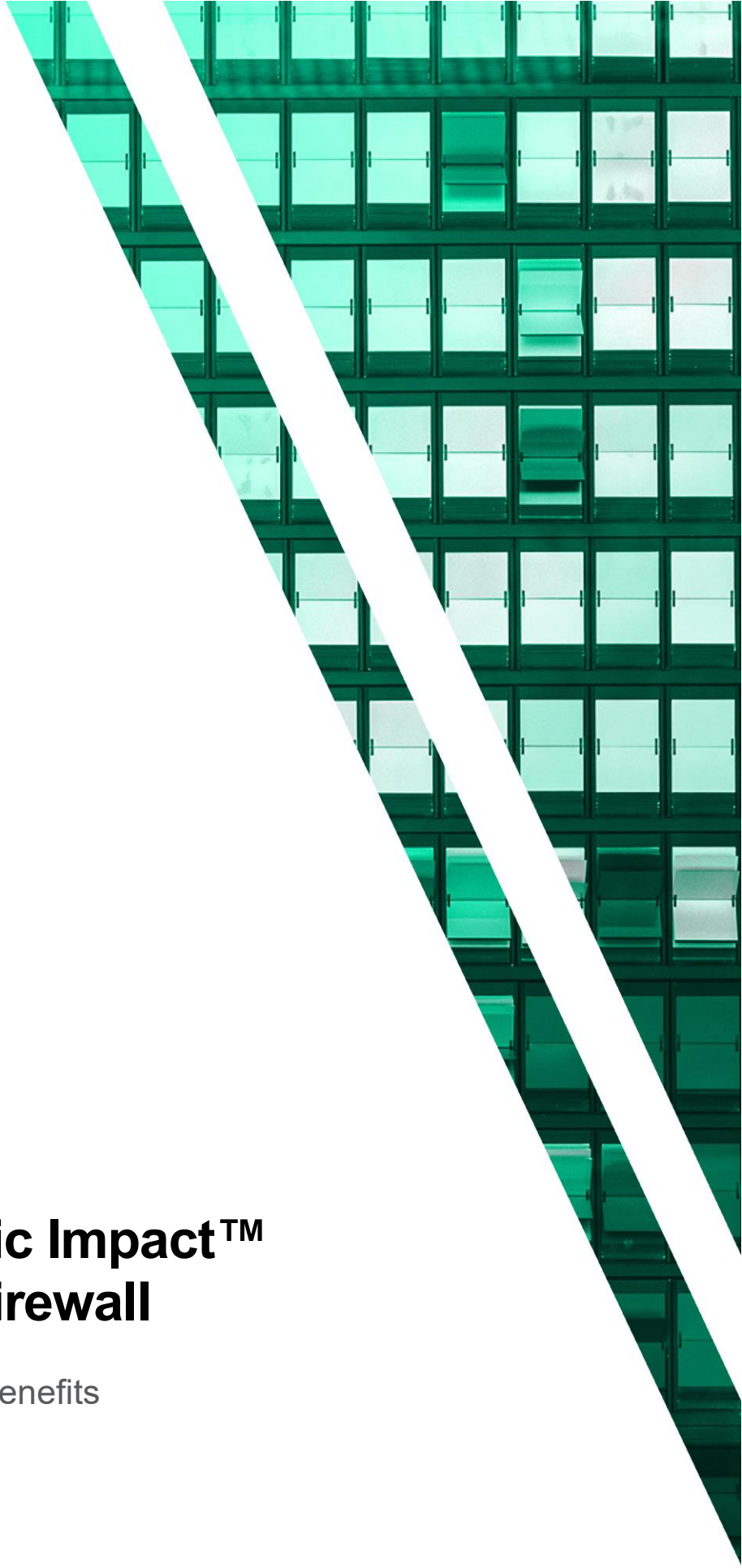
FORRESTER®



# The Total Economic Impact™ Of Cisco Secure Firewall

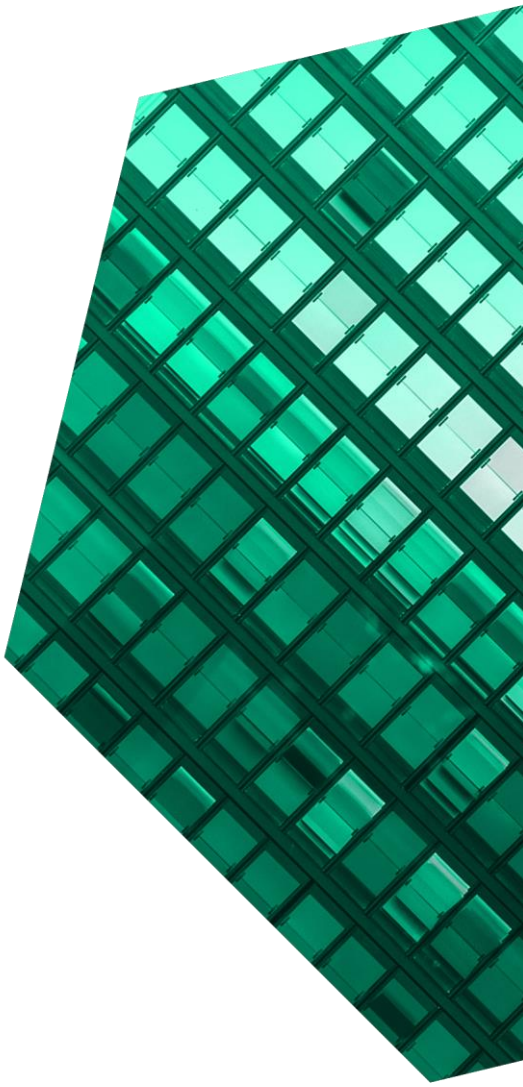
## Cost Savings And Business Benefits Enabled By Secure Firewall

**MARCH 2022**

# Table Of Contents




*Consulting Team: Henry Huang*
*Nick Mayberry*

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

## Executive Summary

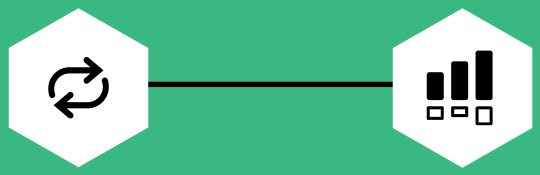
Cisco Secure Firewall and Firewall Management Center improve organizations' visibility and control over their network security. Interviewees' organizations saved up to 95% of firewall-related network professional work and up to 83% of related security professional work. They also reduced the risk of a material breach by up to 80% while improving end-user productivity by minimizing network and VPN disruption. Security posture was improved even while reducing firewall deployments by 25%.

Cisco Secure Firewall is a next-generation, layer 7 network security solution that protects organizations from external and internal threats, while easing the burden on network and security teams for both firewall and threat management. Organizations can manage Cisco Secure Firewall with Firewall Management Center (FMC), a centralized firewall administration and threat defense hub that gives network and security teams added visibility into network activities in a more unified, holistic view, even at the application layer and in threats detected in encrypted traffic. Additionally, it provides increased control with Snort 3 intrusion prevention system (IPS), and software enhancements for URL filtering and malware defense.

Cisco Secure Firewall licensing includes use of SecureX, Cisco's integrated platform that enables organizations to consolidate threat data from the Cisco Secure portfolio and third-party security tools into a single global view of contextually enriched data designed to facilitate rapid investigation and response.

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 Secure Firewall.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Secure Firewall on their organizations.

