FORRESTER®

Estudio Total Economic Impact™ de Cisco Secure Firewall

Ahorros de costos y beneficios empresariales facilitado por Secure Firewall

MARZO DE 2022

Índice

Resumen ejecutivo 1

La trayectoria del cliente de Cisco Secure Firewall.....6

Principales desafíos 6

Organización compuesta.....7

Análisis de beneficios 9

Mejoras en la administración de firewalls 9

Mejoras en los flujos de trabajo de seguridad.....12

Riesgo reducido de vulneraciones de seguridad importantes y pérdida de productividad 15

Beneficios de desempeño para la productividad de los empleados.....18

Costos reducidos y evitados de soluciones anteriores 20

Beneficios no cuantificados.....22

Flexibilidad 23

Análisis de costos 24

Costos de licencia 24

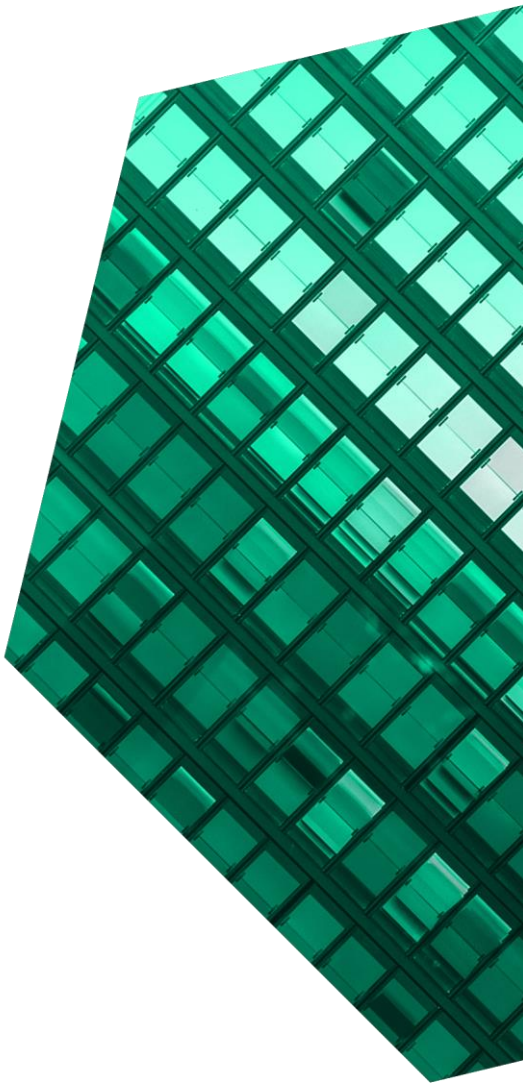
Costos de implementación, creación de políticas y capacitación 27

Resumen financiero.....29

Anexo A: Total Economic Impact.....30

Anexo B: Notas finales.....31

Equipo de consultoría: *Henry Huang*
Nick Mayberry



ACERCA DE FORRESTER CONSULTING

Forrester Consulting presta servicios de consultoría basados en análisis objetivos e independientes para ayudar a los directivos a tener éxito en sus organizaciones. Para obtener más información, visita forrester.com/consulting.

© Forrester Research, Inc. Reservados todos los derechos. Queda estrictamente prohibida la reproducción no autorizada. La información está basada en los mejores recursos disponibles. Las opiniones expresadas reflejan juicios válidos en un momento concreto y están sujetas a cambios. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar y Total Economic Impact son marcas comerciales de Forrester Research, Inc. El resto de las marcas comerciales son propiedad de sus respectivas compañías.

Resumen ejecutivo

Cisco Secure Firewall y Firewall Management Center mejoran la visibilidad de la organización y el control de esta sobre su seguridad de red. Las organizaciones de los entrevistados se ahorraron hasta un 95 % en el trabajo profesional de administración de redes relacionado con firewalls y hasta un 83 % en el trabajo profesional relacionado con seguridad. También redujo el riesgo de una vulneración de seguridad importante hasta en un 80 % a la vez que mejoró la productividad del usuario final al minimizar la interrupción de la red y de la VPN. La posición de seguridad mejoró aun cuando se redujeron los despliegues de firewalls en un 25 %.

Cisco Secure Firewall es una solución de seguridad de 7 capas que protege a las organizaciones de amenazas internas y externas al tiempo que alivia la carga de la red y el personal de seguridad para la administración de firewalls y amenazas. Las organizaciones pueden administrar Cisco Secure Firewall con Firewall Management Center (FMC), un nodo centralizado para la administración de firewalls y de defensa contra amenazas que le da al personal de seguridad y administración de redes una mayor visibilidad de las actividades de la red en una vista más unificada y holística, incluso en la capa de la aplicación y en amenazas detectadas en tráfico encriptado. Además, proporciona más control con el sistema de prevención de intrusiones (IPS) Snort 3 y mejoras de software para el filtrado de URL y defensa frente a malware.

La licencia de Cisco Secure Firewall incluye SecureX, la plataforma integrada de Cisco con la que las organizaciones pueden consolidar los datos sobre amenazas, facilitados por el portafolio de Cisco Secure y de herramientas externas de seguridad, en una única vista global de datos enriquecidos contextualmente. Esta plataforma fue concebida para facilitar la rapidez del proceso de investigación y respuesta.

Cisco encargó a Forrester Consulting la realización de un estudio de tipo Total Economic Impact™ (TEI) y un análisis del posible retorno de la inversión (ROI) que las empresas pudieran obtener con el uso de Secure Firewall.[1] El objetivo de este estudio es proporcionar un marco de referencia que permita evaluar el posible impacto financiero de Secure Firewall en las organizaciones.

Para entender mejor los beneficios, costos y riesgos asociados a esta inversión, Forrester entrevistó a diez responsables de la toma de decisiones en ocho organizaciones con experiencia en el uso de Secure Firewall. Para realizar este estudio, Forrester agrupó las experiencias de los clientes entrevistados y combinó los resultados en una sola organización compuesta.

ESTADÍSTICAS CLAVE

Retorno de la inversión (ROI)
195 %

Valor presente neto (VPN)
USD 12,29 millones

Antes de usar Secure Firewall, estos entrevistados observaron que a sus organizaciones les hacía la falta visibilidad y manejabilidad que necesitaban para administrar de forma adecuada y proteger con eficacia sus redes. Sin esta visibilidad ni una interfaz gráfica de usuario eficiente, los entrevistados notaron que los flujos de trabajo de redes como el despliegue de firewalls, la creación de políticas, las actualizaciones de firewalls y las actualizaciones de políticas tardaban un tiempo considerable. También se invirtió más tiempo en flujos de trabajo de seguridad, tales como la investigación de amenazas y la administración de las acciones de respuesta y de acceso remoto. Los entrevistados también observaron que había un desempeño deficiente de las redes durante períodos de alta demanda y complicaciones por administrar soluciones de varios proveedores.

Después de la inversión en Secure Firewall, los entrevistados no solo redujeron el tiempo que tardaron en completar los flujos de trabajo de redes y seguridad mencionados antes, sino que también mejoraron la seguridad general de sus organizaciones. A la vez, las organizaciones mejoraron la productividad de sus empleados con actualizaciones más rápidas de las políticas, mejoras en la inspección de tráfico de redes y un mejor desempeño de la red en general. Todo lo anterior, al mismo tiempo que se retiraron las soluciones heredadas y, en gran medida, se eliminaron los costos de tiempo de administración asociados.

Beneficios totales

USD 18,6 millones

PRINCIPALES CONCLUSIONES

Beneficios cuantificados. Entre los beneficios cuantificados en valor presente (VP) ajustados en función del riesgo están los siguientes:

- **Reducción de flujos de trabajo de operación de redes en hasta un 95 %.** Gracias a las funcionalidades más recientes de Cisco Secure Firewall y la facilidad de manejo de Firewall Management Center, las organizaciones de los entrevistados redujeron el tiempo de:
    - Despliegue de un firewall en un 36 %.
    - Actualización de un firewall en un 90 %.
    - Actualización de políticas de firewalls en un 95 % en comparación con los firewalls tradicionales de dispositivos adaptables de seguridad (ASA) de la serie 5500-X.
    - Actualización de las políticas de firewalls en un 80 % en comparación con las políticas basadas en la defensa contra amenazas de firewall (FTD) de primera generación.
    - Actualización de firewalls virtuales en un 80 %.
- **Reducción de hasta un 83 % en los tiempos de flujo de trabajo de investigación de seguridad y respuesta.** Los entrevistados también observaron ahorros considerables en el trabajo de los profesionales de seguridad al combinar Cisco Secure Firewall y Firewall Management Center, dado que la información estaba mejor organizada para su consumo y análisis. Los entrevistados mencionaron que hubo una reducción del tiempo dedicado a investigar posibles amenazas en un 49 % y del tiempo dedicado a responder a estas en un 83 %. El uso de SecureX junto con Secure Firewall y Firewall Management Center permitió a las organizaciones ahorrarse hasta un 77 % del tiempo restante invertido en investigación y respuesta.

> **“Nos tomamos muy en serio la seguridad y queremos sacar el máximo provecho a los productos para proteger nuestra empresa. Por eso elegimos Cisco. Ellos crecieron inmersos en el tema de seguridad, para ellos no es solo un complemento”.**
> *Ingeniero sénior de redes, sector de la producción*

- **Reducción del riesgo de vulneraciones de seguridad en hasta un 80 %.** Gracias a la visibilidad y el control combinados que proporcionan Cisco Secure Firewall y Firewall Management Center, las organizaciones de los entrevistados redujeron el riesgo de posibles vulneraciones de seguridad importantes y sus costos asociados. Estas soluciones redujeron el riesgo de una vulneración de seguridad en un 80 % en comparación con los firewalls ASA tradicionales de la serie 5500-X y en un 15 % en comparación con los firewalls de FTD de primera generación. SecureX permitió a la organización de los entrevistados reducir el riesgo y los costos restantes de una vulneración de seguridad en hasta un 23 % más.

