $780,000 | $780,000 |
| | Risk adjustment | ↓20% | | | |
| Btr | Business impact savings from avoided major network security events (risk-adjusted) | | $624,000 | $624,000 | $624,000 |

## IT Resource Cost Savings

With better reporting and automated management of the network, support and management needs were greatly reduced. “We've implemented a ‘ring of steel’ concept. We put Stealthwatch at chokepoints in our network. It’s there to collect information about data flowing between head offices and branches into our data centers,” said the network security team manager at a European bank, “We can categorize and baseline how our critical business systems interact with each other, and can identify any anomalies.”

With Stealthwatch and ISE, IT teams are able to support a more secure network solution without having to add more resources. “Using Stealthwatch, we collate about 90 days of data, so we can immediately see what a particular IP address or user has touched over a period. That’s something that we couldn’t do before,” continued the European bank manager, “With Stealthwatch, I estimate we can halve the time for

> “We can categorize and baseline how our critical business systems interact with each other, and can identify any anomalies.”
>
> *Network security team manager, European bank*

reporting on analysis. We were guessing before, and now we have some really accurate information."

Pinnacle had planned to add two more IT resources per year over the next three years to manage the old solution. All these planned hires can now be avoided, or hired to other, more valuable teams.

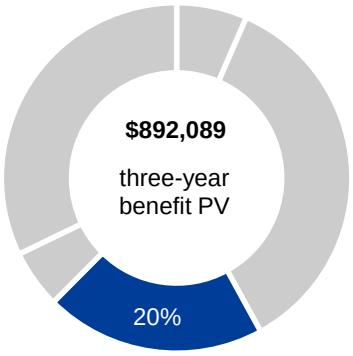
For Pinnacle, Forrester assumes that:

- The current network management security team consists of five people.
- To support its previous solution, it would have needed to add two resources per year over the next three years (for a total of six people hired) to handle network management and security tasks that required manual interaction.
- The recruiting and hiring cost of a new IT network engineer is conservatively estimated to be $25,000.

The reduction in network cost savings will vary with:

- The number of resources expected to be needed today.
- The number of resources planned.
- Salary and recruiting cost estimates.

To account for these risks, Forrester risk-adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $892,000.




IT resource costs savings

**IT Resource Cost Savings: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| C1 | Number of additional employees that would have been required to meet Stealthwatch and ISE results (cumulative) | | 2 | 4 | 6 |
| C2 | Number of new hires that would be required each year to meet Stealthwatch and ISE results | | 2 | 2 | 2 |
| C3 | Cost of recruiting and hiring a new employee | | $25,000 | $25,000 | $25,000 |
| C4 | Network administrator average salary | | $90,000 | $90,000 | $90,000 |
| Ct | IT resource cost savings | C2*C3+C1*C4 | $230,000 | $410,000 | $590,000 |
| | Risk adjustment | ↓10% | | | |
| Ctr | IT resource cost savings (risk-adjusted) | | $207,000 | $369,000 | $531,000 |

## Reduced Hardware Costs

Better network visibility and automated management helps reduce hardware costs. For example, a branch office experiencing network speed issues might pay for extra bandwidth or a new network circuit.

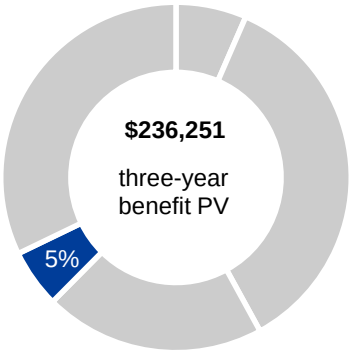
One organization, faced with this issue, was able to use Stealthwatch and ISE to identify that certain users or devices were using a lot of bandwidth — such as one user downloading and syncing a complete database of email message history — which can become a significant share of bandwidth in a small branch office with only a few other people. Pinnacle is able to identify these situations and pinpoint specific users or devices, and resolve the situation without adding more hardware (such

as instructing the user to change their email sync settings).