**KEY STATISTICS**



Return on investment (ROI)
**195%**

Net present value (NPV)
**$12.29M**

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed ten decision-makers across eight organizations with experience using Secure Firewall. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using Secure Firewall, these interviewees noted how their organizations lacked the visibility and manageability they required to adequately administer and effectively secure their networks. Without both this visibility and an efficient graphical user interface (GUI), interviewees noted that network workstreams like firewall deployment, policy creation, firewall upgrades, and policy updates took a significant amount of time. Additional time was also spent on security workstreams such as threat investigation and response and remote access administration. The interviewees also noted poor network performance during periods of high demand and complications from managing multiple vendor solutions.

After the investment in Secure Firewall, the interviewees not only reduced the time it took to accomplish the network and security workstreams mentioned above, but they also enhanced the overall security of their organizations. At the same time, organizations improved employee productivity with faster policy updates, enhanced inspection of network traffic, and improved overall network performance, all while decommissioning legacy solutions and largely eliminating associated management time costs.

Total benefits

**$18.6 million**

**KEY FINDINGS**

**Quantified benefits.** Risk-adjusted present value (PV) quantified benefits include:

- **Reduced network operation workstreams by up to 95%.** Thanks to the latest features of Cisco Secure Firewall and the ease of management via Firewall Management Center, the interviewees' organizations reduced the time to:
  - Deploy a firewall by 36%.
  - Update a firewall by 90%.
  - Update firewall policies by 95%, compared to traditional Adaptive Security Appliances (ASA) 5500-X firewalls.
  - Update firewall policies by 80% compared to early versions of Firewall Threat Defense (FTD)-based policies.
  - Update virtual firewalls by 80%.
- **Reduced security investigation and response workstream times by up to 83%.** Interviewees also noted substantial savings to security professional work from combining Cisco Secure Firewall and Firewall Management Center where information was better organized for consumption and analysis. Interviewees noted reducing the time to investigate potential threats by 49% and the time to respond to threats by 83%. Using SecureX in conjunction with Secure Firewall and FMC enabled organizations to save up to 77% of the remaining time spent on investigation and response.

**"We're very security conscious and want to leverage products to protect our company. That's why we went with Cisco. They grew up in security; for them, it's not just an add-on."**
*Senior network engineer, manufacturing*

- **Reduced risk of breach by up to 80%.** The combined visibility and control provided by Cisco Secure Firewall and Firewall Management Center enabled the interviewees' organizations to reduce the risk of potential material breaches and their associated costs. These solutions reduced the risk of a breach by 80% compared to traditional ASA 5500-X firewalls and by 15% compared to early FTD-based firewalls. SecureX enabled the interviewees' organization to reduce the remaining risk and costs of a breach up to an additional 23%.

- **Improved end-user productivity valued at approximately $2 million annually.** Deploying Cisco Secure Firewall and Firewall Management Center improved the productivity of the interviewees' organizations in two ways. First, it enabled network professionals to fix disruptive policy update errors 80% faster. Second, it reduced the severity of network performance degradation, giving nearly 9 hours of work back annually to each end user impacted.
- **Reduced costs from decommissioned legacy tools.** The interviewees also noted that Cisco Secure Firewall enabled them to decommission the expensive legacy security solutions they had previously implemented. Interviewees noted saving hundreds of thousands of dollars annually on standalone IPS, millions of dollars on avoiding the cost of replacing their existing security solutions, and an additional 25% of costs as Cisco Secure Firewall provided the same level of protection with fewer firewalls.

**Unquantified benefits.** Benefits that are not quantified for this study include:

- **VPN productivity and security enhancements.** Cisco Secure Firewall also enabled better remote-access VPN productivity and security via load balancing, local authentication, and multicertificate authentication. End users established better connections via VPN while the organizations had better control around access.
- **Improved operations for work from home.** Cisco Secure Firewall controls also helped to keep operations running smoothly when VPN use exploded when employees made the transition to working from home. Network professionals could leverage rate limiting and improvements in redundancy to improve employee experience and productivity even at peak demand.
- **Ease of transition to cloud.** Lastly, interviewees shared that Cisco Secure Firewall made their cloud initiatives easier to accomplish, by providing one platform that protected traffic within sites, between sites, and between the organization and multiple cloud platforms. Specifically, Cisco provides standardized policies and validated means of deploying Secure Firewall via cloud-platform marketplaces.

**Costs.** Risk-adjusted PV costs include:

- **Licensing costs.** Although licensing costs were the highest costs the interviewees' organizations incurred, establishing a Cisco Enterprise Agreement saved hundreds of thousands of dollars on additional features and solutions that the organizations lacked before but further enhanced their organization's security posture. SecureX license entitlement is included with Secure Firewall.
- **Costs of implementation, policy creation, and training.** Interviewees noted experiencing internal costs to implement and deploy firewalls and to create policies for them. Firewall deployment is estimated to take 6 hours per site, while policy creation takes an estimated 30 hours. SecureX requires an additional 20 hours of work to implement and 100 hours annually to manage on an ongoing basis. Some interviewees also noted the need to train their network and security professionals to use Cisco Secure Firewall and Firewall Management Center. The internal costs of training amounted to 2 hours of time per employee trained with interviewees noting taking advantage of publicly available training videos featuring Cisco security experts.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $18.59 million over three years versus costs of $6.30 million, adding up to a net present value (NPV) of $12.29 million and an ROI of 195%.

ROI
**195%**

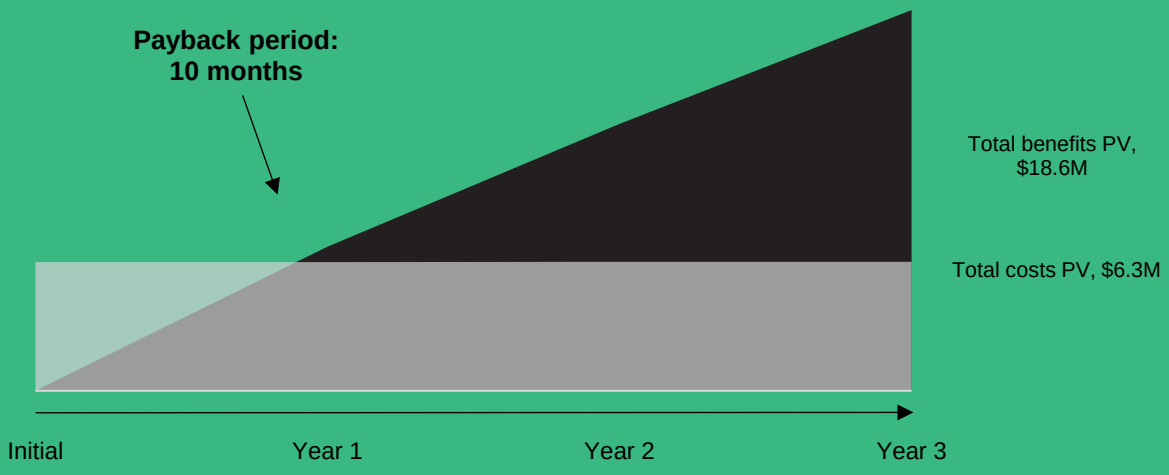
BENEFITS PV
**$18.59M**

NPV
**$12.29M**

PAYBACK
**10 months**

## Benefits (Three-Year)


## Financial Summary



## TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Cisco Secure Firewall.

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 Secure Firewall can have on an organization.

### DUE DILIGENCE

Interviewed Cisco stakeholders and Forrester analysts to gather data relative to Secure Firewall.