- **Mejoras de la productividad del usuario final valoradas en aproximadamente USD 2 millones anuales.** La implementación de Cisco Secure Firewall y Firewall Management Center mejoró la productividad de las organizaciones de los entrevistados de dos formas. Primero, permitió a los profesionales de redes solucionar los errores problemáticos de actualización de políticas un 80 % más rápido. En segundo lugar, redujo la gravedad del deterioro de desempeño de la red y devolvió cerca de 9 horas de trabajo anuales a cada usuario final afectado.
- **Reducción de los costos por el retiro de herramientas heredadas.** Los entrevistados también señalaron que Cisco Secure Firewall les permitió retirar soluciones de seguridad heredadas costosas que se habían implementado en el pasado. Los entrevistados mencionaron que se ahorraron cientos de miles de dólares al año en sistemas de prevención de intrusiones independientes, millones de dólares al ahorrarse el costo de reemplazar sus soluciones de seguridad existentes y un 25 % adicional de los costos, ya que Cisco Secure Firewall les proporcionó el mismo grado de protección con menos firewalls.

Beneficios no cuantificados. Entre los beneficios no cuantificados en este estudio se encuentran los siguientes:

- **Productividad de las VPN y mejoras de seguridad.** Cisco Secure Firewall también permitió tener una mayor productividad de las VPN para acceso remoto y una mayor seguridad gracias al balanceo de cargas, la autenticación local y la autenticación con varios certificados. Los usuarios finales consiguieron mejores conexiones a través de las VPN mientras que las organizaciones tuvieron un mejor control del acceso.
- **Mejores operaciones para trabajar desde casa.** Los controles de Cisco Secure Firewall también ayudaron a que las operaciones siguieran funcionando adecuadamente cuando el uso de las VPN se disparó en el momento en que los empleados hicieron la transición al trabajo desde casa. Los profesionales de administración de redes pudieron aprovechar la limitación de velocidad y las mejoras en la redundancia para mejorar la experiencia y la productividad de los empleados, aun en puntos álgidos de la demanda.
- **Facilidad de transición a la nube.** Por último, los entrevistados compartieron que Cisco Secure Firewall facilitó más sus iniciativas de transición a la nube al ofrecerles una plataforma que protegía el tráfico en un sitio, entre sitios y entre la organización y varias plataformas de servicios en la nube. Más concretamente, Cisco proporciona políticas estandarizadas y medios validados de implantación de Secure Firewall mediante mercados de plataformas de servicios en la nube.

Costos. Los costos en VP ajustados en función del riesgo incluyen:

- **Costos de licencia.** Aunque los costos de licencia fueron los más altos en los que incurrieron las organizaciones de los entrevistados, formar un acuerdo de empresa de Cisco les ahorró cientos de miles de dólares en funcionalidades y soluciones adicionales que las organizaciones no tenían antes, pero perfeccionó la posición de seguridad de sus organizaciones. Los derechos de licencia de SecureX se incluyen en Secure Firewall.
- **Costos de implementación, creación de políticas y capacitación.** Los entrevistados mencionaron que tuvieron costos internos para la implementación y el despliegue de los firewalls, y para la creación de políticas para estos. El despliegue de firewalls se estima en unas 6 horas por instalación, mientras que la creación de políticas tardó un estimado de 30 horas. La implementación de SecureX requiere 20 horas más de trabajo y 100 horas anuales para su administración continua. Algunos entrevistados también señalaron la necesidad de capacitar a sus profesionales de seguridad y administración de redes para usar Cisco Secure Firewall y Firewall Management Center. Los costos internos de la capacitación llegaron a 2 horas por empleado capacitado en los que, según los entrevistados, se aprovecharon los videos de capacitación disponibles públicamente con expertos de seguridad de Cisco.

Las entrevistas a los responsables de la toma de decisiones y el análisis financiero revelaron que la organización compuesta obtuvo beneficios por valor de USD 18,59 millones a lo largo de tres años frente a costos por valor de USD 6,30 millones, lo que da lugar a un valor presente neto de USD 12,29 millones y un ROI del 195 %.

ROI
195 %

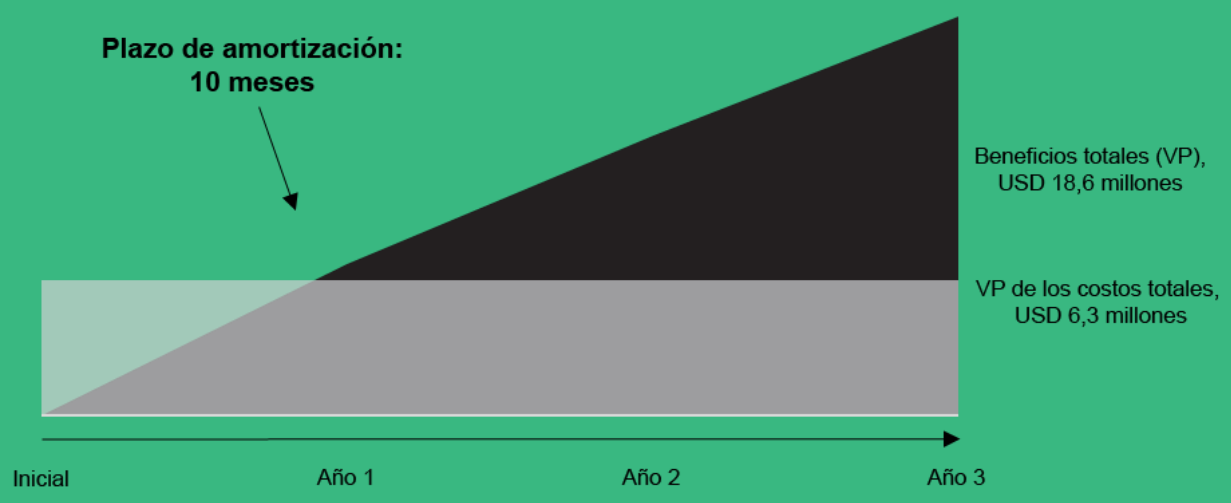
BENEFICIOS (VP)
USD 18,59 millones

VALOR PRESENTE NETO
USD 12,29 millones

PLAZO DE AMORTIZACIÓN
10 meses

Beneficios (a tres años)

Resumen financiero



MARCO DE REFERENCIA Y METODOLOGÍA DEL TEI

A partir de la información proporcionada en las entrevistas, Forrester diseñó un marco de referencia Total Economic Impact™ para las organizaciones que estén considerando invertir en Cisco Secure Firewall.

El objetivo de este marco es determinar los factores de costo, beneficio, flexibilidad y riesgo que afectan a la decisión de inversión. Forrester adoptó un enfoque de varios pasos para evaluar el impacto que Secure Firewall puede tener en una organización.

DEBIDA DILIGENCIA

Se entrevistó a las partes interesadas de Cisco y a los analistas de Forrester para recabar datos relacionados con Secure Firewall.

ENTREVISTAS A RESPONSABLES DE LA TOMA DE DECISIONES

Se entrevistaron a diez responsables de la toma de decisiones en organizaciones que utilizan Secure Firewall para obtener datos relativos a sus costos, beneficios y riesgos.

ORGANIZACIÓN COMPUESTA

Se diseñó una organización compuesta a partir de las características de las empresas de los entrevistados.

MARCO DE REFERENCIA DEL MODELO FINANCIERO

Se desarrolló un modelo financiero representativo de las empresas entrevistadas utilizando el método TEI y se ajustó el modelo financiero en función del riesgo, de acuerdo con las inquietudes y preocupaciones de los responsables de la toma de decisiones.

CASO PRÁCTICO

Se utilizaron cuatro elementos fundamentales de la metodología TEI para modelar el impacto de la inversión: beneficios, costos, flexibilidad y riesgos. Dado el enfoque cada vez más integral de los análisis de retorno de la inversión (ROI) relacionados con las inversiones de TI, la metodología TEI de Forrester permite proyectar un panorama completo del impacto económico total de las decisiones de compra.
El anexo A contiene información adicional sobre la metodología TEI.

AVISOS

Información para el lector:

El estudio fue encargado por Cisco y elaborado por Forrester Consulting. Este estudio no debe usarse como un análisis competitivo.

Forrester no hace suposiciones respecto al posible rendimiento de la inversión que lograrían otras empresas. Forrester recomienda encarecidamente que los lectores utilicen sus propios cálculos, dentro del marco aportado por el estudio, para determinar si una inversión en Secure Firewall es adecuada.

Aunque Cisco revisó el estudio y facilitó a Forrester comentarios y sugerencias, Forrester conserva el control editorial del estudio y sus resultados y no acepta cambios que contradigan las conclusiones extraídas o que enturbien el significado del propio estudio.

Aunque Cisco proporcionó los nombres de los clientes entrevistados, no participó en las entrevistas.