Forrester estimates the following situation for Pinnacle:

- Five hundred branches (about one-quarter of overall total) have bandwidth issues each year.
- About half of these branches would have resolved their bandwidth issues by adding more hardware or services.
- Additional network bandwidth or a new network circuit would cost about $1,200 per year, on average.
- One-third of these hardware purchases could be avoided with Stealthwatch and ISE.

Bandwidth needs and the network decisions for each branch office are hard to estimate. To account for these risks, Forrester risk-adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $236,000.




Reduced hardware costs

**Reduced Hardware Costs: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| D1 | Number of branches that have bandwidth issues each year | | 500 | | |
| D2 | Percentage of branches that would have invested in more hardware | | 50% | | |
| D3 | Cost of new bandwidth (estimated annual cost) | | $1,200 | $1,200 | $1,200 |
| D4 | Percentage of bandwidth issues that could be avoided or mitigated with better network | | 33.3% | | |
| Dt | Avoided hardware costs | D1*D2*D3*D4 | $100,000 | $100,000 | $100,000 |
| | Risk adjustment | ↓5% | | | |
| Dtr | Avoided hardware costs (risk-adjusted) | | $95,000 | $95,000 | $95,000 |

## Employee Productivity

With all the improvements in network reliability and management, plus more accurate network access policies, employees are able to more quickly and conveniently access the secure network resources they need. Pinnacle's employees have seen increased productivity due to:

- Network policy-setting and automated access management with ISE allows the organization to set and maintain their policies, instead of having to lock down certain resources to just a few people. The right employees can gain access to the right resources at the right times, automatically, without having to wait for IT response times.
- Better network management and visibility with ISE and Stealthwatch helps reduce network downtime or slowdowns. The CIO of a worldwide bank reported that, "The diagnostics in Stealthwatch are very handy in an outage — you can see exactly which server fails; it's the go-to tool when a thing is not normal."
- Fewer network issues also means more normal network operation time.

Forrester estimates the following situation for Pinnacle:

"The diagnostics in Stealthwatch are very handy in an outage — you can see exactly which server fails; it's the go-to tool when a thing is not normal."

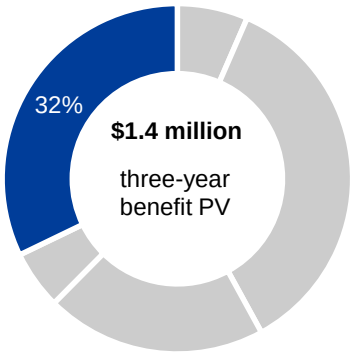
*CIO/network architect, worldwide bank*



FORRESTER®

- Fifteen-thousand employees are impacted by network security or bandwidth issues.
- Fifty-five network security or bandwidth issues occur each year across multiple locations and each issue impacts about one-tenth of those employees, on average.
- Each issue takes two hours less than before (using the minor issue time savings from above as a conservative estimate).
- About one-fourth of that time savings leads to direct employee productivity time savings (such as events that used to occur right in the middle of the business day).
- Employees use about half of any saved time on direct, work-related tasks (with the remaining time spent on breaks, conversations, and other important but not directly task-related work).

Employee productivity is hard to estimate, and times savings may be overestimated. To account for these risks, Forrester risk-adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $1.4 million.




Employee productivity

**Employee Productivity: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| E1 | Employees impacted by security or bandwidth issues (without Stealthwatch or ISE) | | 15,000 | 15,000 | 15,000 |
| E2 | Network or bandwidth issues per year | | 55 | 55 | 55 |
| E3 | Percentage of employees impacted by each issue | | 10% | 10% | 10% |
| E4 | Time to resolve each issue (average, in hours) | | 2 | 2 | 2 |
| E5 | Average hourly employee salary, fully burdened | $60,000/2080 | $28.85 | $28.85 | $28.85 |
| E6 | Percentage of recovered time spent on work-related tasks | | 50% | 50% | 50% |
| E7 | Percentage of savings enabled by Stealthwatch and ISE | | 25% | 25% | 25% |
| Et | Employee productivity benefits | E1*E2*E4*E5 *E6*E7*E3 | $595,031 | $595,031 | $595,031 |
| | Risk adjustment | ↓5% | | | |
| Etr | Employee productivity benefits (risk-adjusted) | | $565,279 | $565,279 | $565,279 |

