A Forrester Total Economic Impact™ Study

Commissioned By

Cisco

Project Director:
Sean Owens

October 2013

The Total Economic Impact™ Of Cisco Identity Services Engine

Cost Savings And Business Benefits Enabled By ISE

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Executive Summary

In January 2013, Cisco Systems commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) enterprises may realize by implementing Cisco Identity Services Engine (ISE). Four customers were interviewed for this study and covered use cases for policy-governed, unified access across the following use case scenarios:

- **Bring-your-own-device (BYOD),** including "choose-your-own-device" (CYOD).
  - **BYOD** refers to allowing employees to bring a preferred device from home and providing support for full or partial network access via wired or wireless networks.
  - **CYOD** refers to an organization providing a list of preferred devices that employees can pick from — hopefully varied enough that providing a full and varied BYOD option is not necessary.
- **Guest wireless access services,** providing guests visiting your offices with basic Internet access (typically not intranet or network resources).
- **Wired, wireless, and VPN services,** supporting the management and authentication of devices, locations, access methods, and accounts to ensure updates are installed and rules followed before providing full access.
- **Policy networking,** managing the rules and business logic for the scenarios listed above in a role-based way in which profiles can be created and users quickly and efficiently added, removed, or updated. Cisco TrustSec extends Cisco ISE policy to build on existing identity management to enforce, manage, and scale policy settings across the organization.

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cisco Secure Access Solutions — particularly Cisco ISE — for their organization taking into consideration the various use case scenarios.

Cisco Identity Services Engine can help save costs and improve end user productivity.

The costs and benefits for a composite organization of 10,000 employees, based on customer interviews, are:

- **Investment costs: $595,000.**
- **Annual costs: $61,000.**
- **Total cost savings and benefits: $855,000 per year.**

Benefits are estimated based on the following business improvements highlighted during Cisco customer interviews:

- **A 75% reduction in support calls related to network issues.**
- **Improved compliance reducing data exposure, breaches, and potential regulatory/remediation costs that could add up to hundreds of thousands or even millions of dollars for some organizations.**

CISCO ISE PROVIDES STREAMLINED, POLICY-GOVERNED, UNIFIED ACCESS INFRASTRUCTURE

Forrester's interviews with Cisco ISE customers spanned various company sizes, industries, and use cases, and the subsequent financial analysis found that a composite organization based on insights from the interviewed customers experienced the risk-adjusted ROI, costs, and benefits shown in Table 1.[1]

TABLE 1
Composite Organization Three-Year Risk-Adjusted ROI and NPV

ROI	Payback period	Total benefits (PV)	Total costs (PV)	Net present value
212%	9 months	$2,127,455	($746,956)	$1,380,499

Source: Forrester Research, Inc.

› **Benefits.** The composite organization experienced the following risk-adjusted benefits with Cisco ISE, organized by use case scenario, totaling about $855,000 per year.

- **Reduced infrastructure, management, and support costs for guest wireless access services.** IT can reduce guest access account setup, monitoring, and removal in favor of ISE's nearly self-service guest management tools to save $182,000 per year.
- **Reduced infrastructure, management, and support costs for BYOD support.** IT can eliminate management and support time with policy-based network authentication that registers not only who and where the user is, but whether the user's PC is up-to-date, what device is used, and what application is needed. It also eliminated the need to manage separate network access for wired, wireless, and VPN networks. This adds up to a savings nearly $275,000 per year for the composite organization.
- **Reduced help desk costs.** With easier device management leading to fewer delays and issues, the composite organization has seen a significant drop in help desk calls related to network issues, for an annual savings of nearly $36,000.
- **Reduced risk of security issues and major outbreaks.** With ISE's policy networking, unknown devices never gain access, and virus and malware issues, in conjunction with user and security management systems, can be quarantined before an outbreak can occur. In many cases issues can be avoided even before that device can access the full network, leading to significant improvements in data and security compliance. The composite organization saved or avoided costs of nearly $365,000 per year related to data security.

› **Costs.** The composite organization incurred the following risk-adjusted costs, totaling about $595,000 in one-time, initial investment and implementation costs, plus $61,000 administration and maintenance costs per year.

- **Hardware and software** purchase costs of about $542,000.
- **Planning, implementation and deployment** effort and services costs of a little less than $53,000.
- **Ongoing management,** licensing and services costs of about $61,000 per year.

Disclosures

The reader should be aware of the following:

› The study is commissioned by Cisco and delivered by Forrester Consulting.

› Forrester makes no assumptions as to the potential return on investment 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 ISE.