### DECISION-MAKER INTERVIEWS

Interviewed ten decision-makers at organizations using Secure Firewall to obtain data with respect to costs, benefits, and risks.

### COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' 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 decision-makers.

### CASE STUDY

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

# The Cisco Secure Firewall Customer Journey

Drivers leading to the Secure Firewall investment

**Interviewed Decision-Makers**

| Interviewee | Industry | Region | Total employees |
|---|---|---|---|
| Engineering services manager | IT services | North America | 750 |
| Lead infrastructure engineer | Financial services | North America | 2,800 |
| Assistant manager of telecom and telephony services | Financial services | North America | 2,800 |
| Principal cybersecurity engineer | Security services | North America | 3,000 |
| Senior network engineer | Manufacturing | Global | 5,500 |
| Senior manager of network engineering | Technology | Global | 40,000 |
| Senior security engineer | Technology | Global | 40,000 |
| Security operations team lead | Education | North America | 46,000 |
| Staff infrastructure architect | Industrial | Global | 205,000 |
| Senior network engineer | Technology | Global | 275,000 |

**KEY CHALLENGES**

Before deploying Cisco Secure Firewall and Firewall Management Center, the interviewees' organizations were largely utilizing traditional ASA 5500-X-based firewall appliances to protect their environments. Some interviewees had made the switch from traditional ASA-based firewalls to early FTD-based firewalls several years ago and noted experiencing additional benefits after upgrading to the latest version of FTD on Cisco Secure Firewall and Firewall Management Center.

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

- **Limited visibility.** The interviewees noted that their prior environments that were reliant on ASA 5500-X-based firewalls provided limited visibility into their overall security. One culprit was a lack of integration. In prior environments, it was difficult for interviewees' organizations to integrate various security solutions to establish unified management and consistent policies, while also getting at one version of the truth. Another reason for limited visibility was that prior environments relied on port inspections as the central viewpoint into the network. Interviewees noted that this prevented them from a deeper look at data with limited visibility into applications and limited historical context.

**"We previously lacked capabilities like modern application control. We couldn't tell how our users were using the network and couldn't respond to this usage adequately."**
*Security operations team lead, education*

- **High time costs to implement and manage firewalls.** The interviewees also noted that deployment and management of their legacy firewalls was time-consuming. Much of this was driven by the lack of ability to push updates to several devices at once. The security operations team lead from the education sector estimated that it used to take as long as 45 minutes to one hour to deploy a simple firewall rule. Additionally, the interviewees noted that their prior environments' lack of visibility meant that they were spending an inordinate amount of time correlating data between different systems to confirm security postures.

**"Ease of administration and integration has been one of the advantages of Cisco. We also benefit from data enrichment as different systems more easily feed each other. We have also established autonomous responses to certain threats. We couldn't do any of this before."**
*Principal cybersecurity engineer, security services*

- **Poor performance.** Interviewees also noted that their prior systems suffered from poor performance. For example, the security operations team lead from the education sector shared that, when demand on their network and security infrastructure skyrocketed, their prior solutions would "fall over, constantly rebooting and dropping packets." This went so far as having an impact to productivity, as "professors utilizing the network to play a video or demonstrate something in class were unable to do so."
- **Vendor management.** Lastly, customers noted that having multiple vendors in their prior environment created vendor management headaches. The lead infrastructure engineer from the financial services firm noted, "With multiple vendors, everything had to be done multiple times, accessing multiple control planes to apply the same changes or updates across the disparate systems."

**COMPOSITE ORGANIZATION**

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas financially affected. The composite organization is representative of the nine decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

**Description of composite.** The composite is a B2B technology organization with $5 billion in annual revenues and 16,000 employees. It serves clients globally. The organization requires high availability at its data centers to ensure consistent client access to their data stored there. These data centers also require heightened security to protect sensitive client data from unwanted access or attack. In addition to the data centers, the organization is moving towards a more distributed approach with the use of multicloud. In addition, the organization is also using Secure Firewalls to protect its edge sites/branch offices.

**Deployment characteristics.** The composite organization has already invested in Cisco next-generation firewalls. Two-thirds of its firewall stock is composed of Cisco Firepower devices, while one-third are composed of ASA 5500-X firewalls. It is now transitioning all its 102 home office, data center, and main office location firewalls to the latest version of Cisco Secure Firewall, updating its 68 Firepower

devices and replacing its 34 ASA-based devices. Some interviewees chose to update existing, traditional devices to FTD software without changing out their hardware. It also deploys Cisco Secure Firewall virtual firewalls in its data centers to handle east-west traffic between the data centers and branch offices, as well as traffic between the data centers and multiple public cloud platforms. It takes advantage of SecureX's inclusion in its Secure Firewall licensing to further enhance its security team's threat investigation and response work.

**Key assumptions**

- **$5 billion in revenues**
- **16,000 employees**
- **Replacing 34 ASA-based firewalls**
- **Updating 68 Firepower firewalls to latest Cisco Secure Firewall**

# Analysis Of Benefits

Quantified benefit data as applied to the composite

| Total Benefits | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Benefit** | **Year 1** | **Year 2** | **Year 3** | **Total** | **Present Value** |
| Atr | Improvements to firewall management | $134,951 | $25,556 | $25,556 | $186,064 | $163,005 |
| Btr | Improvements to security workflows | $2,669,879 | $3,685,484 | $3,685,484 | $10,040,848 | $8,241,976 |
| Ctr | Reduced risk of material breach and productivity loss | $1,291,446 | $1,393,402 | $1,520,848 | $4,205,696 | $3,468,249 |
| Dtr | Performance benefits to employee productivity | $1,656,403 | $1,656,403 | $1,656,403 | $4,969,210 | $4,119,230 |
| Etr | Reduced costs from decommissioned legacy solutions | $1,985,115 | $503,513 | $503,513 | $2,992,142 | $2,599,074 |
| | Total benefits (risk-adjusted) | $7,737,795 | $7,264,360 | $7,391,805 | $22,393,959 | $18,591,534 |

### IMPROVEMENTS TO FIREWALL MANAGEMENT

**Evidence and data.** The interviewed decision-makers noted saving time and costs related to the management of firewalls after deploying Cisco Secure Firewall, regardless of whether they were switching from legacy firewalls or updating from early versions of Firepower Threat Defense. A good portion of these improvements stemmed from the fact that the Firewall Management Center aided networking professionals by providing centralized management of firewalls via a single pane of glass that enabled them to push changes to many devices.

**"FMC gives us one place to manage and upgrade firewalls, instead of hopping around different firewalls as we were doing before."**
*Engineering services manager, IT services*

Interviewees' organizations shared saving time and costs related to firewall deployment. With traditional ASA-based firewalls, the interviewees noted that firewall deployment took a significant amount of time, requiring writing of use case-specific firewall rules and manually distributing those across the diverse set of firewall policies in place.

**"Cisco Secure Firewall enabled us to quickly ramp up and deploy new firewalls. We didn't have to grow employees as we grew firewalls."**
*Senior manager of network engineering, technology*

After switching over to Cisco Secure Firewall and Firewall Management Center, the interviewees noted saving between 30% and 40% of the time deploying firewalls. The reduction in time was attributable to the ability to automate deployment of Cisco Secure

Firewall. For example, the senior manager of network engineering from the technology industry said: "We've automated deployment with Cisco Secure Firewall. We have automation to get the box out, get IP set, set up the chassis, and enforce policy."