## Unquantified Benefits

While somewhat estimated above, the business impact of major security breaches is difficult, even impossible, to estimate a reasonable average that is applicable to many organizations. For Pinnacle, the risk of a major network breach through mistakes, employee maliciousness, or external attacks could lead to:

- Audit or regulatory body issues, fines, or other punishment.
- Customer dissatisfaction or lost sales.
- Customer remediation costs such as credit reporting services.
- Bad press.

- Lost business partnerships.
- And even closing the business.

While none of these have ever happened to Pinnacle, or any of the interviewed customers, the concern is always present for network security teams. With Stealthwatch and ISE, these organizations are much more confident in their ability to avoid any significant security event impact on business costs and revenue.

Business benefits from avoiding major network security events is hard to estimate, but may be very, very large for some organizations.

## Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Stealthwatch and ISE and later realize additional uses and business opportunities, including:

- **Cisco TrustSec.** Cisco ISE is TrustSec-ready, which helps reduce implementation and management time even more. Forrester Consulting conducted a TEI study for Cisco, focused on TrustSec, and it was found that for four interviewed organizations the technology can provide a number of network management and business benefits, adding up to an NPV of $2.3 million.
- **Cisco NetFlow.** Cisco Stealthwatch can incorporate NetFlow network traffic data to improve reporting and data analysis capabilities.
- **Continued ISE deployment to all branches and offices.** Branches are often small and spread out, but ISE takes the time to coordinate an IT deployment without disrupting employees and customers. The CIO of a worldwide bank reported that: “Our branch management unfortunately still requires manual effort. That’s why we need to get ISE in those campuses as well.”

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a 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.

## Total Costs

| REF. | COST | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 | TOTAL | PRESENT VALUE |
|---|---|---|---|---|---|---|---|
| Ftr | Ongoing licensing and resource costs | $0 | $304,500 | $304,500 | $304,500 | $913,500 | $757,246 |
| Gtr | Implementation labor costs | $480,000 | $0 | $0 | $0 | $480,000 | $480,000 |
| Htr | Implementation hardware, software, and services costs | $745,500 | $0 | $0 | $0 | $745,500 | $745,500 |
| | Total costs (risk-adjusted) | $1,225,500 | $304,500 | $304,500 | $304,500 | $2,139,000 | $1,982,746 |

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of nearly than $2 million.

## Ongoing Costs

Pinnacle pays a maintenance and support contract to Cisco, plus it has dedicated internal resources managing Stealthwatch and ISE, including:

- Maintenance fees of $110,000 per year, estimated to be 20% of the upfront licensing costs shown below.
- Five full-time equivalents (FTEs) of IT network administrator resources spending some of their time managing Stealthwatch and ISE. Readers should keep in mind that while these resource costs are included, there are also significant IT resource savings detailed in the Benefits section.

Some organizations deployed Stealthwatch and ISE as a first full network visibility and security solution, while most had a previous solution. For this analysis Forrester assumes that no significant solution was replaced, though that situation may be different for many organizations. One interviewed organization highlighted their experience: "We replaced a solution that cost a million dollars per year with one that cost a half million dollars."

Maintenance and resource costs may be underestimated, so Forrester risk-adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $757,000.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

**Ongoing Costs: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| F1 | Stealthwatch and ISE license and maintenance fees (20%) | | | $110,000 | $110,000 | $110,000 |
| F2 | Ongoing resource costs | | | $180,000 | $180,000 | $180,000 |
| Ft | Ongoing licensing and resource costs | F1+F2 | $0 | $290,000 | $290,000 | $290,000 |
| | Risk adjustment | ↑5% | | | | |
| Ftr | Ongoing licensing and resource costs (risk-adjusted) | | $0 | $304,500 | $304,500 | $304,500 |

## Implementation Costs

Stealthwatch and ISE implementation can vary. One interviewed organization chose to roll out ISE over three years, while another rolled ISE and Stealthwatch out over the course of a year, and a third rolling out Stealthwatch in two months. One organization is also rolling out TrustSec-enabled hardware at all locations — a significant, multi-million-

dollar project on its own. The CIO of a worldwide bank highlighted his team's deployment progress across main office buildings, "We managed to deploy ISE over 27 campuses and 33,000 workstations over the last two months."