› 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.

› The customer names for the interviews were provided by Cisco. Cisco did not participate in the Interviews.

TEI Framework And Methodology

INTRODUCTION

From the information provided during interviews with Cisco subject matter experts and customers, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Cisco ISE. 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 ISE can have on an organization (see Figure 1). Specifically, we:

- Interviewed Cisco marketing, sales, and/or consulting personnel, along with Forrester analysts, to gather data relative to Cisco ISE and the marketplace for Cisco ISE.
- Interviewed four organizations currently using Cisco ISE to obtain data with respect to costs, benefits, and risks.
- Designed a composite organization based on characteristics of the interviewed organizations (see Appendix A).
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews as applied to the composite organization.

Forrester employed four fundamental elements of TEI in modeling Cisco ISE's service:

- Costs.
- Benefits to the entire organization.
- Flexibility.
- Risks.

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

Analysis

COMPOSITE ORGANIZATION

A total of four interviews were conducted for this study, involving representatives from the following Cisco customers:

- A private liberal arts university in the United States, with more than 2,500 undergraduate and post-graduate students.
- A regional drinking water and sewage utility serving 1.6 million people in the Southwestern United States.
- A major financial services company based in the United States, providing personal, home, and student loans and banking and credit card services.
- A regional credit union in the Southeast United States, with over 1,000 employees serving more than 400,000 members from 30 branches.

All of the customers interviewed were using Cisco ISE, which enables inbound and outbound identity management.

FIGURE 1
TEI Approach

Source: Forrester Research, Inc.

A composite organization, referred to as *the organization* throughout the remainder of the case study, was developed based on information and feedback from the interviewed organizations that are described in this study while maintaining interviewee confidentiality. *The organization* initially adopted a solution based on Cisco ISE to replace older Cisco NAC servers to better manage and provision guest access. However, finding ISE to be a useful and effective resource for managing and checking devices that access the network, *the organization* quickly expanded its use of Cisco's solutions to include guest access, policy networking, and bring-your-own-device support (BYOD).

The organization is a Forbes Global 2000 company with global reach but primarily does business in the United States. Its diversified business includes direct sales of a broad portfolio of products and services for both B2C and B2B customers. Its 10,000 employees have continued to bring more personal devices to work, such as mobile phones and tablets. They have requested access to work-related resources from them, such as email and document access, but more and more those requests include a desire to connect to line-of-business (LOB) systems, such as CRM access for sales reps using their tablet device.

The organization saw a need to manage and secure these devices, as well as gain better visibility across all corporate devices, to ensure all devices meet operating system update and security requirements. It maintains relationships with customers, suppliers and vendors, distributors, and business affiliates, and those representatives often visit corporate or regional offices where they would like to access Internet resources.

The organization's user base consists of roughly 10,000 employees and 150 partners and business affiliates that visit a corporate or regional office at least once a year. For the purposes of the financial model, we assume the functional user base to be roughly 10,000 users with 2.25 devices each (a phone, a laptop, and perhaps a tablet or device brought from home), and an average of 100 (usually not more than 200, but occasionally nearing 500 or 1,000) guest device accounts provided per day.

"ISE is fantastic for ensuring compliance of all our devices."

~Network engineer at a regional credit union

INTERVIEW HIGHLIGHTS

Similar to customers interviewed, *the organization* adopted Cisco ISE to:

- **Reduce management and security costs related to device management and BYOD.** Prior to implementing Cisco ISE, *the organization* did not provide device-based identity management, so users were able to log in from a personal device or a device that might not have accessed the corporate network for a month. This meant that parameters such as what kind of device it was, when Windows Update was last run, whether the latest virus profile was installed, and other device-specific details were not checked, which resulted in out-of-policy devices being allowed access too often. This in turn led to a high volume of inbound help desk requests and time spent by IT and security reps resolving system errors, virus outbreaks, etc. With Cisco ISE, corporate devices can be managed much more closely, and personal device access can be limited — whether connecting via the wired or wireless network. Non-user devices, such as shared printers and cameras, can also be managed with the same tools.

"Cisco Identity Services Engine has improved our access services across the board: better reliability and scalability, and simplification of guest management functions."

~Network manager at a major financial services company

- **Reduce or eliminate IT management costs related to guest wireless access.** Before implementing Cisco ISE, *the organization* had implemented an earlier generation of guest access management. However, the system was nearing its capacity on busy days (which was still only a few hundred guests). Additionally, the system required IT interaction to collect requests, set up accounts, and distribute the log-in information. It did not include account expiration, meaning the IT resource had to spend additional time shutting off the account — or leaving a potential security risk open. With Cisco ISE, *the organization* eliminated nearly all IT time for this task,

providing easy-to-use tools that reception staff could use immediately when guests arrive.

