Forrester Consulting Total Economic Impact™ Checklist Commissioned By Broadcom, July 2025

How To Create Your Own Business Case For Broadcom SSE

A Six-Step Checklist For CISOs

Security Service Edge (SSE) platforms, such as Symantec SSE, are a critical component for organizations navigating the complexities of modern cloud-first and remote work environments. The widespread shift to hybrid work models and increasing reliance on cloud applications have created significant demand for cloud-delivered security. As cyber threats become more sophisticated and data protection regulations tighten, businesses urgently need SSE solutions to enforce zero-trust principles and provide secure access to resources regardless of user location or device.

Recognizing that traditional, centralized security models are inadequate for distributed workforces and cloud-hosted applications, Symantec SSE consolidates essential security capabilities into a single solution. Symantec SSE features include Cloud Secure Web Gateway (Cloud SWG) to protect users from web-based threats, a comprehensive Cloud Access Security Broker (CASB) for visibility and control over sanctioned and unsanctioned cloud applications, and Data Loss Prevention (DLP) capabilities to safeguard sensitive information across endpoints and private applications. Furthermore, it incorporates Zero Trust Network Access (ZTNA) to provide secure access to private applications and Remote Browser Isolation (RBI) to execute web content in an isolated environment, thus protecting users from malicious web content and phishing attacks. This checklist is designed to help readers develop a custom ROI assessment in six simple steps.

Organizations improve their security posture and operational reliability by delivering cloud-native threat and data protection.

Many companies struggle to manage disparate security tools and fragmented policies across diverse cloud and remote environments. As a result, they grapple with escalating security vulnerabilities, unpredictable system downtime, and difficulty managing their complex, disjointed legacy infrastructure. Forrester takes a holistic view of Symantec SSE's

Summary of results from the Total Economic Impact™ Of Symantec SSE

METHODOLOGY

Broadcom commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying Symantec SSE.

To achieve these objectives, Forrester interviewed representatives at four organizations with experience using Symantec SSE. The benefit frameworks presented have been simplified and condensed. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. To see the full financial framework and estimate how Symantec SSE can impact your organization, please see the full study.

total economic impact, which includes improved reliability, strengthened security posture, reduced network infrastructure costs, increased security operations time savings, and improved end-user productivity.

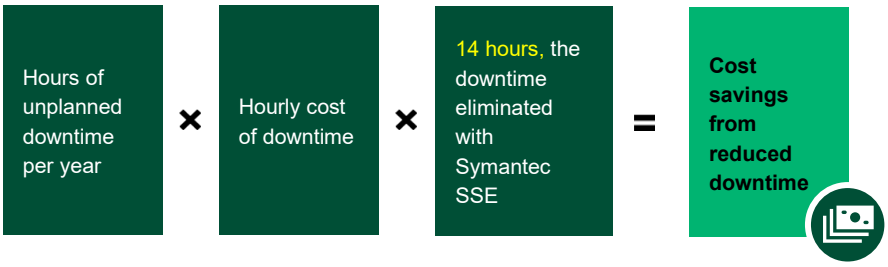
Here's how to start building a business case:

1 Calculate the cost savings of reduced downtime.

When organizations experience system outages, they can incur hundreds of thousands, if not millions, of dollars in lost business, reputational damage, and regulatory penalties. Symantec SSE reduces system downtime by leveraging Google Cloud Platform's (GCP) global infrastructure for high availability and performance. Additionally, Symantec SSE's dedicated egress capabilities help improve resilience by ensuring that traffic exits the security service efficiently and reliably, preventing bottlenecks that could lead to outages.

To calculate the business value of improved reliability, you will need to:

- Find the total customer-impacting downtime or severe performance degradation that you experience, in hours per year.
- Estimate the hourly cost of downtime, including lost revenue, fines, and reputational damage.
- Multiply the hourly cost by 14 hours, which is the total avoided unplanned downtime estimated in Forrester's TEI study.

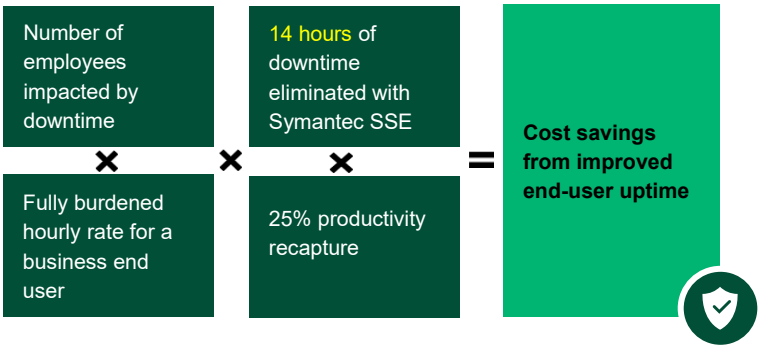


Second, you will need to measure the productivity impact of the improved uptime.