Stealthwatch and ISE are integrated, but different, solutions, and can be (and are often) implemented as separate projects, or different workstreams of a larger project. Implementation can vary across organizations due to current network and security maturity (number of locations and employees) and other scale metrics (current network infrastructure).

**Six months**
Total implementation and deployment time

**Implementation Labor Costs: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| G1 | Implementation resource costs | | $400,000 | | | |
| Gt | Implementation labor costs | G1 | $400,000 | $0 | $0 | $0 |
| | Risk adjustment | ↑20% | | | | |
| Gtr | Implementation labor costs (risk-adjusted) | | $480,000 | $0 | $0 | $0 |

For Pinnacle, based on interviewed organizations, implementation was a six-month process that included:

- Resource costs of $400,000 over a one-year deployment, primarily IT, but also a number of business department representatives that helped develop reports, identify requirements, and other needs.
- For the composite organization, the software license cost for Stealthwatch and ISE is conservatively estimated to be $550,000 based on Cisco standard pricing.
- Required hardware update or replacement costs of $100,000 necessary for Stealthwatch and ISE deployment.
- Additional services costs of $60,000.
- These costs may be overestimated or underestimated, and are thus adjusted by a small risk factor. The resource requirements and costs are more variable and are adjusted at a higher factor.
- To account for these risks, Forrester adjusted implementation costs upward by 5%. Resource costs are risk-adjusted to $480,000 and other costs are risk-adjusted to $746,000 for a total implementation cost of $1.2 million.

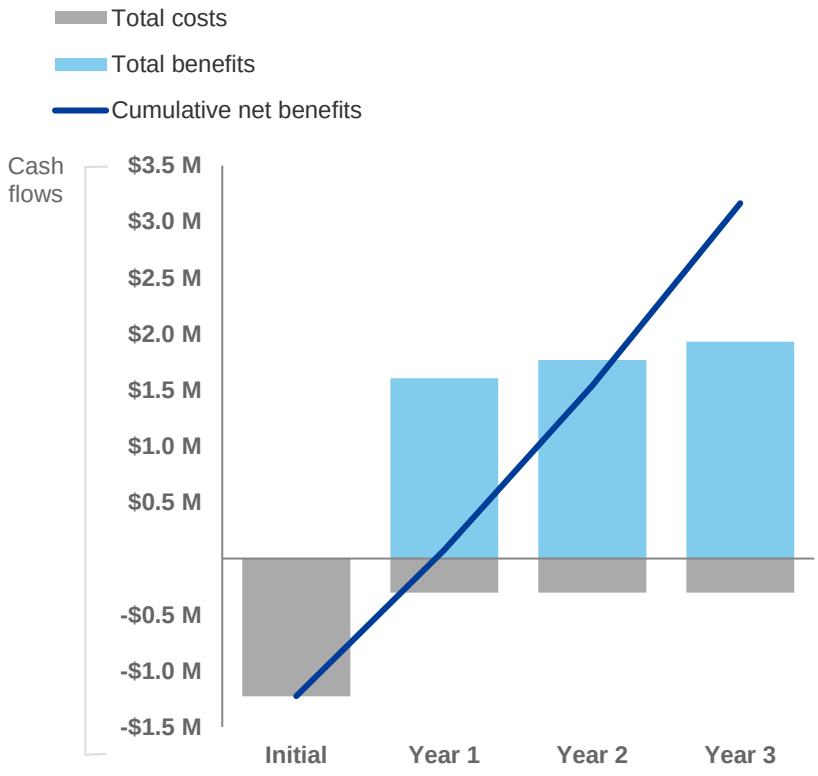
**Implementation Hardware, Software, And Services Costs: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| H1 | Software | | $550,000 | | | |
| H2 | Hardware | | $100,000 | | | |
| H3 | Services | | $60,000 | | | |
| Ht | Implementation hardware, software, and services costs | H1+H2+H3 | $710,000 | $0 | $0 | $0 |
| | Risk adjustment | ↑5% | | | | |
| Htr | Implementation hardware, software, and services costs (risk-adjusted) | | $745,500 | $0 | $0 | $0 |