- **Reduce help desk support costs**. All the above time savings focus on senior network and security administrators having to deal with problems that require their attention, possibly even in person. But first the user likely calls help desk. By significantly avoiding the management and security issues above, the number of help desk calls was also reduced. Assuming that most help desk calls can be resolved without escalating to a network or security admin, and that each issue might take up to 4 hours, the total help desk calls add up to just over 15,000 — nearly all of which could be avoided with a Cisco ISE solution that provides easy-to-access guest wireless and improvements in management and security that stop issues before they occur.

"ISE enables increased device traceability, and we can use that data to deliver improved audit and compliance reports to our internal and external auditors."

~Network engineer at a regional credit union

- **Close security holes that could lead to a major data breach.** Failure to close a guest account, determine if the latest system and virus updates are installed, or check whether the BYOD device a user is logging in from meets standards (e.g., device encryption) can lead to significant security holes. An account kept live can provide a hacker a back door into the system, malware software could be installed that allows access to the network to collect information, or an unsecure device with confidential information could be stolen or lost. Any single one of these issues (or a variety of others) could lead to expensive costs and/or a major public relations blunder; confidential information left on an employee's personal, unencrypted device that was stolen or lost would likely require public notification that could lead to dissatisfaction and reduced sales, plus *the organization* would need to compensate exposed users with money or a service such as free credit report checking over several years. With ISE, these issues are completely avoided or greatly reduced, helping to reduce remediation costs as well as greatly reducing business risks due to lost or stolen data.

BENEFITS

Based on interviews with people at organizations that have deployed Cisco ISE, *the organization* experienced several benefits:

- Reduced labor costs for setting up, supporting, and managing device and BYOD access.
- Reduced labor costs setting up, supporting, and turning off wireless guest accounts.
- Reduced help desk costs.
- Reduced or avoided data breach direct and indirect costs.

Avoided Device Mgmt. And Support Costs, Including BYOD

Cisco ISE authenticates the user and device and determines network access based on who, what, where, and how. Cisco ISE uses additional context from other systems (such as AV or MDM) to determine the security risk and answer questions such as: are updates installed, does it have pin lock, is encryption on? Policy networking allows granular control; for example a user with his or her personal iPad, or another connecting their work laptop via a Starbucks open wireless, may be allowed access, but only to less-critical systems like email or document collaboration.

But a company can't just block all unknown devices; employees are asking for access to company resources (like email) on their personal devices, and companies increasingly see a BYOD strategy as key. But once a company offers BYOD or choose-your-own-device (CYOD) options for employees, it runs the risk of additional issues if it doesn't implement a strong security and management solution such as Cisco ISE. (CYOD is like BYOD but the list is limited to a set of devices provided by the organization.)

A user logging in on a corporate standard laptop after vacation at the office or over VPN can be given limited or no access until virus and system updates are installed, a user logging in from a Starbucks public wireless can be given full access to resources like email and collaboration software but blocked from more confidential resources like the financial system, or a user logging in from his or her personal laptop or tablet device can be blocked from all corporate resources and only given Internet access.

Absent Cisco ISE, often just the user account is checked as a valid account or part of a group that gets special access rights. The user's device and location are not checked. With Cisco ISE issues related to these additional security and compliance risks, and the resulting IT support escalation time, can be greatly reduced or avoided altogether.

Some interviewed organizations chose simple BYOD access – similar to Guest Access. This provides employees (usually) full Internet access, but not access to any internal network resources. Cloud services, such as email or document collaboration, remain accessible, and VPN access can be restricted or provided to the few that might need it. While this does limit employee access from their personal devices, it does have the added benefit of being easier to manage, less risky, and also only requires a Cisco ISE end user base license (instead of the advanced license). It is assumed *the organization* can take advantage of this by provisioning some base licenses to end user devices that require basic internet access, and these assumptions are included in the total base and advanced license needs outlined in the License Fees cost section.

Additionally, some interviewed organizations agreed that

TABLE 2
Avoided Device Management And Support Costs: Time Saved Managing User Devices, Including BYOD

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Hours spent per week setting up, securing and managing BYOD devices without ISE		100		
A2	Percent reduction in time setting up, securing and managing BYOD devices with ISE		75%		
A3	IT administrator hourly rate		$70		
At	**Reduced IT labor costs managing devices including BYOD**	**A1 * A2 * 52 * A3**	**$273,000**	**$273,000**	**$273,000**

Source: Forrester Research, Inc.