La trayectoria del cliente de Cisco Secure Firewall

Factores que conducen a la inversión en Secure Firewall

Responsables de la toma de decisiones entrevistados			
Persona entrevistada	**Sector**	**Región**	**Total de empleados**
Gerente de servicios de ingeniería	Servicios de TI	Norteamérica	750
Ingeniero jefe de infraestructura	Servicios financieros	Norteamérica	2800
Subgerente de servicios de telecomunicaciones y telefonía	Servicios financieros	Norteamérica	2800
Ingeniero principal de ciberseguridad	Servicios de seguridad	Norteamérica	3000
Ingeniero sénior de redes	Ingeniero sénior de redes, sector de la manufactura	Global	5500
Gerente sénior de ingeniería de redes	Tecnología	Global	40.000
Ingeniero sénior de seguridad	Tecnología	Global	40.000
Jefe de equipo de operaciones de seguridad	Educación	Norteamérica	46.000
Arquitecto de infraestructura de personal	Industrial	Global	205.000
Ingeniero sénior de redes	Tecnología	Global	275.000

PRINCIPALES DESAFÍOS

Antes de implementar Cisco Secure Firewall y Firewall Management Center, las organizaciones de los entrevistados usaban, en su mayor parte, dispositivos de firewalls ASA de la serie 5500-X para proteger sus entornos. Algunos entrevistados habían pasado de firewalls ASA tradicionales a firewalls FTD de primera generación desde hace años y mencionaron que habían tenido beneficios adicionales tras actualizarse a la última versión de FTD en Cisco Secure Firewall y Firewall Management Center.

Los entrevistados comentaron que tuvieron que hacer frente a problemas habituales, entre los que se incluyen:

- **Visibilidad limitada.** Los entrevistados mencionaron que sus entornos anteriores dependían de firewalls ASA de la serie 5500-X que proporcionaban poca visibilidad de su seguridad general. Un culpable era la falta de integración. En los entornos anteriores, las organizaciones de los entrevistados tenían dificultades para integrar diversas soluciones de seguridad para conseguir la unificación en la administración y la uniformidad en la aplicación de políticas y, además, solo veían una parte de la realidad. Otro motivo para la visibilidad limitada era que los entornos anteriores dependían de las inspecciones de puertos como el "mirador" principal para ver la red. Los entrevistados indicaron que esto no les permitía ver los datos en profundidad, restringía la visibilidad de las aplicaciones y les daba un contexto histórico limitado.

"Antes no teníamos la capacidad, como el control moderno de aplicaciones. No podíamos saber cómo estaban usando la red nuestros usuarios y no podíamos reaccionar a este uso de forma adecuada".
Jefe de equipo de operaciones de seguridad, sector educativo

- **Costos altos de tiempo para implementar y administrar firewalls.** Los entrevistados también señalaron que el despliegue y la administración de sus firewalls heredados requería una gran inversión de tiempo. Gran parte de esto se debía a la falta de capacidad para enviar actualizaciones a varios dispositivos a la vez. El jefe de equipo de operaciones de seguridad del sector educativo estimó que el despliegue de una regla sencilla de firewall podía tardar hasta 45 minutos. Además, los entrevistados mencionaron que la falta de visibilidad de sus entornos anteriores conllevaba invertir una cantidad excesiva de tiempo para relacionar datos entre distintos sistemas para confirmar las posiciones de seguridad.

"La facilidad de administración e integración ha sido una de las ventajas de Cisco. También nos beneficiamos del enriquecimiento de datos, ya que los diferentes sistemas se retroalimentan con más facilidad. También hemos creado respuestas autónomas a determinadas amenazas. Antes no podíamos hacer nada de esto".
Ingeniero principal de ciberseguridad, sector de servicios de seguridad

- **Mal desempeño.** Los entrevistados también dijeron que sus sistemas anteriores tenían un mal desempeño. Por ejemplo, el jefe de equipo de operaciones de seguridad del sector educativo dijo que sus soluciones anteriores "se caían, se reiniciaban continuamente y se perdían paquetes" cuando se disparaba la demanda de sus redes e infraestructura de seguridad. Esto incluso llegó a tener un efecto en la productividad, ya que "los profesores que utilizaban la red para reproducir un video o demostrar algo en clase no podían hacerlo".

- **Administración de proveedores.** Por último, los clientes hicieron la observación de que tener varios proveedores en su entorno anterior les creaba dolores de cabeza para administrarlos. El ingeniero jefe de infraestructura de una empresa de servicios financieros comentó que: "Con varios proveedores, todo tenía que hacerse varias veces y acceder a varios planos de control para aplicar los mismos cambios o hacer actualizaciones en sistemas desiguales".

ORGANIZACIÓN COMPUESTA

A partir de las entrevistas, Forrester desarrolló un marco de referencia TEI, una organización compuesta y un análisis de ROI en el que se ilustran las áreas afectadas desde el punto de vista financiero. La organización compuesta es representativa de los nueve responsables de la toma de decisiones que fueron entrevistados por Forrester y se utiliza para presentar el análisis financiero que se muestra en la siguiente sección. La organización compuesta tiene las siguientes características:

Descripción de la organización compuesta.
La organización compuesta es una empresa de tecnología B2B con ingresos anuales de USD 5000 millones y 16.000 empleados. Ofrece sus servicios en todo el mundo.
La organización requiere una alta disponibilidad en sus centros de datos para garantizar que el acceso de los clientes a los datos almacenados sea constante. Estos centros de datos también requieren una elevada seguridad para proteger datos confidenciales de los clientes de accesos indeseados o ataques. Además de los centros de datos, la organización se mueve hacia un paradigma más distribuido con el uso de servicios multinube. Adicionalmente, la organización también está usando firewalls de Secure Firewall para proteger sus instalaciones en la frontera y sucursales.

Características de la implementación. La organización compuesta ya ha invertido en firewalls de próxima generación de Cisco. Dos tercios de sus existencias de firewalls son dispositivos Cisco Firepower y el otro tercio se compone de firewalls ASA de la serie 5500-X. La organización ahora está pasando los firewalls de su centros de datos, sus 102 oficinas remotas y la oficina principal a la última versión de Cisco Secure Firewall al actualizar sus 68 dispositivos Firepower y reemplazar sus 34 dispositivos ASA. Algunos entrevistados eligieron

actualizar los dispositivos tradicionales ya existentes a software de FTD sin cambiar su hardware. También despliegan los firewalls virtuales de Cisco Secure Firewall en sus centros de datos para manejar el tráfico de este a oeste entre los centros de datos y las sucursales, así como el tráfico entre los centros de datos y las distintas plataformas de nube pública. La organización aprovecha la inclusión de SecureX en su licencia de Secure Firewall para realizar más mejoras en el trabajo de investigación de amenazas y respuesta de su personal de seguridad.

Principales premisas

- **USD 5000 millones en ingresos**
- **16.000 empleados**
- **Reemplazo de 34 firewalls ASA**
- **Actualización de 68 firewalls Firepower a la última versión de Cisco Secure Firewall**

Análisis de beneficios

Beneficios cuantificados aplicados a la organización compuesta

Beneficios totales						
Ref.	**Beneficio**	**Año 1**	**Año 2**	**Año 3**	**Total**	**Valor presente**
Atr	Mejoras en la administración de firewalls	USD 134.951	USD 25.556	USD 25.556	USD 186.064	USD 163.005
Btr	Mejoras en los flujos de trabajo de seguridad	USD 2.669.879	USD 3.685.484	USD 3.685.484	USD 10.040.848	USD 8.241.976
Ctr	Riesgo reducido de vulneraciones de seguridad importantes y pérdida de productividad	USD 1.291.446	USD 1.393.402	USD 1.520.848	USD 4.205.696	USD 3.468.249
Dtr	Beneficios de desempeño para la productividad de los empleados	USD 1.656.403	USD 1.656.403	USD 1.656.403	USD 4.969.210	USD 4.119.230
Etr	Reducción de los costos por el retiro de soluciones heredadas	USD 1.985.115	USD 503.513	USD 503.513	USD 2.992.142	USD 2.599.074
	Beneficios totales (ajustados en función del riesgo)	USD 7.737.795	USD 7.264.360	USD 7.391.805	USD 22.393.959	USD 18.591.534

MEJORAS EN LA ADMINISTRACIÓN DE FIREWALLS

Pruebas y datos. Los encargados de la toma de decisiones entrevistados mencionaron los ahorros en tiempo y costos relacionados con la administración de firewalls después de implementar Cisco Secure Firewall, independientemente de si estaban haciendo el cambio desde firewalls heredados o si eran actualizaciones de versiones previas de Firepower Threat Defense. Una gran parte de estas mejoras provenía del hecho de que Firewall Management Center ayudaba a los profesionales de administración de redes al proporcionarles la posibilidad de administración centralizada de los firewalls mediante una única “ventana” que les permitía realizar cambios en muchos dispositivos.

“Firewall Management Center nos da un solo lugar para la administración y actualización de firewalls, en lugar de tener que saltar de un firewall al otro como hacíamos antes”.
Gerente de servicios de ingeniería, sector de servicios de TI

Las organizaciones de los entrevistados tuvieron en común que ahorraron tiempo y costos relacionados con el despliegue de firewalls. Con los firewalls ASA tradicionales, los entrevistados señalaron que el despliegue de firewalls tardaba un tiempo considerable, requería redactar reglas de firewalls para casos de uso específicos y distribuirlas manualmente en las distintas políticas de firewalls que existían.

“Cisco Secure Firewall nos permitió inicializar y desplegar rápidamente nuevos firewalls. No tuvimos que aumentar los empleados a medida que aumentábamos los firewalls”.
Gerente sénior de ingeniería de redes, sector tecnológico

Tras pasarse a Cisco Secure Firewall y Firewall Management Center, los entrevistados indicaron que ahorraron entre un 30 % y un 40 % de tiempo en el despliegue de firewalls. La reducción del tiempo se atribuyó a la capacidad de automatizar el despliegue que ofrece Cisco Secure Firewall. Por ejemplo el gerente sénior

de ingeniería de redes del sector tecnológico dijo: "Automatizamos la implementación con Cisco Secure Firewall. Tenemos automatización para instalar la caja, dejar lista la IP, configurar el chasis y aplicar las políticas".