**"Built-in automation is saving us the most time. Even around upgrades. I no longer have to sit around and babysit the upgrade process like I had to with ASAs. I can go away, and Firepower lets me know if it doesn't come back online in enough time."**
*Senior manager of network engineering, technology*

Automation also helped the interviewees when it came to managing and maintaining their Cisco Secure Firewalls after deployment. Cisco Secure Firewall comes with automated upgrades built in. The interviewees reported that upgrading ASA-based firewalls could take multiple hours, going from firewall to firewall, uploading update files, and rebooting systems. Using Cisco Secure Firewall and Firewall Management Center, the interviewees reported just clicking through the interface to upgrade the firewalls and then checking back after 30 minutes to see if upgrades were successful.

**"We're seeing 60% to 70% over time savings on policy management after moving from ASA to Cisco Secure Firewall."**
*Engineering services manager, IT services*

With Cisco Secure Firewall and Firewall Management Center, the interviewees noted that policies could be organized into categories and zones without needing long access control lists (ACLs) using an object-oriented system. Policies could also be automatically deployed and updated now, as opposed to manually updating each device.

**"Cisco Secure Firewall autodeploys 90% of the policy for you. We're no longer dealing with one-off configurations."**
*Senior manager of network engineering, technology*

The interviewees noted additional time savings after upgrading from early FTD to late FTD with Cisco Secure Firepower. For example, the lead infrastructure engineer from the financial services sector noted that, with early FTD, policy deployment took between 10 and 15 minutes, but with upgraded FTD deployment times dropped to about 3 minutes.

**"Policy management with Cisco Secure Firewall is straightforward and easy. The Firewall Management Center GUI is light, clean, and intuitive."**
*Senior manager of network engineering, technology*

One of the interviewees was not using Firewall Management Center, but cloud software-as-a-service (SaaS) Cisco Defense Orchestrator (CDO) management. Regarding CDO, the staff infrastructure architect from the industrial sector shared: “Adopting CDO has been painless. Because our engineers were already familiar with [Cisco Security Manager (CSM)], they could already operate the command-line interface and build macros. It was much easier than switching to another vendor where there would have been complexity in having to learn new upper-layer concepts.”

**Modeling and assumptions.** For the composite organization, Forrester models:

- Thirty-four traditional ASA 5500-X firewalls are replaced by Cisco Secure Firewalls.
- The composite organization avoids the 55 hours of labor it would take to deploy and create policies for each replacement traditional firewall.
- The composite avoids 90% of the 30 minutes it used to take each quarter to upgrade each firewall.
- The composite updates a firewall policy on average once a day. By switching to Cisco Secure Firewall, it avoids 95% of the 1 hour it used to take to make each of these updates.
- The average fully burdened hourly rate for a network security operations (NetSecOps) professional is $65.
- Sixty-eight FTD firewalls are upgraded to the latest version of Cisco Secure Firewall. For each daily policy update, the composite saves 80% of the time it takes on early generation FTD firewalls.
- Additionally, the composite saves 80% of the time it used to take to update virtual firewall policies.

**Risks.** Firewall management improvements may vary with:

- The type and number of existing firewalls.
- The number of firewalls replaced with Cisco Secure Firewalls and the rate of this deployment.
- The decision to deploy virtual firewalls at data centers to handle east-west and public-cloud traffic.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of about $163,000.

| Improvements To Firewall Management | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| A1 | Number of next-gen firewalls replacing legacy firewalls | Composite; 1/3 of 102 total | 34 | 0 | 0 |
| A2 | Avoided hours to deploy each firewall | Interviews | 55.00 | 55.00 | 55.00 |
| A3 | Avoided hours to update each ASA firewall | 90%*17 hours quarterly | 61.2 | 61.2 | 61.2 |
| A4 | Avoided hours to manually update policies for ASA firewalls | 95%*1 hour, once daily*33% of environment | 114 | 114 | 114 |
| A5 | Hourly rate for NetSecOps professional | Composite | $65 | $65 | $65 |
| A6 | Subtotal: Reduced time to deploy and upgrade to next-gen firewalls from legacy layer 4 firewalls | ((A1*A2)+(A3+A4))*A5 | $132,938 | $11,388 | $11,388 |
| A7 | Number of updated FTD firewalls | Composite; 2/3 of 102 total | 68 | 68 | 68 |
| A8 | Prior hours to deploy policies with early FTD | Interviews | 0.25 | 0.25 | 0.25 |
| A9 | Reduction in policy deployment time from upgrading to later FTD | Interviews; from 15 minutes to 3 minutes | 80% | 80% | 80% |
| A10 | Subtotal: Reduced time to deploy policies on Firepower from older layer 7 firewalls | 365*A8*A9*A5*A7/102 | $3,163 | $3,163 | $3,163 |
| A11 | Total number of virtual firewalls | Composite | 100 | 100 | 100 |
| A12 | Annual voided hours to update virtual firewall policies | 80%*266 hours annually | 213 | 213 | 213 |
| A13 | Subtotal: Reduced time to manage virtual firewalls | A12*A5 | $13,845 | $13,845 | $13,845 |
| At | Improvements to firewall management | A6+A10+A13 | $149,946 | $28,396 | $28,396 |
| | Risk adjustment | ↓10% | | | |
| Atr | Improvements to firewall management (risk-adjusted) | | $134,951 | $25,556 | $25,556 |
| | **Three-year total: $186,064** | | | **Three-year present value: $163,005** | |

### IMPROVEMENTS TO SECURITY WORKFLOWS

**Evidence and data.** Deploying Cisco Secure Firewall and utilizing FMC also helped the interviewees streamline security workflows. The decision-makers noted that ASA-based devices required multiple, separate tools to track and log events across firewalls. With FMC, Cisco Secure Firewall data was consolidated into one place where indicators of compromise (IOC) and blocked intrusions could be tracked or up-leveled coherently to a security information and event management (SIEM) solution.

With FMC, interviewees gained the ability to review connections, events, and telemetry as a whole in a more correlated manner across the entire network.

> **"Security investigations used to feel like building a puzzle with only one piece."**
> *Security operations team lead, education*

With consolidation via Firewall Management Center, the interviewees reported reducing the time costs of security investigation work. For example, the principal cybersecurity engineer from the security services industry noted reduced time to investigate from hours down to 3 to 5 minutes with help from Secure Firewall and Firewall Management Center. Before, this interviewee noted having to go through multiple systems including a SIEM and an e-mail console, logging in and coordinating data. Now, they can log into FMC and look for specific IOCs in that environment.

**"Firewall Management Center acts as a single console to manage all Cisco Secure Firewalls. It eases administration, and saves time to investigate and collate events, and on making decisions regarding malicious activity."**
*Engineering services manager, IT*

Interviewees also noted a reduction to their response times as well. For example, the security operations team lead from the education industry reported having to send tickets to client support multiple times a week before investing in Cisco Secure Firewall. Support would then track down the user and run malware testing, which could take hours to scan. Then the interviewee's team would clean the system or even reimage it. This process could take up to a full day. With Cisco Secure Firewall, this interviewee sends a similar ticket once a month and they go straight into FMC to resolve the issue, taking about one hour.

**"Our legacy firewalls required a lot of overhead to run security incident response; it took a lot of time and cost a lot of money. With Firepower, we're seeing massive time savings and doing way less incident response as more is blocked."**
*Security operations team lead, education*

Interviewees moving from an early version of FTD to an updated version also experienced benefits related to security investigation and response workflows. As the lead infrastructure engineer from the financial services sector reported, an earlier version of FTD still allowed for an aggregate view of security alerts via Firewall Management Center but after upgrading, definitions and trigger capabilities improved. This interviewee also noted that the further integrations with Cisco products, including AMP and Umbrella, provided even more benefits from additional correlation.