BYOD provides additional benefits in terms of greater employee job satisfaction and reduced turnover. The ability to bring a preferred device from home or to choose a preferred device from a list of supported corporate devices can be a factor in job satisfaction and longevity. And organizations that would otherwise have to provide common devices, like a cell phone, to ensure security policies, can instead allow employees to use their own phone at work if they choose to, again helping with job satisfaction as well as potentially avoiding phone hardware costs.

For *the organization*, before Cisco ISE, around 100 hours per week was spent setting up, securing, and managing devices (including BYOD devices) and dealing with device management and security escalations. With ISE, *the organization* was able to eliminate nearly all related issues due to out-of-date system or virus updates. It was also able to close a number of security holes and reduce time managing and reviewing device characteristics and unusual behavior (such as a high amount of network traffic from a previously quiet work device — even devices such as printers). It could then apply the appropriate level of security and access, all from one management interface. Overall, *the organization* saw a 75% reduction in time spent on tasks in this category, adding up to a non-risk-adjusted total of nearly $275,000 in labor cost savings per year as shown in Table 2. Over three years, the non-risk-adjusted net present value (NPV) of this benefit is just over $675,000.

Reduced IT Labor Costs For Guest Account Configuration

Guest accounts are a great way to welcome business partners and allow them to communicate and collaborate while at your offices. But without a good and easy-to-use guest account management system, significant costs may be spent on alternatives. Providing a simple wireless network may require additional hardware or could open security holes. A more secure policy may require a lot of extra time for IT managers to review requests, create accounts, deal with any follow-up issues with the guest, and delete accounts once the guest has left (if they remember to at all!). The time spent setting up and deleting accounts once the guest has left is a common process, based on interviews with Cisco ISE customers, and is modeled here.

With Cisco ISE, basic wireless Internet access can be provided using the same hardware, and the reception staff can easily create and manage accounts using a guest account creation page. This page connects to the Cisco ISE system and automatically fills in start and end account activation times. The guest simply receives a unique login and password, signs in to the page automatically opened in their browser, and the account is automatically deactivated at the end of the day. Unless there is a system issue, IT does not need to get involved.

The organization, based on customer interviews, set up about 100 guest accounts per day, primarily at the headquarters offices; each account took 8 minutes to set up — plus as long as 30 minutes before the guest finally was provided access credentials. With Cisco ISE, guest access is easier to manage and more automated, and reception can help guests set up their account quickly. As shown in Table 3, *the organization* estimates a 75% reduction in time spent on guest account creation, not counting the waiting

TABLE 3

Avoided Guest Access Management And Support Costs: Time Saved Managing And Setting Up Guest Accounts

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Number of new guest account requests per day		100		
B2	Minutes spent per guest account configuration without ISE		8		
B3	Percent time saved on guest account configuration with ISE		75%		
B4	IT administrator hourly rate		$70		
Bt	**Reduced IT labor cost for guest account configuration**	**B1 * 260 * B2 / 60 * B3 * B4**	**$182,000**	**$182,000**	**$182,000**

Source: Forrester Research, Inc.

time the guest might have sat through. This adds up to a non-risk-adjusted total of more than $180,000 in labor cost savings per year, as shown in Table 3, and a three-year NPV of more than $450,000.

Reduced Help Desk Support Costs

Because of the improvements in network management and the delivery of services like guest access, the overall number of help desk calls was reduced for *the organization*. Assuming that each employee and average guest might make three help desk calls per year, that half of those calls might be related to BYOD and guest access management and support (covered above, and thus excluded here to avoid double-counting), the total network- and security-related help desk calls that could be improved or eliminated with Cisco ISE is more than 15,000 per year. If each call takes about 5 minutes to resolve or escalate, and with Cisco ISE's better management of security, device access, BYOD, and guest access, it's expected that nearly all (75%) of these calls could be greatly reduced or avoided.

This adds up to a non-risk-adjusted total of about $38,000 per year in annual help desk cost savings, as shown in Table 4, and a three-year NPV of nearly $95,000.