"La automatización integrada es la que nos ahorra más tiempo. Incluso en las actualizaciones. Ya no me tengo que sentar y hacer de 'niñero' del proceso de actualización, como pasaba con los dispositivos ASA. Ahora me puedo ir y Firepower me informa si no vuelve a estar en línea tras un tiempo suficiente".
Gerente sénior de ingeniería de redes, sector tecnológico

La automatización también ayudó a los entrevistados en lo que respecta a la administración y el mantenimiento de sus firewalls de Cisco Secure Firewall tras la implementación. Cisco Secure Firewall incluye actualizaciones automatizadas integradas. Los entrevistados dijeron que actualizar los firewalls ASA se podía tardar varias horas en las que había que ir de firewall a firewall, subir los archivos actualizados y reiniciar los sistemas. Con Cisco Secure Firewall y Firewall Management Center, comentaron que solo tenían que hacer clic en la interfaz para actualizar los firewalls y después volvían a revisar dentro de 30 minutos para ver que todo hubiera salido bien.

"Estamos viendo ahorros de entre un 60 % y un 70 % a lo largo del tiempo en la administración de políticas después de pasarnos de ASA a Cisco Secure Firewall".
Gerente de servicios de ingeniería, sector de servicios de TI

Con Cisco Secure Firewall y Firewall Management Center, los entrevistados mencionaron que las políticas podían organizarse en categorías y zonas sin necesidad de tener largas listas de control de acceso que usaban un sistema orientado a objetos. Las políticas también podían desplegarse y actualizarse automáticamente ahora, a diferencia de actualizar manualmente todos los dispositivos.

"Cisco Secure Firewall despliega automáticamente el 90 % de la política por nosotros. Ya no tenemos que lidiar con configuraciones únicas".
Gerente sénior de ingeniería de redes, sector tecnológico

Los entrevistados señalaron que también ahorraron tiempo tras actualizar desde FTD de primera a última generación con Cisco Secure Firepower. Por ejemplo, el ingeniero jefe de infraestructura del sector de los servicios financieros dijo que con FTD de primera generación, el despliegue de políticas tardaba entre 10 y 15 minutos, pero con los FTD mejorados, el tiempo bajaba hasta cerca de 3 minutos.

"La administración de políticas con Cisco Secure Firewall es un proceso directo y fácil. La interfaz gráfica de usuario de Firewall Management Center es ligera, limpia e intuitiva".
Gerente sénior de ingeniería de redes, sector tecnológico

Uno de los entrevistados no usaba Firewall Management Center, sino la administración en la nube del software como servicio (SaaS) Cisco Defense Orchestrator (CDO). Con respecto a CDO, el arquitecto de infraestructura de personal del sector industrial compartió que: “Adoptar CDO ha sido indoloro. Como nuestros ingenieros ya estaban familiarizados con [Cisco Security Manager (CSM)], podían manejar la interfaz de líneas de comando y crear macros. Fue mucho más fácil que cambiar a otro proveedor donde podría haber sido complejo tener que aprender nuevos conceptos de la capa superior”.

Modelado y premisas. En el caso de la organización compuesta, Forrester toma el siguiente modelo:

- Se reemplazaron 34 firewalls ASA tradicionales de la serie 5500-X por Cisco Secure Firewalls.
- La organización compuesta se ahorra las 55 horas de mano de obra que podría tomar desplegar y crear políticas para el reemplazo de cada firewall tradicional.
- La organización se ahorra el 90 % de los 30 minutos que invertía cada trimestre en la actualización de cada firewall.
- En promedio, la organización compuesta actualiza una política de firewall diariamente. Al pasarse a Cisco Secure Firewall, se ahorra el 95 % de la hora que invertía en hacer estas actualizaciones.
- La tarifa horaria promedio con todas las prestaciones de un profesional de operaciones de seguridad de redes (NetSecOps) es USD 65.
- Se actualizaron 68 firewalls FTD a la última versión de Cisco Secure Firewall. Por cada actualización de política diaria, la organización compuesta se ahorra el 80 % del tiempo que se tarda en firewalls FTD de primera generación.
- Además, se ahorra el 80 % del tiempo que invertía en actualizar las políticas de firewalls virtuales.

Riesgos. Las mejoras de administración de firewalls podrían variar en función de los siguientes:

- El tipo y número de firewalls que tienen.
- El número de firewalls que se reemplaza con Cisco Secure Firewalls y el ritmo de este despliegue.
- La decisión de desplegar firewalls virtuales en centros de datos para administrar el tráfico de este a oeste y el tráfico de nubes públicas.

Resultados. Para tomar en cuenta estos riesgos, Forrester redujo este beneficio en un 10 %, lo cual produjo un VP a 3 años ajustado al riesgo (descontando el 10 %) de cerca de USD 163.000.

Mejoras en la administración de firewalls					
Ref.	**Métrica**	**Fuente**	**Año 1**	**Año 2**	**Año 3**
A1	Número de firewalls de próxima generación que reemplazan a firewalls heredados	Org. compuesta; 1/3 de 102 total	34	0	0
A2	Horas ahorradas en el despliegue de cada firewall	Entrevistas	55,00	55,00	55,00
A3	Horas ahorradas en la actualización de cada firewall ASA	90 %*17 horas trimestrales	61,2	61,2	61,2
A4	Horas ahorradas en la actualización manual de políticas para firewalls ASA	95 %*1 hora, una vez al día*33 % del entorno	114	114	114
A5	Tarifa horaria de profesionales NetSecOps	Organización compuesta	USD 65	USD 65	USD 65
A6	Subtotal: Reducción de tiempo para el despliegue y la actualización de firewalls de próxima generación desde firewalls de capa 4 heredados	((A1*A2)+(A3+A4))*A5	USD 132.938	USD 11.388	USD 11.388
A7	Número de firewalls FTD actualizados	Org. compuesta; 2/3 de 102 total	68	68	68
A8	Horas anteriores para el despliegue de políticas con FTD de primera generación	Entrevistas	0,25	0,25	0,25
A9	Reducción del tiempo de despliegue de políticas al pasarse a FTD de próxima generación	Entrevistas; de 15 minutos a 3 minutos	80 %	80 %	80 %
A10	Subtotal: Tiempo reducido al desplegar políticas en Firepower desde firewalls de capa 7 más antiguos	365*A8*A9*A5*A7/102	USD 3163	USD 3163	USD 3163
A11	Número total de firewalls virtuales	Organización compuesta	100	100	100
A12	Horas ahorradas para la actualización de políticas de firewalls virtuales	80 %*266 horas anuales	213	213	213
A13	Subtotal: Reducción del tiempo para administrar firewalls virtuales	A12*A5	USD 13.845	USD 13.845	USD 13.845
At	Mejoras en la administración de firewalls	A6+A10+A13	USD 149.946	USD 28.396	USD 28.396
	Ajuste en función del riesgo	↓10 %			
Atr	Mejoras en la administración de firewalls (ajustadas en función del riesgo)		USD 134.951	USD 25.556	USD 25.556
Total a tres años: USD 186.064			**Valor presente a tres años: USD 163.005**		

MEJORAS EN LOS FLUJOS DE TRABAJO DE SEGURIDAD

Pruebas y datos. La implementación de Cisco Secure Firewall y el uso de Firewall Management Center también ayudó a optimizar los flujos de trabajo de seguridad de los entrevistados. Los encargados de la toma de decisiones mencionaron que los dispositivos ASA requerían varias herramientas separadas para supervisar y registrar eventos entre los firewalls. Con Firewall Management Center, los datos de Cisco Secure Firewall se consolidaron en un solo lugar donde los indicadores de peligro (IOC) y las intrusiones bloqueadas podrían monitorearse o ser escaladas con coherencia a una solución de administración de información de seguridad y eventos (SIEM). Con Firewall Management Center, los entrevistados obtuvieron la capacidad de revisar conexiones, eventos y telemetría como un todo, de una manera más relacionada en toda la red.

> **“Las investigaciones de seguridad solían ser como armar un rompecabezas con una sola pieza”.**
> *Jefe de equipo de operaciones de seguridad, sector educativo*

Al consolidar los datos mediante Firewall Management Center, los entrevistados dijeron que se habían reducido los costos de tiempo del trabajo de investigación de seguridad. Por ejemplo, el ingeniero principal de ciberseguridad del sector de los servicios de seguridad mencionó que hubo una reducción del tiempo que se tardaba en investigar, que pasó de horas a 3-5 minutos con ayuda de Secure Firewall y Firewall Management Center. Antes de esto, este entrevistado mencionó que tenía que pasar por varios sistemas, incluido un SIEM y una consola de correos electrónicos, iniciar sesión y coordinar los datos. Ahora, solo tiene que iniciar sesión en Firewall Management Center y buscar los IOC específicos en ese entorno.

"Firewall Management Center funciona como una consola única para administrar todos los firewalls de Cisco Secure Firewall. Facilita la administración y ahorra tiempo para investigar y ordenar eventos y tomar decisiones con respecto a la actividad maliciosa".
Gerente de servicios de ingeniería, sector de servicios de TI

Los entrevistados también observaron una reducción en sus tiempos de respuesta. Por ejemplo, el jefe de equipo de operaciones de seguridad del sector educativo dijo que antes de invertir en Cisco Secure Firewall, tenía que enviar tickets al equipo de soporte de clientes varias veces por semana. El equipo de soporte rastreaba al usuario y realizaba una prueba de malware; un análisis que podía tardar horas. Luego, el equipo del entrevistado podía limpiar todo el sistema o incluso restablecer la imagen inicial. Este proceso podía tardar todo un día. Con Cisco Secure Firewall, este entrevistado envía un ticket parecido una vez al mes y va directamente al Firewall Management Center para solucionar el problema, lo que toma cerca de una hora.