**"FMC gives us great visibility. Now, with this visibility, we spend more time looking and making sure everything is ok. But we're still spending less time than we used to on incident response."**
*Security operations team lead, education*

Those organizations that took advantage of SecureX's inclusion in their Secure Firewall licensing further improved their security teams' operational efficiency through visibility and customization. For example, the security operations team lead from the education sector also noted that SecureX allowed for personalized, customizable dashboards, so that their team was not only getting additional visibility into the environment but also showing different users the most important information for their responsibilities.

**Modeling and assumptions.** For the composite organization, Forrester models:

- Total annual security alerts of 100,000.
- Twenty-six percent of these require security analyst attention.
- Seventy percent of the alerts requiring attention require investigation as well.
- Cisco Secure Firewall and Firewall Management Center save 49% of the 2.8 hours it used to take to investigate alerts.
- Ten percent of alerts requiring investigation require response.
- Cisco Secure Firewall and Firewall Management Center save 83% of the 6 hours it used to take to respond.
- SecureX enables additional time savings to investigation and response workflows of 42% in Year 1 and 77% in Years 2 and 3.

**Risks.** The improvement to security workflows may vary with:

- The number of annual alerts, alerts requiring attention, alerts requiring investigation, and alerts requiring response.
- The fully burdened hourly rate of NetSecOps professionals.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of over $8.2 million.

| Improvements To Security Workflows | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| B1 | Total annual alerts | Composite | 100,000 | 100,000 | 100,000 |
| B2 | Alerts requiring analyst attention | Forrester research; 26% | 26,000 | 26,000 | 26,000 |
| B3 | Percentage of alerts requiring investigation | Interviews | 70% | 70% | 70% |
| B4 | Prior average hours to investigate | Interviews | 2.8 | 2.8 | 2.8 |
| B5 | Reduction in time to investigate from FMC | Interviews | 49% | 49% | 49% |
| B6 | Alerts requiring response | Interviews | 260 | 260 | 260 |
| B7 | Prior average hours to respond | Interviews | 6 | 6 | 6 |
| B8 | Reduction in time to respond from FMC | Interviews | 83% | 83% | 83% |
| B9 | Additional reduction to investigation and response from SecureX | Interviews | 42% | 77% | 77% |
| B10 | Fully burdened hourly rate of security professional | A5 | $65 | $65 | $65 |
| Bt | Improvements to security workflows | ((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10 | $3,141,034 | $4,335,864 | $4,335,864 |
| | Risk adjustment | ↓15% | | | |
| Btr | Improvements to security workflows (risk-adjusted) | | $2,669,879 | $3,685,484 | $3,685,484 |
| **Three-year total: $10,040,848** | | | **Three-year present value: $8,241,976** | | |

### REDUCED RISK OF MATERIAL BREACH AND PRODUCTIVITY LOSS

**Evidence and data.** The interviewees also reported experiencing financial benefits associated with reducing the risk of a material breach and the associated productivity costs after deploying Cisco Secure Firewall.

One means by which interviewees' organizations' security posture improved was from the added visibility that Cisco Secure Firewall and Firewall Management Center provided. For example, the security operations team lead from the education sector noted: "Compared to traditional ASAs, Cisco Secure Firewall gives us better visibility. This is especially important as users are bringing a growing number of mobile devices onto our network and

**"We've seen a vast improvement in the number of threats and IOCs blocked. It's orders of magnitude difference. Before, our business was at risk every day we didn't run Secure Firewall. We now have added visibility, and risks have immeasurably reduced. We feel comfortable now."**
*Engineering services manager, IT services*

accessing services like printing via the network. Upgrading to Firepower gives us better visibility and the ability to filter internal network traffic as well as north-south traffic."

Improved automated blocking also assisted in reducing the potential risk of a successful breach. The senior manager of network engineering from the technology sector noted: "Firepower is an industry leader in [intrusion protection systems (IPS)]. We were able to increase our security posture and remediate issues right out of the gate. For every potential incident we remediate early, we save money." This same customer reported an 80% improvement in blocking when moving from an ASA-based system to Cisco Secure Firewall.

**"With Secure Firewall, we eliminated 80% of our threats right away without the need for any additional headcount."**
*Senior manager of network engineering, technology*

Importantly, the interviewees also noted improved blocking by updating their FTD firewalls to the latest versions. The senior network engineer from the technology firm shared that upgrading to the latest version of FTD enabled between 10% and 15% more automated blocking than earlier versions.

This same interviewee also shared an anecdote about the impact automated blocking could have: "We once had a potential compromise based on social engineering where a hacker was able to get a 24-hour access token from an authenticated user. When the hacker tried to use [the token], Cisco Secure Firewalls saved us. We were able to check the posture and verify if the attacker was using a corporate machine. Secure Firewall automatically denied the hacker VPN access. Without this, the hacker would have gotten access to our corporate network, and I'm not sure badly how that could have impacted us."

**"Cisco Secure Firewall is a one-stop shop. It has all the integration capabilities with other tools to provide relevant data to help security. It has different flavors; we can address different throughput requirements, and it supports both vertical and horizontal scaling. It has all the functionality that is needed to address today's security risks, and it's continuously improving."**
*Senior network engineer, internet*

The senior network engineer from the technology firm also noted a security benefit that Secure Firewall provides by being able to manage access at the application level: "We were seeing huge use of BitTorrent on our guest network. By leveraging FTD to block BitTorrent, we are not only preventing potential threats to other guests, but also brought down circuit utilization by about 400 Mbps."

In addition to application-layer detection and blocking, interviewees noted Cisco Secure Firewall's use of Snort-based automated threat feeds also reduced their organizations' risk of a successful material breach. The lead infrastructure engineer from financial services said, "We wanted Cisco Secure Firewall for the added visibility and the automated response from Snort, looking for things

like unpatched servers exposed to the internet and holistically blocking malicious traffic."

Those organizations that took advantage of SecureX's inclusion in their Secure Firewall licensing further reduced the risk and cost of material breaches. For example, the lead infrastructure engineer from the financial services organization noted that SecureX enabled them to get even more visibility into identifying security issues and identifying the root cause of potential threats.

**"SecureX can give us a single view of our entire security environment. With FMC, we get a view into all our firewalls, with SecureX we get a view into FMC as well as all of our integration Cisco security solutions."**
*Security operations team lead, education*

**Modeling and assumptions.** For the composite organization, Forrester models:

- A prior number of annual material security breaches of three.
- The average combined internal and external costs of a material breach is $968,480.
- The percentage of external attacks, internal incidents, and attacks/incidents involving partners and third parties is 79%.
- Cisco Secure Firewall and Firewall Management Center reduce the risk of a breach by 80% for the percentage of the organization previously covered by traditional ASA firewalls.
- Cisco Secure Firewall and Firewall Management Center reduce the risk of a breach by 15% for the percentage of the organization previously covered by FTD-based firewalls.
- Sixty-six percent of the composite organization's employees are impacted by each breach, regaining 70% of their productivity thanks to Cisco Secure Firewall and Firewall Management Center's reduction in breach risk.
- A fully burdened hourly rate for general employees of $40.