Avoided Potential Data Breach Costs

With the improved security enabled by Cisco ISE, avoiding security breaches not only reduces management and resolution labor costs but also helps avoid potential significant costs that often must be paid after a breach of private or customer data. For example:

- A guest account that isn't disabled or deleted after the guest leaves means it remains an active account, which could provide hackers with an easy front door to more secure systems and data.
- A user who hasn't accessed the network for a while, or has brought a device from home, may not have updated his or her system and virus settings. While Windows Update and virus software will typically check within a day and apply updates, that window could provide an opportunity for malware software to be installed, which could collect and send data to an identity thief.
- An unencrypted personal device granted network access could have confidential information stored on it, leading to a potential breach if that device is lost or stolen.

Any single one of these issues can result in expensive compliance issues and remediation costs such as paying for credit reports for customers with exposed accounts. And it can become a major public relations event leading to bad press, reduced sales, partnerships put at risk — or even the end of the business.

Research by a number of organizations has estimated that the cost of a single lost or exposed data record is about $180. It's assumed that *the organization* has relatively mature security policies; it maintains an up-to-date virus security solution across all servers and user devices, keeps software up-to-date and refreshes hardware regularly, and has documented data management processes for sensitive

TABLE 4

Avoided Help Desk Call Costs: Time Recovered From Help Desk Calls Avoided Due To Simpler, Easier, And Faster ISE Tools

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Number of help desk calls per year related to network access and device updates without ISE (not related to BYOD and guest setup, above)		15,150		
C2	Percent reduction in help desk calls related to network access and device updates with ISE		75%		
C3	Average length per call (minutes)		5		
C4	Help desk support hourly rate		$40		
Ct	**Reduced help desk support costs**	**C1 * C2 * C3 / 60 * C4**	**$37,875**	**$37,875**	**$37,875**

Source: Forrester Research, Inc.

data. For a company of this size and overall security maturity, it's estimated that a data breach at *the organization* would include around 30,000 records and has about a 9% chance of happening in a given year. In other words, without significant change, a major data breach would likely happen about once every 10 or 11 years.[2] While the actual costs would either be $0 or a very large number in any single year, over the long run, the average potential cost can be estimated, but multiplying the likelihood of occurring, times the cost per exposed record, times the total number of records.

Closing these security holes with Cisco ISE can lead to significant reduction in business risk, measured here as a 75% improvement by:

- Ensuring that all devices are up-to-date and comply with security standards (even ones that are new or haven't maintained consistent network connectivity).
- Ensuring that out-of-policy devices are not allowed access to sensitive materials.
- Guest accounts are closed automatically and quickly.

These can lead to significant reductions in the number of exposed records and the likelihood of a breach. As shown in Table 5, for *the organization* this adds up to nearly $365,000 per year in average potential data breach avoided costs, and a three-year NPV of more than $900,000.

Total Benefits

Table 6 shows the total of all non-risk-adjusted benefits mentioned above as well as associated present values, discounted at 10%.

TABLE 5
Avoided Device Management And Support Costs: Time Saved Managing User Devices, Including BYOD

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Chance of a data security breach in given year		9%		
D2	Average number of records exposed		30,000		
D3	Cost of data breach, per record exposed		$180		
D4	Estimated reduction in chance of data security breach with Cisco ISE		75%		
Dt	**Avoided potential data breach costs**	**D1 * D2 * D3 * D4**	**$364,500**	**$364,500**	**$364,500**

Source: Forrester Research, Inc.

TABLE 6
Total Benefits (Non-Risk-Adjusted)

Benefit	Initial	Year 1	Year 2	Year 3	Total	Present value
Reduced IT labor cost managing devices including BYOD	$0	$273,000	$273,000	$273,000	$819,000	$678,911
Reduced IT labor cost for guest account configuration	$0	$182,000	$182,000	$182,000	$546,000	$452,607
Reduced help desk support costs	$0	$37,875	$37,875	$37,875	$113,625	$94,190
Avoided potential data breach costs	$0	$364,500	$364,500	$364,500	$1,093,500	$906,458
Total benefits (non-risk-adjusted)	**$0**	**$857,375**	**$857,375**	**$857,375**	**$2,572,125**	**$2,132,165**

Source: Forrester Research, Inc.

COSTS

Similar to customers interviewed, *the organization* incurred three costs for implementing and maintaining Cisco ISE:

- Cisco ISE purchase costs, which includes retail costs of hardware, software, and endpoint licenses.
- Internal and external resources required for implementation and deployment.
- Ongoing management and support costs.