# Financial Summary

**CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS**

## Cash Flow Chart (Risk-Adjusted)




The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

**Cash Flow Table (Risk-Adjusted)**

| | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 | TOTAL | PRESENT VALUE |
|---|---|---|---|---|---|---|
| Total costs | ($1,225,500) | ($304,500) | ($304,500) | ($304,500) | ($2,139,000) | ($1,982,746) |
| Total benefits | $0 | $1,605,964 | $1,767,964 | $1,929,964 | $5,303,893 | $4,371,106 |
| Net benefits | ($1,225,500) | $1,301,464 | $1,463,464 | $1,625,464 | $3,164,893 | $2,388,360 |
| ROI | | | | | | 120% |
| Payback period | | | | | | 12.0 |



FORRESTER®

# Cisco Stealthwatch And ISE: Overview

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

## Get True Visibility With Stealthwatch And ISE

**USE SECURITY AS A GROWTH ENABLER**

Fueled by trends such as mobility, IoT, cloud, and advanced analytics organizations are racing to reap the benefits of digitization. The key to these benefits is adapting networks to operate at digital speeds and keeping them secure against threats. When companies are confident about their security, they are able to innovate, adopt new technologies, and develop new services. Unfortunately, in a recent survey, 39% of organizations have halted a mission-critical initiative due to cybersecurity concerns. Even when people know their system is compromised, they don't always know where it's happening and how, making them susceptible to network abuse and insider threats. Organizations need a solution that provides extensive network visibility enhanced by rich user and device details to speed up threat detection and response. Only the combination of Stealthwatch and Cisco's Identity Services Engine helps organizations get a 360° view, respond to threats faster, and secure a growing digital business.