- Calculate the number of employees that each outage impacts. In Forrester's TEI study, each outage affected 25% of the composite's employees.

> "Symantec SSE is the best of breed when it comes to the functionality that it gives us and to its support [team]."
>
> **PRODUCT OWNER, FINANCIAL SERVICES**

- Multiply the number of employees impacted by 14, the downtime hours eliminated with Symantec SSE. This will give you the number of employee hours regained with Symantec SSE.
- Multiply the number of employee hours regained per year by the average fully burdened hourly rate for a business end user. Apply a productivity recapture percentage — Forrester recommends 25% in this case — since not all hours saved are redeployed productively.



2 Measure your savings in expected breach costs.

A major security breach has many costs, including customer loss, fines, remediation, productivity impacts, and brand rebuilding. To reduce the likelihood of a breach, Symantec SSE continuously inspects and controls user access to applications, data, and websites, blocking malicious activity before it reaches critical systems. Symantec SSE also integrates Zero Trust principles and real-time threat prevention to further reduce the attack surface.

To measure the value of reduced breach likelihood, you will need to:

- Estimate the average potential cost of a data breach for your organization and multiply this by your estimated likelihood of experiencing a breach each year, which will give you your annual expected breach costs. Forrester's study found that a $12 billion composite organization has a 68% likelihood of experiencing a breach, with each breach costing $4.6 million.
- Multiply your expected annual breach costs by the percentage of breaches that originate from either external attacks or attacks targeting employees' remote networks. Forrester's 2024 security

Forrester developed a composite organization based on data gathered from customer interviews to reflect the total economic impact that Symantec SSE could have on an organization and concluded that Symantec SSE has the following three-year financial impact.

ROI
125%

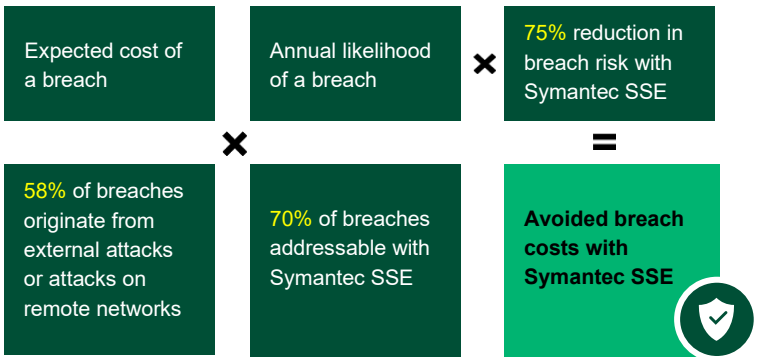
BENEFITS PV
$28.7 million

NPV
$15.9 million

PAYBACK
<6 months

survey found that these account for 58% of breaches on average. Then, multiply this total by 70%, which is the percentage of these breaches addressable with Symantec SSE. This will give you the total risk exposure addressable with Symantec SSE.

- Forrester found that a composite organization experiences a 75% reduction in these types of breaches from using Symantec SSE, so multiply the total risk exposure by 75%. This will give you your total expected breach cost savings per year from using Symantec SSE.



> "[Symantec's] Global Intelligence Network is second to none. The web categorization that Symantec provides is superior to any other product."
>
> **GATEWAY SECURITY ANALYST, INSURANCE**

3 Estimate network infrastructure cost savings from adopting Symantec SSE.

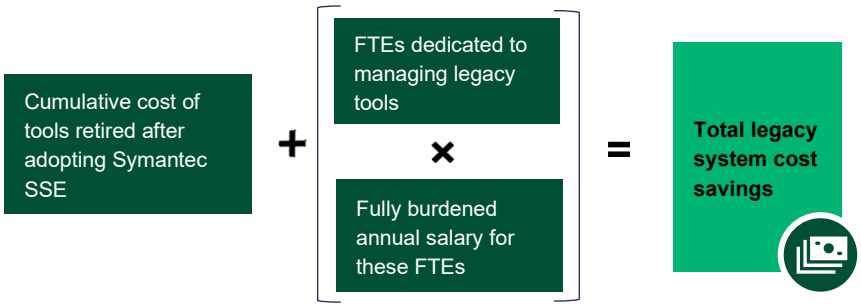
A major benefit of adopting Symantec SSE is the ability to retire incumbent on-prem proxies, VPNs, hardware firewalls, and other legacy security appliances. In addition to the direct cost savings, adopting Symantec SSE can lead to employee time savings, as it may be easier to maintain than legacy infrastructure.

To calculate the cost savings, you will need to:

- Determine which incumbent tools and legacy appliances your organization can retire by consolidating onto Symantec SSE. Add up all of these costs to determine the networking costs avoided with Symantec SSE. Forrester found that a composite organization can eliminate $3.6 million in annual networking costs by Year 3.
- Calculate how many FTEs your organization dedicates to managing legacy tools; in the Forrester TEI study, the composite

dedicated eight FTEs to legacy hardware maintenance. Multiply the number of FTEs by their average fully burdened annual salary. Multiply this value by 80% to apply the productivity recapture, since not all employee time savings are redeployed productively. This value will provide your total maintenance cost savings.