Cisco ISE Appliance And Licensing Fees

Cisco ISE is available as either a virtual or physical appliance and comes with a variety of options. While any organization's costs will depend on the organization's size and licensing agreement, *the organization*'s costs are based on interview results for the number of appliances and licenses and publicly available retail information for license costs. A Cisco ISE appliance for an organization of this size lists for around $23,000. Six devices provide high availability and full coverage across key workloads (management, administration, and runtime), with advanced user licenses for employee primary business devices, and base user licenses for lighter roles such as BYOD and guest access. Based on *the organization*'s profile, we determine that it purchased and deployed six Cisco ISE appliances plus nearly 17,000 endpoint licenses (of which 25% are base and 75% are advanced, and have list prices of $5 and $30 respectively – note that the $25 additional cost for the advanced license can be a subscription-term-based license, though is assumed to be paid upfront here). (See the benefit section detailing Avoided Device Management for more detail on the division base versus advanced licenses.)

TABLE 7
Appliance And Licensing Fees

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Number of new ISE appliances		6			
E2	Cost per appliance (list price)		$23,000			
E3	Number of workers with mobile devices		10,000			
E4	Devices per worker with mobile devices, including BYOD		2.25			
E5	Percent worker devices that require advanced license		75%			
E6	Percent maximum concurrent worker devices		70%			
E7	Number of concurrent guest accounts required		1,000			
E8	Total base device licenses, including BYOD and guest access	E3 * E4 * (1 - E5) * E6	3,938			
E9	Total advanced device licenses	E3 * E4 * E5 * E6 + E7	12,813			
E10	Additional license cost per endpoint device (Base license list price)		$5			
E11	Additional license cost per endpoint device (Advanced + Base license list price)		$30			
Et	**ISE appliance and licensing fees**	**E1 * E2 + E9 * E11 + E8 * E10**	**$542,080**	**$0**	**$0**	**$0**

Source: Forrester Research, Inc.

For *the organization*, these costs totaled nearly $542,000, as shown in Table 7.

Planning, Implementation, And Deployment Costs

The organization incurred internal labor costs for implementation of and planning for ISE, which included one full-time administrator and a part-time consultant for six weeks. Cisco recommends — and will help identify — trained and dedicated professional services resources that can help facilitate a quick and thorough deployment. Cisco also provides guidance and instructions to help speed up deployment and avoid common issues. The labor and professional fees costs for planning, implementation, and deployment cost added up to nearly $53,000 as shown in Table 8.

Annual ISE Administration Costs

To run the Cisco ISE platform, *the organization* allocated

TABLE 8
Planning, Implementation, And Deployment Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Length of implementation (weeks)		6			
F2	Number of company IT admins working on deployment		1			
F3	Admin hours spent per week		40			
F4	Administrator hourly rate		$70			
F5	Number of consultants working on deployment		1			
F6	Consultant hours spent per week		20			
F7	Consultant hourly rate		$300			
Ft	**Planning, implementation and deployment costs**	**F1 * (F2 * F3 * F4 + F5 * F6 * F7)**	**$52,800**	**$0**	**$0**	**$0**

Source: Forrester Research, Inc.

TABLE 9
Annual Administration Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
G1	Number of administrators maintaining ISE			1		
G2	Hours spent per week maintaining ISE			16		
G3	Administrator hourly rate			$70		
Gt	**Annual ISE administration costs**	**G1 * G2 * 52 * G3**	**$0**	**$58,240**	**$58,240**	**$58,240**

Source: Forrester Research, Inc.

TABLE 10
Total Costs (Non-Risk-Adjusted)

Benefit	Initial	Year 1	Year 2	Year 3	Total	Present value
ISE appliance and licensing fees	($542,080)	$0	$0	$0	($542,080)	($542,080)
Planning, implementation and deployment costs	($52,800)	$0	$0	$0	($52,800)	($52,800)
Annual ISE administration costs	$0	($58,240)	($58,240)	($58,240)	($174,720)	($144,834)
Total costs (non-risk-adjusted)	**($594,880)**	**($58,240)**	**($58,240)**	**($58,240)**	**($769,600)**	**($739,714)**

Source: Forrester Research, Inc.

one part-time internal FTE spending about 16 hours per week on Cisco ISE-related management tasks (actually two people, with the total time split roughly equally between them). This adds up to a little less than $60,000 per year in ongoing management costs as shown in Table 9.

Total Costs

As shown in the sections above, costs incurred by the customer include one-time purchase and implementation costs and recurring fees for ongoing support and maintenance. Table 10 shows the total of all costs mentioned above as well as associated present values, discounted at 10%.

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 engage with Cisco ISE and later realize additional benefits and business opportunities; two are outlined here. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix B).