"Nuestros firewalls heredados requerían muchos gastos generales para ejecutar la respuesta a incidentes de seguridad: costaba mucho en tiempo y dinero. Con Firepower, estamos obteniendo grandes ahorros de tiempo y efectuando menos respuestas de incidentes, ya que realiza más bloqueos".
Jefe de equipo de operaciones de seguridad, sector educativo

Los entrevistados que pasaron de una versión de primera generación de FTD a una versión actualizada también experimentaron beneficios relacionados con los flujos de trabajo de investigación de seguridad y respuesta. Como dijo el ingeniero jefe de infraestructura del sector de los servicios financieros, la versión anterior de FTD sí permitía una vista total de las alertas de seguridad mediante Firewall Management Center, pero tras la actualización, mejoraron las definiciones y las capacidades de alerta. Este entrevistado también mencionó que las demás integraciones con los productos de Cisco, tales como AMP y Umbrella, proporcionaron incluso más beneficios gracias a las correlaciones adicionales.

"Firewall Management Center nos da una excelente visibilidad. Con este grado de visibilidad que tenemos ahora, pasamos más tiempo revisando y asegurándonos de que todo esté bien. Pero aun así pasamos menos tiempo del que solíamos pasar en la respuesta a incidentes".
Jefe de equipo de operaciones de seguridad, sector educativo

Las organizaciones que aprovecharon la inclusión de SecureX en su licencia de Secure Firewall mejoraron todavía más la eficiencia operativa de su personal de seguridad mediante la visibilidad y personalización. Por ejemplo, el jefe de equipo de operaciones de seguridad del sector educativo también mencionó que SecureX les permitió tener tableros individualizados y personalizables, de modo que su equipo no solo obtenía más visibilidad del entorno, sino que también mostraba a los distintos usuarios la información más importante según sus responsabilidades.

Modelado y premisas. En el caso de la organización compuesta, Forrester toma el siguiente modelo:

- Una cifra de 100.000 de total anual de alertas de seguridad.
- El 26 % de estas requerían la atención de un analista de seguridad.
- El 70 % de las alertas que requerían atención también requerían ser investigadas.
- Cisco Secure Firewall y Firewall Management Center ahorraron un 49 % de las 2,8 horas que se invertían en investigar alertas.
- Un 10 % de las alertas que requerían investigación requerían una respuesta.
- Cisco Secure Firewall y Firewall Management Center ahorraron un 83 % de las 6 horas que se invertían en responder.
- SecureX permite conseguir más ahorros de tiempo para flujos de trabajo de investigación y respuesta de un 42 % en el primer año y un 77 % en el segundo y tercer año.

Riesgos. La mejora de flujos de trabajo de seguridad variará en función de lo siguiente:

- El número de alertas anuales, alertas que requieren atención, alertas que requieren investigación y alertas que requieren una respuesta.
- La tarifa horaria con todas las prestaciones de los profesionales de NetSecOps.

Resultados. Para contemplar estos riesgos, Forrester ajustó este beneficio y lo redujo en un 15 %, lo que dio como resultado un VP total a 3 años ajustado en función del riesgo de más de USD 8,2 millones.

Mejoras en los flujos de trabajo de seguridad					
Ref.	**Métrica**	**Fuente**	**Año 1**	**Año 2**	**Año 3**
B1	Total de alertas anuales	Organización compuesta	100.000	100.000	100.000
B2	Alertas que requieren atención de un analista	Forrester Research; 26 %	26.000	26.000	26.000
B3	Porcentaje de alertas que requieren investigación	Entrevistas	70 %	70 %	70 %
B4	Horas anteriores promedio para investigar	Entrevistas	2,8	2,8	2,8
B5	Reducción del tiempo para investigar debido a FMC	Entrevistas	49 %	49 %	49 %
B6	Alertas que requieren una respuesta	Entrevistas	260	260	260
B7	Horas anteriores promedio para responder	Entrevistas	6	6	6
B8	Reducción del tiempo para responder debido a FMC	Entrevistas	83 %	83 %	83 %
B9	Reducción adicional de la investigación y la respuesta debido a SecureX	Entrevistas	42 %	77 %	77 %
B10	Tarifa horaria con todas las prestaciones de un profesional de seguridad	A5	USD 65	USD 65	USD 65
Bt	Mejoras en los flujos de trabajo de seguridad	((B2*B3*B4*B5)+(B6*B7*B8)+ (B2*B3*B4*B5)+(B6*B7*B9))*B10	USD 3.141.034	USD 4.335.864	USD 4.335.864
	Ajuste en función del riesgo	↓15 %			
Btr	Mejoras en los flujos de trabajo de seguridad (ajustadas en función del riesgo)		USD 2.669.879	USD 3.685.484	USD 3.685.484
Total a tres años: USD 10.040.848			**Valor presente a tres años: USD 8.241.976**		

RIESGO REDUCIDO DE VULNERACIONES DE SEGURIDAD IMPORTANTES Y PÉRDIDA DE PRODUCTIVIDAD

Pruebas y datos. Los entrevistados también mencionaron que obtuvieron beneficios económicos relacionados con la reducción del riesgo de una vulneración de seguridad importante y los costos de productividad asociados después de implementar Cisco Secure Firewall.

Una forma en la que mejoró la posición de seguridad de las organizaciones de los entrevistados fue con la mayor visibilidad que les proporcionaban Cisco Secure Firewall y Firewall Management Center. Por ejemplo, el jefe de equipo de operaciones de seguridad del sector educativo dijo: “En comparación con los dispositivos ASA tradicionales, Cisco Secure Firewall nos da más visibilidad. Esto es especialmente importante porque los usuarios están entrando cada vez más con dispositivos móviles a nuestra red y accediendo a servicios como impresión mediante la red. Cambiarnos a Firepower nos da una

“Hemos visto una gran mejora en el número de amenazas e IOC bloqueados. Es una diferencia de varios órdenes de magnitud. Antes, nuestro negocio estaba en riesgo cada día que no ejecutábamos Secure Firewall. Ahora tenemos más visibilidad y los riesgos se han reducido inconmensurablemente. Ahora nos sentimos cómodos”.
Gerente de servicios de ingeniería, sector de servicios de TI

mayor visibilidad y capacidad de filtrar el tráfico de red interno, así como el tráfico de norte a sur".

Las mejoras en el bloqueo automatizado también ayudaron a reducir el posible riesgo de una vulneración de seguridad exitosa. El gerente sénior de ingeniería de redes del sector tecnológico señaló que: "Firepower es líder en el sector en Sistemas de Prevención de Ataques [IPS]. Pudimos mejorar nuestra posición de seguridad y solucionar problemas desde un primer momento. Por cada incidente potencial que solucionamos antes, ahorramos dinero". El mismo cliente informó que tuvo una mejora del 80 % en el bloqueo cuando pasó de un sistema con dispositivos ASA a Cisco Secure Firewall.

"Con Secure Firewall, eliminamos un 80 % de nuestras amenazas inmediatamente sin la necesidad de más personal".
Gerente sénior de ingeniería de redes, sector tecnológico

Como algo a destacar, los entrevistados también observaron una mejora en el bloqueo cuando actualizaron sus firewalls FTD a la última versión. El ingeniero sénior de redes de la empresa tecnológica dijo que al actualizarse a la última versión de FTD, les permitió tener entre un 10 % y un 15 % de más bloqueos automatizados que en las versiones anteriores.

Este mismo entrevistado también compartió una anécdota sobre el impacto que el bloqueo automatizado podía tener: "Una vez tuvimos un peligro potencial relacionado con ingeniería social, en el que un hacker consiguió obtener una identificación de acceso de 24 horas de un usuario autenticado. Cuando el hacker intentó usarla [la identificación de acceso], Cisco Secure Firewalls nos salvó. Pudimos comprobar la posición y verificar si el atacante estaba usando una máquina corporativa. Secure Firewall denegó automáticamente el acceso a la VPN al hacker. Sin esto, el hacker habría podido acceder a nuestra red corporativa y no estoy seguro de la gravedad del impacto que habría tenido".

"Cisco Secure Firewall es una solución todo en uno. Tiene todas las capacidades de integración con otras herramientas para ofrecer datos relevantes que contribuyan a la seguridad. Tiene diferentes 'sabores': podemos abordar diferentes requisitos de producción y admite el escalado vertical y horizontal. Tiene toda la funcionalidad necesaria para abordar los riesgos de seguridad actuales y seguir mejorando continuamente".
Ingeniero sénior de redes, internet

El ingeniero sénior de redes de la empresa tecnológica también declaró que un beneficio de seguridad que Secure Firewall proporciona es la capacidad de administrar el acceso a nivel de aplicación: "Estábamos viendo un uso muy grande de BitTorrent en nuestra red de invitados. Al utilizar FTD para bloquear BitTorrent, no solo prevenimos posibles amenazas a otros invitados, sino que también vimos una bajada de unos 400 Mbps en la utilización del circuito".

Además de la detección y bloqueo en la capa de la aplicación, los entrevistados mencionaron que el uso que Cisco Secure Firewall hacía de las fuentes automatizadas de amenazas de Snort también redujo el riesgo para sus organizaciones de que hubiera una vulneración de seguridad exitosa. El ingeniero jefe de infraestructura del sector de los servicios financieros dijo: "Queríamos Cisco Secure Firewall por la visibilidad añadida y la respuesta automática de Snort, que busca elementos como servidores sin parches expuestos a internet y bloquea holísticamente el tráfico malicioso".