**Risks.** The reduced risk of a material breach may vary with:

- The number of annual material breaches currently experienced.
- The total internal and external costs of a material breach.
- The percentage of external attacks, internal incidents, and attacks/incidents involving partners and third parties.
- The type and number of existing firewalls.
- The number of employees impacted by a material breach, their fully burdened hourly rate, and their ability to recoup productivity when these material breaches are reduced.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of nearly $3.5 million.

| Reduced Risk Of Material Breach And Productivity Loss | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| C1 | Average number of material breaches | Forester research | 3 | 3 | 3 |
| C2 | Average cost per material breach | Forrester research | $968,480 | $968,480 | $968,480 |
| C3 | Percentage of external attacks, internal incidents, and attacks/incidents involving partners and third parties | Interviews | 79% | 79% | 79% |
| C4 | Percentage of organization moving from ASA to Firepower | Composite | 33% | 33% | 33% |
| C5 | Percentage risk reduction from Firepower | Interviews | 80% | 80% | 80% |
| C6 | Percentage of organization moving from early Firepower to upgraded Firepower | Composite | 67% | 67% | 67% |
| C7 | Percentage risk reduction from upgraded Firepower | Interviews | 15% | 15% | 15% |
| C8 | Additional reduction from SecureX | Interviews | 14% | 18% | 23% |
| C9 | Subtotal: Reduced risk of breach | (C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8) | $1,162,951 | $1,254,763 | $1,369,528 |
| C10 | Number of users impacted by each breach | Forrester research | 10,600 | 10,600 | 10,600 |
| C11 | Average fully burdened hourly rate of general employee | Composite | $40 | $40 | $40 |
| C12 | Productivity rate capture | Composite | 70% | 70% | 70% |
| C13 | Subtotal: Improved productivity from reduced risk of breach | (C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8 | $356,397 | $384,534 | $419,705 |
| Ct | Reduced risk of material breach and productivity loss | C9+C13 | $1,519,348 | $1,639,297 | $1,789,232 |
| | Risk adjustment | ↓15% | | | |
| Ctr | Reduced risk of material breach and productivity loss (risk-adjusted) | | $1,291,446 | $1,393,402 | $1,520,848 |
| | **Three-year total: $4,205,696** | | | **Three-year present value: $3,468,249** | |

## PERFORMANCE BENEFITS TO EMPLOYEE PRODUCTIVITY

**Evidence and data.** Cisco Secure Firewall enabled the interviewees' organizations to improve employee productivity broadly by two means: 1) providing application level visibility and control that enhanced network performance and 2) limiting downtime fallout from policy updates.

Interviewees noted that their network performance degraded less often after implementing Cisco Secure Firewall thanks to its ability to control network access at the application layer. Before, customers reported that their networks frequently slowed and performance degraded to the point of impacting employee productivity when there was high demand from specific applications, especially those related to video media. The security operations team lead from the education sector shared: "Although the network notably slowed daily, the degradation was so bad it impacted productivity once every couple of weeks. This mostly happened when we had a burst in activity, such as thousands of users watching a video."

As Cisco Secure Firewall enabled interviewees' organizations to set network security policy at multiple layers, including the application layer, interviewees had more granular control over network permissions. As a result, these firms could better control which and when certain applications could access their networks, preventing network overload from high-bandwidth applications, improving network performance, and increasing the productivity of their employees.

**"Cisco Secure Firewall gives us much better visibility into how the network is being used and the ability to control this use. We currently have 4,000 different systems monitored, so if I wanted, I could see how much [a popular video-based social app] was used last week. We could right rules to disallow this type of traffic if need be."**
*Security operations team lead, education*

Other interviewees noted that their firms boosted employee productivity by limiting the negative impact that human errors in policy updates sometimes created. For example, the engineering services manager from the IT services firm noted that, because policies could be created and updated much faster with Firewall Management Center, they also received feedback on whether updates were successful faster.

Before this firm implemented Secure Firewall, it would take 15 minutes to update a policy and an additional 15 minutes to know if it was set correctly. If not, it would take another 15 minutes out and back to update the policy a second time. On occasion, an erroneously updated policy would have a negative impact on employee productivity, especially in production environments.

After upgrading to the latest version of FTD with Cisco Secure Firewall, the engineering services manager noted reducing the time for policy updates and feedback to 3 minutes out and 3 minutes back in reduced the total time for updating, feedback, and troubleshooting by 80% from 60 minutes to 12 minutes.

**Modeling and assumptions.** For the composite organization, Forrester models:

- It takes a full hour to fix an erroneously updated policy (15 minutes to send the erroneous update, 15 minutes to receive feedback, and 30 minutes to update and receive feedback once fixed).
- Cisco Secure Firewall and Firewall Management Center reduce the time it takes to fix erroneous policies by 80%.
- An assumed 2% of the organization on average is impacted by erroneous policy updates.
- The network used to incur serious degradation that impacted employee productivity for 20 minutes approximately once every two weeks.
- Thirty-three percent of employees that traditional ASA firewalls used to cover were impacted by network degradation.

**Risks.** The performance benefits to employee productivity may vary with:

- The percentage of employees impacted by erroneous policy updates.
- The frequency and length of network degradation impacting employee productivity.
- The number of employees impacted by network degradation.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of over $4.1 million.

**Performance Benefits To Employee Productivity**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| D1 | Prior hours to adjust policies with early FTD | Interviews | 1 | 1 | 1 |
| D2 | New hours to adjust policies with updated FTD | Interviews | 0.2 | 0.2 | 0.2 |
| D3 | Average employees impacted | Composite | 320 | 320 | 320 |
| D4 | Average fully burdened hourly rate of general employee | C10 | $40 | $40 | $40 |
| D5 | Productivity recapture rate | Composite | 25% | 25% | 25% |
| D6 | Subtotal: Improved productivity from earlier policy feedback | 365*(D1-D2)*D3*D4*D5 | $934,400 | $934,400 | $934,400 |
| D7 | Frequency of performance degradation from network usage abuse | Interviews | 26 | 26 | 26 |
| D8 | Average length of performance degradation in hours | Interviews | 0.33 | 0.33 | 0.33 |
| D9 | Number of employees impacted (ASA migrations only) | Composite | 5,280 | 5,280 | 5,280 |
| D10 | Average fully burdened hourly rate of general employee | C11 | $40 | $40 | $40 |
| D11 | Productivity recapture rate | Composite | 50% | 50% | 50% |
| D12 | Subtotal: Improved productivity of end-user employees | D7*D8*D9*D10*D11 | $906,048 | $906,048 | $906,048 |
| Dt | Performance benefits to employee productivity | D6+D12 | $1,840,448 | $1,840,448 | $1,840,448 |
| | Risk adjustment | ↓10% | | | |
| Dtr | Performance benefits to employee productivity (risk-adjusted) | | $1,656,403 | $1,656,403 | $1,656,403 |
| | **Three-year total: $4,969,210** | | | **Three-year present value: $4,119,230** | |

### REDUCED AND AVOIDED COSTS OF PRIOR SOLUTIONS

**Evidence and data.** By migrating their network security infrastructure to the latest version of Cisco Secure Firewall, the interviewees' organizations reduced and avoided costs associated with their legacy network infrastructure. Not surprisingly, the interviewees reported avoiding costs on relicensing their traditional ASA-based firewalls, as well as any early FTD-based firewalls, as Cisco Secure Firewalls replaced these.

In addition to the physical and virtual firewall replacements, interviewees' organizations switching from ASA-based environments decommissioned their standalone IPS solutions as Cisco Secure Firewall includes IPS.

**“With traditional ASA firewalls, we also needed to invest in IPS units to place between the links and the firewall. With Cisco Secure Firewall, IPS is built in. We’re no longer managing two different solutions with two different ecosystems, and we’re not relying on IPS engineers.”**
*Senior manager of network engineering, technology*

Importantly, interviewees noted additional savings when upgrading their organizations’ firewalls from early FTD to Cisco Secure Firewall. Because of the efficiency of these latest firewalls, interviewees reported needing between 20% and 25% less of them to achieve the same results.

