

Cisco Secure Firewall, Firewall Management Center, and SecureX collaborate to provide superior visibility, protection, and management efficiency

Cisco Secure Firewall is a next-generation, layer 7 network security solution that protects organizations' networks from external and internal threats, while easing the burden on network and security teams regarding 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. Cisco Secure Firewall licensing includes use of SecureX, Cisco's integrated platform that enables organizations to consolidate threat data from Cisco Secure and third-party security tools into a single global view of contextually enriched data designed to facilitate rapid investigation and response.

To better understand the benefits, costs, and risks associated with the combination of Cisco Secure Firewall, Firewall Management Center, and SecureX, Cisco commissioned Forrester Consulting to interview ten decision-makers across eight organizations and conduct a Total Economic Impact™ (TEI) study.¹

This abstract will focus on the use of Cisco SecureX in conjunction with Secure Firewall and Firewall Management Center and its value to the six organizations that used the three solutions.



Return on investment (ROI)
195%



Net present value (NPV)
\$12.29M

INVESTMENT DRIVERS

The interviewed decision-makers shared common reasons for seeking out a Cisco Secure Firewall investment, including:

- **Unified management and policy consistency.** The interviewee's sought to gain better visibility and control over security policies via the integration of various security tools. They looked for a solution that could establish unified management and consistent policies, providing a single source of truth for their security teams.



READ THE FULL STUDY

- **Security workflow efficiency.** The interviewed decision-makers also noted seeking a solution that would reduce the burden of manual processes and multiple-tool workflows on their security teams, while maintaining their security posture. They shared that Secure Firewall and FMC successfully met these needs, while those decision-makers that deployed SecureX saw even further operational efficiency.

“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.”

Engineering services manager, IT services

SECURE FIREWALL FEATURES

Features that enable additional value from the investment in Cisco Secure Firewall and Firewall Management Center include:

- **Unified visibility and management.** Secure Firewall and FMC drive a unified approach to security posture across physical, virtual, containerized, and private and public cloud firewalls. Decision-makers also noted improved network control and performance thanks to application-layer detection and blocking. By deploying policies once to multiple devices, FMC enables policy harmonization across hybrid and multicloud environments.
- **Entitlement to SecureX.** An investment in Secure Firewall entitles the customer organization to use and deployment of SecureX at no additional charge. SecureX enables further risk reduction and security workflow efficiencies by providing XDR capabilities, routine task automation, and threat response orchestration.

“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

KEY RESULTS

The composite organization experiences the following benefits over three years:

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%.

“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

Reduction of security investigation and response workstream times by up to 83%.

Decision-makers experienced substantial reductions to security professional work from combining Cisco Secure Firewall, Firewall Management Center, and SecureX. With Secure Firewall and FMC alone, interviewees noted reducing the time to investigate 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 an additional 77% of time spent on investigation and response.

“SecureX enables personalized, customizable dashboards, so that our team is not only getting additional visibility into the environment but also seeing only the most important information for their specific responsibilities.”

Security operations team lead, education

Reduced risk of breach by up to 80%. The combined visibility and control provided by Cisco Secure Firewall, FMC, and SecureX enabled the interviewees’ organizations to reduce the risk of a potential material breach and the associated costs. Secure Firewall and FMC alone reduced the risk of a breach by between 15% and 80%, depending on prior environments. SecureX enabled the interviewees’ organizations to reduce the risk and costs of a breach up to an additional average of 23%.

“SecureX gives 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 and all of our integrated Cisco security solutions.”

Security operations team lead, education

Improved end-user productivity valued at approximately \$2 million annually.

Deploying Cisco Secure Firewall and FMC 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.

“Cisco Secure Firewall gives us much better visibility into how the network is being used and the ability to control this use.”

Security operations team lead, education

Reduced costs from decommissioned legacy tools.

Cisco Secure Firewall also enabled decision-makers to decommission the 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.

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "[The Total Economic Impact™ Of Cisco Secure Firewall](#)," a commissioned study conducted by Forrester Consulting on behalf of Cisco, March 2022.

STUDY FINDINGS

Forrester interviewed ten decision-makers at eight organizations with experience using Cisco Secure Firewall and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Improvement to security workflows valued at \$8.2 million.
- Reduced risk of material breaches and productivity loss worth \$3.5 million.
- Performance benefits to employee productivity of \$4.1 million.



Return on investment (ROI)
195%



Net present value (NPV)
12.29M

Appendix A: 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.

DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Cisco and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Cisco Secure Firewall and Firewall Management Center.
- Cisco reviewed and provided feedback to Forrester. 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.
- Cisco provided the customer names for the interview(s) but did not participate in the interviews.

ABOUT TEI

Total Economic Impact™ (TEI) 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.

FORRESTER®