Estas organizaciones que aprovecharon la inclusión de SecureX en su licencia de Secure Firewall redujeron todavía más el riesgo y el costo de las vulneraciones de seguridad importantes. Por ejemplo, el ingeniero jefe de infraestructura de la organización de servicios financieros mencionó que SecureX les permitió obtener aún más visibilidad para identificar problemas de seguridad e identificar el origen de las posibles amenazas.

"SecureX nos puede dar una vista única de todo nuestro entorno de seguridad. Con Firewall Management Center, podemos ver todos nuestros firewalls y con SecureX podemos ver Firewall Management Center y todas nuestras soluciones de seguridad de integración de Cisco".
Jefe de equipo de operaciones de seguridad, sector educativo

Modelado y premisas. En el caso de la organización compuesta, Forrester toma el siguiente modelo:

- Un número anterior de vulneraciones de seguridad anuales de 3.
- Los costos combinados internos y externos promedios de una vulneración de seguridad son USD 968.480.
- El porcentaje de ataques externos, incidentes internos y ataques/incidentes que involucran a socios y terceros es del 79 %.
- Cisco Secure Firewall y Firewall Management Center reducen el riesgo de una vulneración de seguridad en un 80 % para el porcentaje de la organización que antes cubrían los firewalls ASA tradicionales.
- Cisco Secure Firewall y Firewall Management Center reducen el riesgo de una vulneración de seguridad en un 15 % para el porcentaje de la organización que antes cubrían los firewalls FTD tradicionales.
- Un 66 % de los empleados de la organización compuesta se ven afectados por cada vulneración de seguridad, por lo que se recupera un 70 % de su productividad gracias a la reducción de riesgo de vulneraciones que ofrece Cisco Secure Firewall y Firewall Management Center.
- La tarifa horaria con todas las prestaciones para empleados generales es de USD 40.

Riesgos. El menor riesgo de una vulneración de seguridad variará en función de los siguientes:

- El número de vulneraciones de seguridad importantes anuales que se sufren ahora.
- Los costos internos y externos totales de una vulneración de seguridad.
- El porcentaje de ataques externos, incidentes internos y ataques/incidentes que involucran a los socios y terceros.
- El tipo y número de firewalls que tienen.
- El número de empleados afectados por una vulneración de seguridad importante, su tarifa horaria con todas las prestaciones y su capacidad de recuperar la productividad cuando se reducen estas vulneraciones de seguridad.

Resultados. Para contemplar estos riesgos, Forrester ajustó este beneficio y lo redujo en un 15 %, lo que dio como resultado un VP total a 3 años ajustado en función del riesgo de cerca de USD 3,5 millones.

Riesgo reducido de vulneraciones de seguridad importantes y pérdida de productividad					
Ref.	**Métrica**	**Fuente**	**Año 1**	**Año 2**	**Año 3**
C1	Número promedio de vulneraciones de seguridad importantes	Forrester Research	3	3	3
C2	Costo promedio por vulneración de seguridad importante	Forrester Research	USD 968.480	USD 968.480	USD 968.480
C3	Porcentaje de ataques externos, incidentes internos y ataques/incidentes que involucran a los socios y terceros	Entrevistas	79 %	79 %	79 %
C4	Porcentaje de la organización que pasa de ASA a Firepower	Organización compuesta	33 %	33 %	33 %
C5	Porcentaje de reducción de riesgos debido a Firepower	Entrevistas	80 %	80 %	80 %
C6	Porcentaje de la organización que pasa de Firepower de primera generación a versión actualizada	Organización compuesta	67 %	67 %	67 %
C7	Porcentaje de reducción de riesgo debido a Firepower actualizado	Entrevistas	15 %	15 %	15 %
C8	Reducción adicional debido a SecureX	Entrevistas	14 %	18 %	23 %
C9	Subtotal: Reducción del riesgo de vulneración de seguridad	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	USD 1.162.951	USD 1.254.763	USD 1.369.528
C10	Número de usuarios afectados por cada vulneración de seguridad	Forrester Research	10.600	10.600	10.600
C11	Tarifa promedio por hora con todas las prestaciones de un empleado general	Organización compuesta	USD 40	USD 40	USD 40
C12	Mejora en la recuperación de productividad	Organización compuesta	70 %	70 %	70 %
C13	Subtotal: Mejora de la productividad gracias a la reducción del riesgo de vulneraciones de seguridad	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8)	USD 356.397	USD 384.534	USD 419.705
Ct	Riesgo reducido de vulneraciones de seguridad importantes y pérdida de productividad	C9+C13	USD 1.519.348	USD 1.639.297	USD 1.789.232
	Ajuste en función del riesgo	↓15 %			
Ctr	Riesgo reducido de vulneraciones de seguridad importantes y pérdida de productividad (ajustado en función del riesgo)		USD 1.291.446	USD 1.393.402	USD 1.520.848
Total a tres años: USD 4.205.696			**Valor presente a tres años: USD 3,468,249**		

BENEFICIOS DE DESEMPEÑO PARA LA PRODUCTIVIDAD DE LOS EMPLEADOS

Pruebas y datos. Cisco Secure Firewall permitió a las organizaciones de los entrevistados mejorar la productividad de los empleados de forma general de dos maneras: 1) visibilidad y control a nivel de la aplicación que mejoró el desempeño de la red; y 2) limitación del tiempo de inactividad debido a las actualizaciones de políticas.

Los entrevistados mencionaron que el desempeño de su red se deterioró con menos frecuencia después de implementar Cisco Secure Firewall gracias a su capacidad de controlar el acceso a la red al nivel de la aplicación.

Antes de esto, los clientes reportaban que sus redes se enlentecían con frecuencia y que el desempeño se deterioraba hasta el punto de afectar la productividad de los empleados cuando había una gran demanda de aplicaciones específicas, especialmente las relacionadas con contenido de videos. El jefe de equipo de operaciones de seguridad del sector educativo dijo: “Aunque la red se enlentecía diariamente de forma notoria, el deterioro era tan grave que afectaba a la productividad una vez cada par de semanas. Esto pasaba principalmente cuando tuvimos una subida repentina de actividad, como cuando miles de usuarios veían un video”.

A medida que Cisco Secure Firewall permitía a las organizaciones de los entrevistados configurar políticas de seguridad de red en varias capas, como la capa de la aplicación, los entrevistados tenían un control más granular sobre los permisos de la red. Como resultado, estas empresas podían controlar mejor a qué y cuándo accedían a sus redes ciertas aplicaciones, lo que evitaba una sobrecarga de redes debido a las aplicaciones que consumen mayor ancho de banda, mejoraba el desempeño de la red e incrementaba la productividad de sus empleados.

“Cisco Secure Firewall nos da una visibilidad mucho mejor de cómo se está usando la red y la capacidad de controlar su uso. Actualmente tenemos 4000 sistemas monitoreados, así que si quisiera, podría ver cuánto se usó [una aplicación social popular basada en videos] la semana pasada. Podríamos rectificar las reglas para prohibir este tipo de tráfico, si así lo quisiéramos”.
Jefe de equipo de operaciones de seguridad, sector educativo

Otros entrevistados dijeron que en sus empresas aumentó la productividad de los empleados al limitar el efecto negativo que a veces creaban los errores humanos en las actualizaciones de políticas. Por ejemplo, el gerente de servicios de ingeniería de la empresa de servicios de TI mencionó que, debido a que era posible crear y actualizar las políticas mucho más rápido con Firewall Management Center, también recibían la confirmación de que las actualizaciones estaban correctas con mayor rapidez.

Antes de que esta empresa implementara Secure Firewall, podían demorar 15 minutos en actualizar una política y otros 15 minutos para saber si estaba configurada correctamente. Si no lo estaba, podían tardar otros 30 minutos en total en actualizar la política una segunda vez.

Ocasionalmente, una política que se actualizó incorrectamente tenía un efecto negativo en la productividad de los empleados, especialmente en ambientes de producción.

Después de actualizar a la última versión de FTD con Cisco Secure Firewall, el gerente de servicios de ingeniería comentó que el hecho de reducir el tiempo que se tardaba en actualizar las políticas a 3 minutos y el tiempo en recibir la confirmación a otros 3 minutos, disminuyó el tiempo total para las actualizaciones, confirmación y solución de problemas en un 80 %: de 60 minutos a 12 minutos.

Modelado y premisas. En el caso de la organización compuesta, Forrester toma el siguiente modelo:

- Se tarda 1 hora entera en arreglar una política actualizada incorrectamente (15 minutos en enviar una actualización incorrecta, 15 minutos en recibir la confirmación, 30 minutos en volver a actualizarla y recibir la confirmación de que se arregló).
- Cisco Secure Firewall y Firewall Management Center reducen el tiempo que se tarda en arreglar políticas incorrectas en un 80 %.
- Se presupone que un 2 % de la organización se ve afectada, en promedio, por actualizaciones de políticas incorrectas.
- La red solía sufrir deterioros serios que perjudicaban la productividad de los empleados en 20 minutos aproximadamente 1 vez cada 2 semanas.
- El 33 % de los empleados a los que solían cubrir los firewalls ASA tradicionales se vieron afectados por el deterioro de la red.

Riesgos. Los beneficios de desempeño para la productividad de los empleados variarán en función de los siguientes:

- El porcentaje de empleados afectados por actualizaciones de políticas incorrectas.
- La frecuencia y duración del deterioro de la red que afecta a la productividad de los empleados.
- El número de empleados afectados por el deterioro de la red.