- Add your annual networking costs avoided with Symantec SSE and the total maintenance cost savings to determine the total costs eliminated with Symantec SSE.



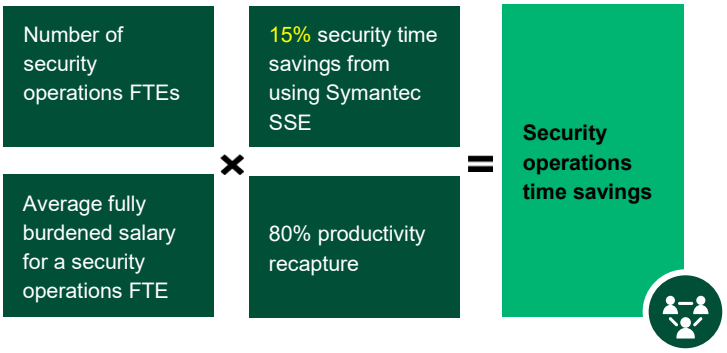
4 Calculate security operations time savings.

Symantec SSE can help organizations reduce their attack surface by centralizing and securing all web and cloud application access, leading to fewer security incidents that security operations teams need to investigate and remediate. This reduction results in significant time savings for the security team.

To calculate this for your organization, you will need to:

- Count the number of security operations FTEs that you have responding to security alerts. In the Forrester TEI study, the $12 billion annual revenue composite organization had a team of 28.
- Multiply the number of security operations FTEs by their average fully burdened annual salary. This will give you the total headcount costs for the security team.
- Forrester's study found that the security team will see a 15% productivity lift from using Symantec SSE. Multiply the total headcount costs by 15% to see the dollar value of the time savings.

- Multiply the dollar value of the time savings by 80%, since not all time savings are redeployed productively. This will give you the total dollar value of the security productivity improvement.



5 Determine the impact of improved end-user productivity.

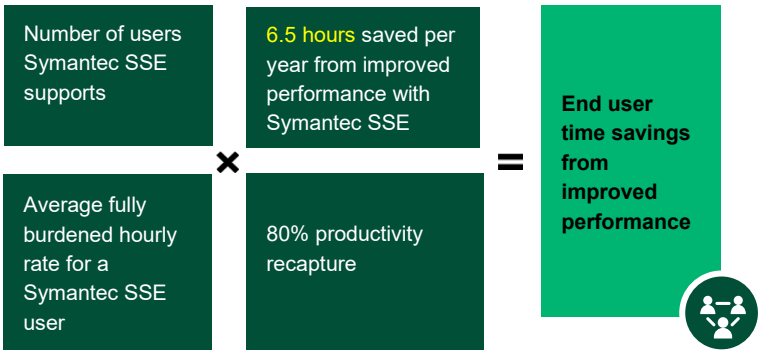
Symantec SSE reduces end-user latency in two ways. First, it leverages dedicated egress capabilities to ensure that traffic exits the security service close to the destination, minimizing unnecessary routing and delays. Second, Symantec SSE's deep integration with GCP allows organizations to reduce latency by routing traffic over high-capacity private pathways instead of the private internet.

To estimate the end-user impact of reduced latency for your organization:

- Measure how many end users Symantec SSE will support at your organization. In the Forrester TEI study, Symantec SSE supported 100% of the composite's 40,000 employees by Year 3 of the investment.
- Multiply the number of end users by 6.5, the total number of hours that Forrester found each employee saves per year in reduced latency and load times. This will give you the total number of employee hours saved by reduced latency per year.
- Multiply the total number of employee hours saved by the average fully burdened hourly rate for an employee.
- Apply a 25% productivity recapture since not all hours saved are redeployed productively. This will give you the total dollar value of the reduction in latency from using Symantec SSE.

"If I compare Symantec DLP with the other SSE players, the Symantec DLP solution is way ahead. It's enterprise-built, whereas those [competitors] will need at least one to two years to reach the level where Symantec is in DLP."

HEAD OF GLOBAL SECURITY, IT CONSULTING



6 Consider further benefits when building a business case for Symantec SSE.

Beyond the above benefits, there are other advantages that may result from an investment in Symantec SSE:

- Potential cybersecurity insurance cost savings from reporting your Symantec SSE use to insurance underwriters.
- User experience benefits from reduced latency and more precise website and application blocking.
- Optimized Symantec SSE deployment with high-quality support from Broadcom.
- Additional security improvements from adopting Symantec SSE's ZTNA capabilities, which provide a "never trust, always verify" model for every user and device accessing applications.
- Further cost and time savings from syncing Symantec SSE policies with Broadcom's mobile protection policies.

To read the full results of this study, please refer to the Total Economic Impact™ study commissioned by Broadcom.

Project Director: Matt Dunham