The organization recognizes that there are additional benefits related to BYOD above and beyond management and security time savings. End users themselves may be able to complete tasks faster and feel more comfortable in their job if allowed to use a device they prefer (either because they brought it from home or chose it from a list of provided devices), which could additionally lead to reduced turnover. If turnover was several hundred people per year, but could be reduced by just 50 people per year by implementing a popular BYOD benefit, and if it costs around $20,000 to recruit and train a new employee (industry benchmarks estimate 10% to 20%; higher for highly skilled positions), that would mean as much as an additional $1 million per year in avoided recruiting and training costs.

Other potential flexibility benefits, though not part of *the organization's* plans at this time, are:

- Deployment of Cisco TrustSec, which simplifies the provisioning and management of secure network access policies. Interviewed organizations are not currently using TrustSec, but they recognized that there were additional benefits that could be enabled by adding it, and many were already planning investigation/testing projects. Just in terms of added reductions in device, BYOD, and guest access management, adding TrustSec to *the organization's* solution could result in an additional $100,000 in annual benefits based on an incremental increase in avoided device management and guest services management labor costs.
- Deploying ISE along with an existing mobile device management (MDM) system (or deploying both at the same time) translates the deep mobile device insight of MDM into network access policy via Cisco ISE providing enhanced security for mobile devices.
- Integrating ISE with security information and event management (SIEM) and threat defense can enrich both solutions by sharing more detailed data between the two systems resulting in faster and smarter security.

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 ISE 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 ISE, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

Quantitatively capturing investment and impact risk, by directly adjusting the financial estimates, results in 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 implementation risks that affect costs are identified as part of this analysis:

- Unanticipated costs for deployment or ongoing management such as additional resources or professional services required.
- Unanticipated increase in endpoint licenses required, particularly from increased BYOD and guest access use.

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

- Help desk calls come from a variety of sources and may not be reduced as much as expected.

Additionally, it's worth noting that Cisco ISE, as a security-focused solution, is in part designed to reduce overall business risk. Many of the benefits listed above focus on or are closely related to risk reduction — such as simplifying management and reducing security holes opened by less thorough BYOD and guest access policies. Avoiding potential data breaches is another category — often considered a low "it won't happen to us" risk, but with potentially very high costs if a data breach event occurs. Those risk factors are already covered in the benefit discussion, so are not repeated here.

Table Table 11 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.

TABLE 11
Cost And Benefit Risk Adjustments

Costs	Adjustment
ISE appliance and licensing fees	↑ 5%
Planning, implementation and deployment costs, and annual ISE administration costs	↑ 5%
Benefits	**Adjustment**
Reduced help desk support costs	↓ 5%

Source: Forrester Research, Inc.

Financial Summary

The financial results calculated in the Costs and Benefits sections can be used to determine the ROI, net present value, and payback period for *the organization's* investment in Cisco ISE. These are shown in Table 12.

Table 13 shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 11 in the Risks section to the cost and benefits totals in Table 6 and Table 10.

TABLE 12
Cash Flow: Non-Risk-Adjusted

Cash flow: original estimates

	Initial	Year 1	Year 2	Year 3	Total	Present value
Costs	($594,880)	($58,240)	($58,240)	($58,240)	($769,600)	($739,714)
Benefits	$0	$857,375	$857,375	$857,375	$2,572,125	$2,132,165
Net benefits	($594,880)	$799,135	$799,135	$799,135	$1,802,525	$1,392,450
ROI	188%					
Payback period	9 months					

Source: Forrester Research, Inc.

TABLE 13
Cash Flow: Risk-Adjusted

Cash flow: risk-adjusted estimates

	Initial	Year 1	Year 2	Year 3	Total	Present value
Costs	($594,880)	($61,152)	($61,152)	($61,152)	($778,336)	($746,956)
Benefits	$0	$855,481	$855,481	$855,481	$2,566,444	$2,127,455
Net benefits	($594,880)	$794,329	$794,329	$794,329	$1,788,108	$1,380,499
ROI	185%					
Payback period	9 months					

Source: Forrester Research, Inc.

Cisco Identity Services Engine: Overview

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

Cisco ISE is a unified, policy-based access control enablement platform that helps ensure the corporate and regulatory compliance of network-connected devices. It gathers real-time contextual information from networks, users, and devices, and makes proactive governance decisions by enforcing policy across the network infrastructure. Policy decisions are based on who is trying to access the network, what type of access is requested, where the user is connecting from, when the user is trying to connect, and what device is used. ISE minimizes IT disruption with zero-touch onboarding that allows users to easily self-register their device. Its device-agnostic approach accommodates any personal or IT device type.