**“Shifting from early FTD to the latest FTD on Cisco Secure Firewall, we saw better processing efficiency. Cisco Secure Firewall is somewhere between 20% and 25% more efficient than earlier iterations, meaning we need fewer firewalls.”**
*Senior network engineer, internet*

**Modeling and assumptions.** For the composite organization, Forrester models:

- A reduction in standalone IPS licensing costs from replacing traditional ASA firewalls with Cisco Secure Firewalls of $171,600 annually.
- Avoided maintenance fees for standalone IPS equivalent to 20% of licensing fees.
- A reduction of ongoing management costs related to IPS of 80% of 30 minutes for 2 FTEs weekly.
- Avoided costs to replace existing firewalls with those of a similar type of over $1.3 million in Year 1.
- Avoided costs to replace virtual firewalls of $300,000 annually.
- Avoided costs of an additional 25% of physical firewalls thanks to the efficiency of Cisco Secure Firewalls.

**“We finally retired our costlier and less performant IPS appliances when deploying Cisco Secure Firewall.”**
*Lead infrastructure engineer, financial services*

**Risks.** The reduction in legacy solution costs will vary with:

- The number and type of existing firewalls.
- The ability to decommission standalone IPS solutions.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of nearly $2.6 million.

**Reduced Costs From Decommissioned Legacy Solutions**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| E1 | Reduced cost of legacy IPS | Interviews | $171,600 | $171,600 | $171,600 |
| E2 | Reduced cost of maintenance fees | E1*20% | $34,320 | $34,320 | $34,320 |
| E3 | Reduced cost of legacy IPS ongoing management | Interviews | $53,539 | $53,539 | $53,539 |
| E4 | Avoided cost of firewalls for replacement cycle | Composite | $1,616,980 | $300,000 | $300,000 |
| E5 | Avoided costs from additional firewall efficiency | Composite | $329,245 | $0 | $0 |
| Et | Reduced costs from decommissioned legacy solutions | E1+E2+E3+E4+E5 | $2,205,684 | $559,459 | $559,459 |
| | Risk adjustment | ↓10% | | | |
| Etr | Reduced costs from decommissioned legacy solutions (risk-adjusted) | | $1,985,115 | $503,513 | $503,513 |
| | **Three-year total: $2,992,142** | | | **Three-year present value: $2,599,074** | |

### UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **VPN productivity and security enhancements.** Interviewees also noted that Cisco Secure Firewall enabled better remote-access VPN productivity and security. With load balancing, Secure Firewall distributed sessions among grouped devices, providing performance, resiliency, and end-user productivity. Similarly, local authentication with Secure Firewall enabled users to remain productive if a remote AAA server became inaccessible. For security, Cisco Secure Firewall enables multicertificate authentication, so organizations can ensure a remote device is corporate issued, in addition to validating the end user themselves.
- **Improved compliance.** The interviewees also shared that Cisco Secure Firewall and Firewall Management Center provided an unquantifiable benefit to compliance workflows. The lead infrastructure engineer from the financial services firm shared that, before deploying Secure Firewall and FMC, reporting on compliance was more difficult. Prior solutions lacked an easy reporting function. However, Secure Firewall and FMC enabled their organization to run reports that were more encompassing of components and more detailed as to activities and views. Interviewees also mentioned that Cisco Secure Firewall supports the transport layer security (TLS) 1.3 encryption standard. For example, the senior network engineer from the internet firm noted that their team was not currently decrypting such flows due to the administrative burden. After investing in Cisco Secure Firewall, TLS 1.3 decryption became easier and more efficient.

**"Before, we didn't have reporting output for a lot of the different configuration components, but now we can get wide-ranging and detailed reports more easily. For example, I just got a report of every access control change that I have made for the last year. It shows the output of all the page views and the changes that were made."**
*Lead infrastructure engineer, financials services*

- Improved **employee experience.** Interviewees also noted that their organizations' employee experience improved. For example, the senior network engineer from the internet firm said: "Being able to better control application access on our networks has improved employee satisfaction. Our local IT teams used to have a difficult time tracking down users to ask them to stop using particular apps or to block them from access. With Secure Firewall and FMC, we can just do that remotely now."

**FLEXIBILITY**

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

- **Additional Cisco Security integrations.** In addition to the benefits of SecureX, the interviewees noted that Cisco's ecosystem of security offerings provided flexibility to further bolster their organizational security postures. For example, the engineering services manager from the IT services firm shared: "Cisco Security has a deep stack of integrated security solutions, which is something other vendors struggle with. It's not just Secure Firewall, it's all those other pieces that integrate well together and allow us to better build our defenses."
- **Improved operations for work from home.** Cisco Secure Firewall controls also helped to keep operations running smoothly when VPN use exploded when employees made the transition to working from home. The senior network engineer from the internet firm noted, "During the pandemic our simultaneous VPN connections increased from an average of 100,000 to close to 350,000 globally. In order to maintain viability of our network, we used Cisco Secure Firewall to set rate limits, smoothing operations."
- **Ease of transition to cloud.** Lastly, interviewees shared that Cisco Secure Firewall made their cloud initiatives easier to accomplish. The engineering services manager from the IT services organization said, "We needed a single platform to reach on-site, remote sites, and also for the cloud, but it had to be easy to deploy. Well, with cloud platforms, you can just drop a FTD box, install it right there and then and connect it into Firewall Management Center. It took no time at all to get set up and deployed. And we could push a standardized policy out to those boxes."

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

# Analysis Of Costs

Quantified cost data as applied to the composite

| Total Costs | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ref.** | **Cost** | **Initial** | **Year 1** | **Year 2** | **Year 3** | **Total** | **Present Value** |
| Ftr | Licensing costs | $6,000,690 | $0 | $0 | $0 | $6,000,690 | $6,000,690 |
| Gtr | Costs of implementation, policy creation, and training | $278,220 | $7,924 | $7,924 | $7,924 | $301,990 | $297,924 |
| | Total costs (risk-adjusted) | $6,278,910 | $7,924 | $7,924 | $7,924 | $6,302,680 | $6,298,614 |

### LICENSING COSTS

**Evidence and data.** Customers shared incurring several different costs associated with their Secure Firewall investment, including:

- Physical firewall costs, which varied depending on required throughput.
- Virtual firewalls deployed to the data center or data centers to handle east-west traffic.
- Costs of Threat Protection, Malware Defense, and URL filtering licenses.
- Firewall Management Center licenses.

**"We struggled to find any other option with the depth of architecture, toolset, and features that Cisco Secure Firewall has all in one box. But adding to that, the price-to-performance ratio was also compelling."**
*Lead infrastructure engineer, financials services*

Customers noted that they were able to deploy Cisco SecureX based at no extra cost as it was included in their Secure Firewall licenses.

**Modeling and assumptions.** For the composite organization, with 100 offices and four physical data centers requiring redundancy, Forrester models:

- All licenses at list price for a term of three years.
- The cost of a firewall for the corporate office is $328,443. The corporate office requires a large, enterprise-class firewall, with throughput of up to 75 Gbps.
- The cost of data center firewalls is $978,067. At each ach data center, the composite deploys a data-center perimeter clustering or high availability bundle of two physical firewalls to handle north-south traffic into and out of the data center.
- The cost of 100 virtual firewalls is $2,628,561. These virtual firewalls handle the east-west traffic within the data centers and also between the data centers and public cloud platforms.
- The physical and virtual firewalls at the data centers all have an additional Threat Protection license at a three-year subscription rate. This provides additional security, including Snort 3 to

better detect and mitigate indicators of compromise and malicious traffic.