Resultados. Para contemplar estos riesgos, Forrester ajustó este beneficio y lo redujo en un 10 %, lo que dio como resultado un VP total a 3 años ajustado en función del riesgo de USD 4,1 millones.

Beneficios de desempeño para la productividad de los empleados

Ref.	Métrica	Fuente	Año 1	Año 2	Año 3
D1	Horas anteriores para el ajuste de políticas con FTD de primera generación	Entrevistas	1	1	1
D2	Horas actuales para el ajuste de políticas con FTD actualizados	Entrevistas	0,2	0,2	0,2
D3	Número promedio de empleados afectados	Organización compuesta	320	320	320
D4	Tarifa promedio por hora con todas las prestaciones de un empleado general	C10	USD 40	USD 40	USD 40
D5	Tasa de recuperación de la productividad	Organización compuesta	25 %	25 %	25 %
D6	Subtotal: Mejora en la productividad a partir de la confirmación anterior de políticas	365*(D1-D2)*D3*D4*D5	USD 934.400	USD 934.400	USD 934.400
D7	Frecuencia de deterioro del desempeño debido al abuso de la red	Entrevistas	26	26	26
D8	Duración promedio del deterioro del desempeño en horas	Entrevistas	0,33	0,33	0,33
D9	Número de empleados afectados (solo migraciones de ASA)	Organización compuesta	5280	5280	5280
D10	Tarifa promedio por hora con todas las prestaciones de un empleado general	C11	USD 40	USD 40	USD 40
D11	Tasa de recuperación de la productividad	Organización compuesta	50 %	50 %	50 %
D12	Subtotal: Mejora en la productividad de los empleados que son usuarios finales	D7*D8*D9*D10*D11	USD 906.048	USD 906.048	USD 906.048
Dt	Beneficios de desempeño para la productividad de los empleados	D6+D12	USD 1.840.448	USD 1.840.448	USD 1.840.448
	Ajuste en función del riesgo	↓10 %			
Dtr	Beneficios de desempeño para la productividad de los empleados (ajustado en función del riesgo)		USD 1.656.403	USD 1.656.403	USD 1.656.403
	Total a tres años: USD 4.969.210		**Valor presente a tres años: USD 4.119.230**		

COSTOS REDUCIDOS Y EVITADOS DE SOLUCIONES ANTERIORES

Pruebas y datos. Al migrar su infraestructura de seguridad de red a la última versión de Cisco Secure Firewall, las organizaciones de los entrevistados redujeron y evitaron los costos asociados con la infraestructura de red heredada. No es de sorprender que los entrevistados hayan reportado que se ahorraron costos de readquisición de licencias de sus firewalls ASA tradicionales, así como de los firewalls FTD de primera generación, ya que los firewalls de Cisco Secure Firewall los reemplazaron.

Además de los reemplazos de firewalls físicos y virtuales, las organizaciones de los entrevistados que se cambiaban desde entornos basados en dispositivos ASA, retiraron sus soluciones IPS independientes, ya que Cisco Secure Firewall incluye un IPS.

“Con los firewalls ASA tradicionales, también necesitamos invertir en unidades de IPS que hay que colocar entre los enlaces y el firewall. Con Cisco Secure Firewall, el IPS viene incluido. Ya no necesitamos administrar dos soluciones distintas con dos ecosistemas distintos y no dependemos de ingenieros de IPS”.
Gerente sénior de ingeniería de redes, sector tecnológico

Es importante destacar que los entrevistados tuvieron otros ahorros relacionados con la actualización de los firewalls de sus organizaciones, que pasaron de FTD de primera generación a Cisco Secure Firewall. Debido a la eficiencia de estos nuevos firewalls, los entrevistados declararon que necesitaron entre un 20 % y un 25 % menos para conseguir los mismos resultados.

“Al cambiar de FTD de primera generación a FTD de última generación en Cisco Secure Firewall, observamos una mejor eficiencia de procesamiento. Cisco Secure Firewall ofrece alrededor de entre un 20 % y un 25 % más de eficiencia que las iteraciones anteriores, lo que significa que necesitamos menos firewalls”.
Ingeniero sénior de redes, internet

Modelado y premisas. En el caso de la organización compuesta, Forrester toma el siguiente modelo:

- Reducción de costos de licencia de IPS independientes debido al reemplazo de firewalls tradicionales ASA por firewalls de Cisco Secure Firewall de USD 171.600 anuales.
- Ahorro de costos de mantenimiento para IPS independientes equivalente al 20 % de los costos de licencias.
- Reducción de costos de administración continua debido al IPS del 80 % de 30 minutos para 2 empleados de tiempo completo semanalmente.
- Ahorro de costos de reemplazo de los firewalls existentes con los de un tipo parecido de más de USD 1,3 millones en el primer año.
- Ahorro de costos de reemplazo de los firewalls virtuales de USD 300.000 anuales.
- Ahorro de costos de un 25 % adicional de firewalls físicos gracias a la eficiencia de los firewalls de Cisco Secure Firewall.

“Finalmente retiramos nuestros dispositivos de IPS más costosos y con menor desempeño cuando implementamos Cisco Secure Firewall”.
Ingeniero jefe de infraestructura, servicios financieros

Riesgos. La reducción en costos de soluciones heredadas variará en función de los siguientes:

- El tipo y número de firewalls que tienen.
- La capacidad de retirar soluciones de IPS independientes.

Resultados. Para contemplar estos riesgos, Forrester ajustó este beneficio y lo redujo en un 10 %, lo que dio como resultado un VP total a 3 años ajustado en función del riesgo de casi USD 2,6 millones.

Reducción de los costos por el retiro de soluciones heredadas

Ref.	Métrica	Fuente	Año 1	Año 2	Año 3
E1	Costo reducido de IPS heredado	Entrevistas	USD 171.600	USD 171.600	USD 171.600
E2	Costo reducido de tarifas de mantenimiento	E1*20 %	USD 34.320	USD 34.320	USD 34.320
E3	Costo reducido de administración continua de IPS heredados	Entrevistas	USD 53.539	USD 53.539	USD 53.539
E4	Costos ahorrados de firewalls para el ciclo de reemplazo	Organización compuesta	USD 1.616.980	USD 300.000	USD 300.000
E5	Costos ahorrados por la eficiencia de firewalls adicionales	Organización compuesta	USD 329.245	USD 0	USD 0
Et	Reducción de los costos por el retiro de soluciones heredadas	E1+E2+E3+E4+E5	USD 2.205.684	USD 559.459	USD 559.459
	Ajuste en función del riesgo	↓10 %			
Etr	Reducción de los costos por el retiro de soluciones heredadas (ajustado en función del riesgo)		USD 1.985.115	USD 503.513	USD 503.513
	Total a tres años: USD 2.992.142		**Valor presente a tres años: USD 2,599,074**		

BENEFICIOS NO CUANTIFICADOS

Otros beneficios que observaron los usuarios, pero que no pudieron cuantificar, fueron los siguientes, entre otros:

- **Mejoras en la productividad y seguridad de las VPN.** Los entrevistados también indicaron que Cisco Secure Firewall les permitió tener una mejor productividad y seguridad con las VPN para acceso remoto. Con el balanceo de cargas, Secure Firewall distribuyó las sesiones entre dispositivos agrupados, lo que proporcionó desempeño, resiliencia y productividad a los usuarios finales. De forma parecida, la autenticación local con Secure Firewall permitió a los usuarios seguir siendo productivos si un servidor AAA remoto se hacía inaccesible. En cuanto a seguridad, Cisco Secure Firewall permitía la autenticación con varios certificados, así que las organizaciones pudieron garantizar que un dispositivo remoto pertenecía a la corporación, además de validar al usuario final por ellos mismos.
- **Mejor cumplimiento normativo.** Los entrevistados también dijeron que Cisco Secure Firewall y Firewall Management Center proporcionaron un beneficio no cuantificado con respecto al cumplimiento de flujos de trabajo. El ingeniero jefe de infraestructura de la empresa de servicios financieros compartió que, antes de desplegar Secure Firewall y Firewall Management Center, reportar sobre cumplimiento normativo era más difícil. A las soluciones anteriores les hacía falta una función fácil de reporte. Sin embargo, Secure Firewall y Firewall Management Center permitieron que sus organizaciones crearan reportes que englobaran más los componentes y fueran más detallados en lo que respecta a actividades y visualizaciones. Los entrevistados también mencionaron que Cisco Secure Firewall es compatible con el estándar de cifrado de seguridad de capa de transporte (TLS) 1.3. Por ejemplo, el ingeniero sénior de redes de la empresa de internet señaló que su equipo actualmente no descifraba estos flujos debido a la carga administrativa. Después de invertir en Cisco Secure Firewall, el descifrado de TLS 1.3 fue más fácil y eficiente.

“En el pasado, no teníamos la opción de crear reportes para muchos de los distintos componentes de la configuración, pero ahora podemos obtener reportes amplios y detallados más fácilmente. Por ejemplo, acabo de recibir un reporte de todos los cambios de control del acceso que efectué en el último año. Me muestra el resultado de todas las visitas de páginas y los cambios realizados”.
Ingeniero jefe de infraestructura, servicios financieros

- Mejoras en la **experiencia de los empleados.** Los entrevistados también mencionaron que se mejoró la experiencia de los empleados de sus organizaciones. Por ejemplo, el ingeniero sénior de redes de la empresa de internet dijo: “La capacidad de controlar mejor el acceso a las aplicaciones en nuestras redes mejoró la satisfacción de los empleados. Nuestros equipos locales de TI solían tener dificultades para rastrear a los usuarios a fin de pedirles que dejaran de usar determinadas aplicaciones o para bloquearles el acceso. Con Secure Firewall y Firewall Management Center, ahora podemos hacerlo de forma remota”.