A policy-governed unified access infrastructure ensures secure access to data, applications, and systems with high-performance connectivity for every device, and is part of a solution platform that includes other technologies, products and services:

- TrustSec is a security enforcement technology that segments campus and data center networks using plain-language policies. TrustSec helps enable policy networking, managing the rules and business logic for the user and device management listed above. It does this in a role-based way where profiles can be created, and users can be quickly added, removed, or updated efficiently. TrustSec simplifies repetitive and time-consuming network engineering tasks including VLAN, access control list (ACL), and firewall rule engineering and administration. Embedded in Cisco switching, routing, wireless LAN, and firewall products, TrustSec segmentation protects assets, endpoints, and applications in enterprise and data center networks.

Cisco ISE end user licenses come in two levels. All users require the Base license, and some, many or even all users may also require the add-on Advanced license.

- The Base license is intended for organizations that want to authenticate and authorize users and devices on their network (wired, wireless, and virtual private network – or "VPN"). Base licenses include support for authentication, authorization and accounting services, guest lifecycle management, compliance reporting, and end-to-end monitoring and troubleshooting. The Base license is a perpetual license.
- The Advanced license expands upon the Base license and enables organizations to make more advanced policy decisions based on user and device compliance. Advanced license features include device onboarding and provisioning, device profiling, posture services, mobile device management integration capabilities and Security Group Access enforcement capabilities across the entire network (wired, wireless, and VPN). The Advanced license is a subscription-term-based license, with a choice of 3- or 5-year term subscriptions.

For more information, please visit: http://www.cisco.com/en/US/products/ps11640/index.html.

Appendix A: Composite Organization Overview

All of the customers interviewed were using Cisco ISE, which enables inbound and outbound identity management. A composite organization was developed based on information and feedback from the interviewed organizations, while maintaining interviewee confidentiality. The composite organization initially adopted a solution based on Cisco ISE to replace older Cisco NAC servers to better manage and provision guest access. However, finding ISE to be a useful and effective resource for managing and checking devices that access the network, *the organization* quickly expanded its use of Cisco's solutions to include guest access, policy networking, and BYOD support.

The composite organization, referred to as *the organization*:

- Is a Forbes Global 2000 company with global reach but that primarily does business in the United States.
- Is a diversified business that includes direct sales of a broad portfolio of products and services for both B2C and B2B customers.
- Has 10,000 employees that average more than one device per person (e.g., a computer and a phone). Additionally, many have brought personal devices to work, such as personal mobile phones and tablets. They have requested access to work-related resources from them, such as email and documents. More and more of those requests include a desire to connect to LOB systems, such as CRM access for sales reps using their tablet device.
- Has about 100 guests who visit corporate offices each day that request guest wireless access; this can be as high as 1,000 for large events.

Appendix B: 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, risks and flexibility.

BENEFITS

Benefits represent the value delivered to the employee 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 employee 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.

RISKS

Risk measures 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 minimum, three values are calculated to estimate the underlying range around each cost and benefit.

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 in time. However, having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value.

FRAMEWORK ASSUMPTIONS

All figures shown in the case study have been rounded to the nearest whole US dollar.

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

TABLE 14
Model Assumptions

Ref.	Metric	Calculation	Value
H1	Working days per year		260
H2	Working hours per year (M-F, 9-5)		2,080
H3	Security architect salary (fully loaded)		$150,000
H4	Security architect hourly rate	A3/A2	$72
H5	Project manager salary (fully loaded)		$131,250
H6	Project manager hourly rate	A5/A2	$63
H7	Developer salary (fully loaded)		$125,000
H8	Developer hourly rate	A7/A2	$60
H9	Employee salary (fully loaded)		$100,000
H10	Employee hourly rate	A9/A2	$48
H11	Help desk support salary (fully loaded)		$62,500
H12	Help desk support hourly rate	A11/A2	$30

Source: Forrester Research, Inc.

Appendix C: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a 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 organization 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 net present value of cash flows.

Payback period: The breakeven point for an investment. The point in time at which net benefits (benefits minus costs) equal initial investment or cost.

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

A NOTE ON CASH FLOW TABLES

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

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.

Appendix D: Endnotes

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

[2] Cost per record, the amount of records, and likelihood of occurrence data all collected from research conducted by the Ponemon Institute. Source: "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013 (https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf) and "Data Breach Risk Calculator," Ponemon Institute and Symantec (https://databreachcalculator.com/).