- The total cost of 60 branch firewalls is $1,848,160. Sixty offices require Secure Firewalls with throughput of up to 1.9 Gbps.
- The total cost of 39 small-branch firewalls of is $137,779. The 39 remaining offices only required throughput of up to 650 Mbps.
- All office firewalls have additional Threat Protection, Malware Defense, and URL filtering licenses at a three-year subscription rate.
- Firewall Management Center is also licensed at a size appropriately to handle all of these firewalls. The cost of Firewall Management Center is $79,680.

**Risks.** The licensing costs of Cisco Secure Firewall and Firewall Management Center will vary with:

- The number of virtual firewalls desired.
- The number of enterprise-grade firewalls needed.
- The size and number of data centers and need for high availability.
- The size and number of branch offices.

**Results.** As Forrester priced the composite organization directly with Cisco, we have not adjusted this cost for risk, yielding a three-year total PV (discounted at 10%) of $6 million.

**“With our Cisco enterprise security agreement, our total cost is cheaper than everything would be a la carte. Although Firepower is the bulk of that cost, we’re saving hundreds of thousands of dollars getting additional protection with products we didn’t have before.”**
*Security operations team lead, education*

## Licensing Costs

| Ref. | Metric | Source | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| F1 | Cost of virtual firewalls | Cisco | $2,628,561 | | | |
| F2 | Cost of corporate office firewall | Cisco | $328,443 | | | |
| F3 | Cost of data center physical firewalls | Cisco | $978,067 | | | |
| F4 | Cost of small branch office firewalls | Cisco | $137,779 | | | |
| F5 | Cost of large branch office firewalls | Cisco | $1,848,160 | | | |
| F6 | Cost of Firewall Management Center | Cisco | $79,680 | | | |
| Ft | Licensing costs | F1+F2+F3+F4+F5+F6 | $6,000,690 | $0 | $0 | $0 |
| | Risk adjustment | 0% | | | | |
| Ftr | Licensing costs (risk-adjusted) | | $6,000,690 | $0 | $0 | $0 |
| | **Three-year total: $6,000,690** | | | **Three-year present value: $6,000,690** | | |

### COSTS OF IMPLEMENTATION, POLICY CREATION, AND TRAINING

**Evidence and data.** The interviewees shared experiencing internal time and labor costs associated with deploying and implementing firewalls across their data centers and offices. The first of these costs involved physically deploying the firewalls at each site. The second involved implementing these firewalls by creating and deploying the appropriate policies across each set of firewalls.

**"Implementation and deployment were really quick and relatively simple. The actual switchover took three weeks, as we already had a design in place and knew how to turn everything on."**
*Security operations team lead, education*

Lastly, the interviewed decision-makers also noted experiencing time costs related to training. Training took about 2 hours for any employee needing such training to deploy and manage Cisco Secure Firewalls. Some interviewees noted taking advantage of publicly available training videos featuring Cisco security experts.

**Modeling and assumptions.** For the composite organization, Forrester models:

- On average, 6 hours of implementation time is required at each of two data centers and 100 offices.
- On average, policy creation takes 30 hours per firewall.
- SecureX requires 20 hours of work to implement upfront and an additional 100 hours annually to manage on an ongoing basis.
- Fifteen employees needing training initially with three additional employee needing training each year due to employee turnover.

**Risks.** The cost of implementation and policy creation will vary with:

- The number of Cisco Secure Firewalls to be deployed.
- The number of employees needing to be trained initially.
- The rate of employee turnover.
- The fully burdened hourly rate of NetSecOps professionals.

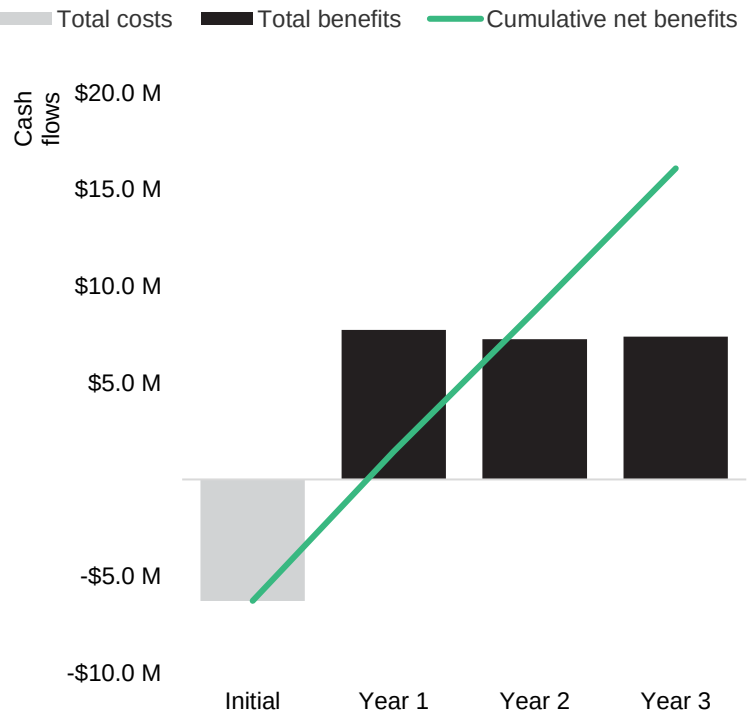
**Results.** To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of under $298,000.

| Costs Of Implementation, Policy Creation, And Training | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| G1 | Sites to deploy | Composite | 102 | | | |
| G2 | Average hours for physical implementation at each site | Composite | 6 | | | |
| G3 | Hours for policy creation | Interviews | 30 | | | |
| G4 | Hours for SecureX implementation and management | Interviews | 20 | 100 | 100 | 100 |
| G5 | Employees needing training | Interviews | 15 | 3 | 3 | 3 |
| G6 | Hours needed for training | Interviews | 2 | 2 | 2 | 2 |
| G7 | Average fully burdened rate of NetSecOps professional | A5 | $65 | $65 | $65 | $65 |
| Gt | Costs of implementation, policy creation, and training | ((G1*(G2+G3))+,G4+(G5*G6))*G7 | $241,930 | $6,890 | $6,890 | $6,890 |
| | Risk adjustment | ↑15% | | | | |
| Gtr | Costs of implementation, policy creation, and training (risk-adjusted) | | $278,220 | $7,924 | $7,924 | $7,924 |
| **Three-year total: $301,990** | | | **Three-year present value: $297,924** | | | |

# Financial Summary

## CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

### Cash Flow Chart (Risk-Adjusted)




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

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

**Cash Flow Analysis (Risk-Adjusted Estimates)**

| | Initial | Year 1 | Year 2 | Year 3 | Total | Present Value |
|---|---|---|---|---|---|---|
| Total costs | ($6,278,910) | ($7,924) | ($7,924) | ($7,924) | ($6,302,680) | ($6,298,614) |
| Total benefits | $0 | $7,737,795 | $7,264,360 | $7,391,805 | $22,393,959 | $18,591,534 |
| Net benefits | ($6,278,910) | $7,729,871 | $7,256,436 | $7,383,881 | $16,091,279 | $12,292,920 |
| ROI | | | | | | 195% |
| Payback period (months) | | | | | | 10 |

# 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] 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.


FORRESTER®