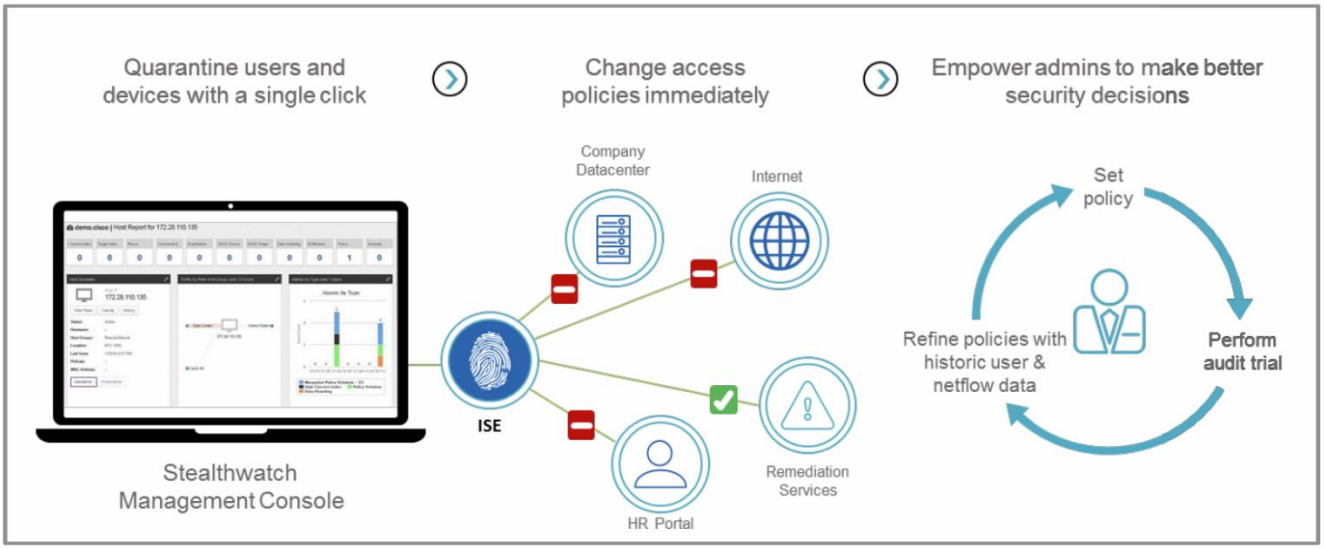

**GET A 360° VIEW**

Gain unmatched visibility and control with integration between Stealthwatch and ISE:

- Continuously monitor, analyze, separate, categorize, and store host and user information from your network with Stealthwatch.
- Enable administrators to see details about each individual device — type, operating system, compliance status, connection method, geographical location and more with ISE.
- Discover anomalous traffic in your environment. Applying context-aware security analysis to automatically detect anomalous behaviors, Stealthwatch can identify a wide range of attacks, including malware, zero-day attacks, DDoS attempts, advanced persistent threats (APTs), and insider threats.
- Know exactly when individual user behavior becomes suspicious. Stealthwatch enables admins to set their own behavior thresholds, once a user crosses the threshold it triggers an alert.

## RESPOND WITH RAPID THREAT CONTAINMENT

No matter how advanced the security, some threats will still get in. The solution isn't to build larger walls, it's about speeding up the way you respond.




- Once Stealthwatch detects anomalous traffic, it issues an alert, giving the admin the option to quarantine the user. pxGrid enables Stealthwatch to hand off the quarantine command directly to ISE.
- Admins can make a decision based on analysis, revoking users' access, and quarantining them through ISE with a single click. Admins don't need to modify or change the overall system policies in place because ISE reassigns the access policy of the quarantined individual.
- Find the root cause of a breach with post-incident audit trails. Stealthwatch stores records of all network activity for months or years. For more on responding to threats faster, go to: www.cisco.com/go/rtc.

## SECURE YOUR GROWING DIGITAL BUSINESS

To move forward with new initiatives or technologies confidently, businesses must know they can scale without creating new security issues.

- Stop thinking about security as an obstacle and provide a foundation for network segmentation for secure access and visibility.
- Enable admins to carefully control access to sensitive assets, know precisely when someone tries to access information, and extend that visibility to any new area of the network, environment, or cloud.
- Add users, devices, and business without compromising network visibility. Reduce the administrative burden of setting up new devices with constantly updating device profile feeds from ISE.
- Scale the environment without creating blind spots. A deployment of Stealthwatch can process data from 50,000 flow sources at 6 million flows per second (fps) all while stitching and deduplicating flows.
- Reduce the administrative burden associated with siloed management sources. Networkwide flow is centrally displayed in the Stealthwatch Management Console. Easily integrate 3rd party technologies and services through a REST API.

## NEXT STEPS

To learn more visit www.cisco.com/go/Stealthwatch or www.cisco.com/go/ise.

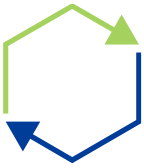
# Appendix A: Total Economic Impact

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

## Total Economic Impact Approach

**Benefits** represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

**Costs** consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.



**Flexibility** represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

**Risks** measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

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

**PRESENT VALUE (PV)**

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

**NET PRESENT VALUE (NPV)**

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

**RETURN ON INVESTMENT (ROI)**

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

**DISCOUNT RATE**

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

**PAYBACK PERIOD**

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

# Appendix B: Endnotes

[1] Forrester Consulting conducted a TEI study for Cisco that was focused on TrustSec. Source: "The Total Economic Impact Of Cisco TrustSec," a commissioned study conducted by Forrester Consulting on behalf of Cisco, August 2016 (https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-access-control-system/tei-of-cisco-trustsec.pdf)