FLEXIBILIDAD

El valor de la flexibilidad es único para cada cliente. Existen múltiples escenarios en los que un cliente podría implementar Secure Firewall y posteriormente incorporar otros usos y oportunidades de negocio, entre ellos:

- **Otras integraciones de seguridad de Cisco.** Además de los beneficios de SecureX, los entrevistados indicaron que el ecosistema de oferta de seguridad de Cisco proporcionaba flexibilidad para reforzar la postura de seguridad de las organizaciones. Por ejemplo, el gerente de servicios de ingeniería de la empresa de servicios de TI dijo: “Cisco Security tiene una gran cantidad de soluciones integradas de seguridad, que es algo que no es fácil para otros proveedores. No es solo Secure Firewall, son todas esas piezas que se integran bien y nos permiten crear nuestras defensas”.
- **Mejores operaciones para trabajar desde casa.** Los controles de Cisco Secure Firewall también ayudaron a que las operaciones siguieran funcionando adecuadamente cuando el uso de las VPN se disparó en el momento en que los empleados hicieron la transición al trabajo desde casa. El ingeniero sénior de redes de la empresa de internet mencionó que: “Durante la pandemia, nuestras conexiones VPN simultáneas pasaron de un promedio de 100.000 a cerca de 350.000 en todo el mundo. Para mantener la viabilidad de nuestra red, usamos Cisco Secure Firewall para establecer límites de velocidad, lo que optimizó las operaciones”.
- **Facilidad de transición a la nube.** Por último, los entrevistados dijeron que Cisco Secure Firewall facilitó el cumplimiento de sus iniciativas de paso a la nube. El gerente de servicios de ingeniería de la organización de servicios de TI dijo: “Necesitábamos una sola plataforma que llegara a la infraestructura local y remota y también a la nube, pero tenía que ser fácil de desplegar. Pues con las plataformas en la nube, solo hay que poner una caja de FTD, instalarla en el momento y conectarla a Firewall Management Center. La instalación y el despliegue no tardan nada. Y podemos enviar una política estandarizada desde estas cajas”.

La flexibilidad también se cuantificaría cuando se evaluara en el marco de un proyecto específico (consulte más detalles en el anexo A).

Análisis de costos

Datos de costos cuantificados aplicados a la organización compuesta

Costos totales

Ref.	Costo	Inicial	Año 1	Año 2	Año 3	Total	Valor presente
Ftr	Costos de licencia	USD 6.000.690	USD 0	USD 0	USD 0	USD 6.000.690	USD 6.000.690
Gtr	Costos de implementación, creación de políticas y capacitación	USD 278.220	USD 7924	USD 7924	USD 7924	USD 301.990	USD 297.924
	Costos totales (ajustados en función del riesgo)	USD 6.278.910	USD 7924	USD 7924	USD 7924	USD 6.302.680	USD 6.298.614

COSTOS DE LICENCIA

Pruebas y datos. Los clientes tuvieron en común que incurrieron en varios costos distintos asociados con su inversión en Secure Firewall, tales como:

- Los costos de firewalls físicos, que variaron en función de la capacidad requerida.
- Los firewalls virtuales desplegados en los centros de datos para que administren el tráfico de este a oeste.
- Los costos de licencias de protección contra amenazas, defensa frente a malware y de filtro de URL.
- Las licencias del Firewall Management Center.

“No fue fácil encontrar otra opción que igualara la profundidad de la arquitectura, el conjunto de herramientas y las características que ofrecía Cisco Secure Firewall en un mismo lugar. Pero además de eso, la relación precio-desempeño también nos convenció”.
Ingeniero jefe de infraestructura, servicios financieros

Los clientes señalaron que pudieron desplegar Cisco SecureX sin ningún costo adicional, ya que estaba incluido en las licencias de Cisco Secure Firewall.

Modelado y premisas. Para la organización compuesta, con 100 oficinas y 4 centros de datos físicos que requieren redundancia, Forrester toma el siguiente modelo:

- Todas las licencias a precios de lista para un término de 3 años.
- El costo de un firewall para la oficina central es de USD 328.443. La oficina central requiere un firewall grande para empresas de gran tamaño con una capacidad de 75 Gbps.
- El costo de los firewalls del centro de datos es USD 978.067. En cada centro de datos, la organización compuesta despliega una agrupación del perímetro del centro de datos o grupo de alta disponibilidad de dos firewalls físicos para administrar el tráfico de norte a sur que entra y sale del centro de datos.
- El costo de 100 firewalls virtuales es USD 2.628.561. Estos firewalls virtuales manejan el tráfico este-oeste al interior del centros de datos y también entre los centros de datos y las plataformas de nubes públicas.
- Todos los firewalls físicos y virtuales en los centros de datos tienen una licencia de protección adicional con una tarifa de suscripción de tres años. Esto proporciona seguridad adicional, que incluye Snort 3, para detectar y mitigar mejor los indicadores de peligro y el tráfico malicioso.

- El costo total de 60 firewalls para las sucursales es de USD 1.848.160. Las 60 oficinas requieren firewalls Secure Firewall con capacidad de hasta 1,9 Gbps.
- El costo total de 39 firewalls para sucursales pequeñas es de USD 137.779. Las 39 oficinas restantes solo requieren una capacidad de hasta 650 Mbps.
- Todos los firewalls de las oficinas tienen licencias adicionales de protección contra amenazas, defensa frente a malware y filtro de URL con una tarifa de suscripción de 3 años.
- Firewall Management Center también tiene una licencia para un tamaño adecuado a fin de administrar todos estos firewalls. El costo de Firewall Management Center es USD 79.680.

Riesgos. Los costos de licencia de Cisco Secure Firewall y Firewall Management Center variarán en función de los siguientes:

- El número de firewalls virtuales deseados.
- El número de firewalls de nivel empresarial requeridos.
- El tamaño y número de centros de datos y la necesidad de disponibilidad alta.
- El tamaño y número de las oficinas sucursales.

Resultados. Dado que Forrester fijó el precio de la organización compuesta directamente con Cisco, este costo no se ha ajustado en función del riesgo y da un VP total a 3 años (descontado al 10 %) de USD 6 millones.

“Con nuestro acuerdo de seguridad de empresa con Cisco, nuestro costo total es más económico que lo que sería todo pedido a la carta. Aunque Firepower equivale a la mayor parte de ese costo, estamos ahorrándonos cientos de miles de dólares para obtener más protección con productos que no teníamos antes”.
Jefe de equipo de operaciones de seguridad, sector educativo

Costos de licencia

Ref.	Métrica	Fuente	Inicial	Año 1	Año 2	Año 3
F1	Costo de firewalls virtuales	Cisco	USD 2.628.561			
F2	Costo de firewall de oficina corporativa	Cisco	USD 328.443			
F3	Costo de los firewalls físicos para el centro de datos	Cisco	USD 978.067			
F4	Costo de firewalls para sucursales pequeñas	Cisco	USD 137.779			
F5	Costo de firewalls para sucursales grandes	Cisco	USD 1.848.160			
F6	Costo de Firewall Management Center	Cisco	USD 79.680			
Ft	Costos de licencia	F1+F2+F3+F4+F5+F6	USD 6.000.690	USD 0	USD 0	USD 0
	Ajuste en función del riesgo	0 %				
Ftr	Costos de licencia (ajustado en función del riesgo)		USD 6.000.690	USD 0	USD 0	USD 0
	Total a tres años: USD 6.000.690			**Valor presente a tres años: USD 6.000.690**		

COSTOS DE IMPLEMENTACIÓN, CREACIÓN DE POLÍTICAS Y CAPACITACIÓN

Pruebas y datos. Los entrevistados indicaron que tuvieron costos internos de tiempo y mano de obra al desplegar e implementar los firewalls en sus centros de datos y oficinas. El primero de estos costos involucró el despliegue físico de firewalls en cada instalación. El segundo costo implicó la implementación de estos firewalls al crear y desplegar las políticas adecuadas en cada grupo de firewalls.

“La implementación y el despliegue fueron muy rápidos y bastante sencillos. El cambio como tal tardó unas tres semanas porque ya teníamos un diseño existente y sabíamos cómo encender todo”.
Jefe de equipo de operaciones de seguridad, sector educativo

Por último, los entrevistados encargados de la toma de decisiones también observaron que hubo costos de tiempo relacionados con la capacitación. La capacitación tomó 2 horas para todos los empleados que lo necesitaran para desplegar y administrar Cisco Secure Firewalls. Algunos entrevistados mencionaron que aprovecharon los videos de capacitación disponibles públicamente con los expertos de seguridad de Cisco.

Modelado y premisas. En el caso de la organización compuesta, Forrester toma el siguiente modelo:

- En promedio, se necesitaron 6 horas de implementación en cada uno de los 2 centros de datos y 100 oficinas.
- En promedio, la creación de políticas tarda 30 horas por firewall.
- La implementación de SecureX requiere 20 horas de trabajo anticipado y 100 horas anuales más para su administración continua.
- Hubo 15 empleados que necesitaron capacitación inicialmente y 3 más que necesitaron capacitarse cada año debido a la rotación de empleados.

Riesgos. El costo de la implementación y la creación de políticas variará en función de:

- El número de firewalls de Cisco Secure Firewall a desplegar.
- El número de empleados que necesitan capacitarse inicialmente.
- El ritmo de rotación de empleados.
- La tarifa horaria con todas las prestaciones de los profesionales de NetSecOps.

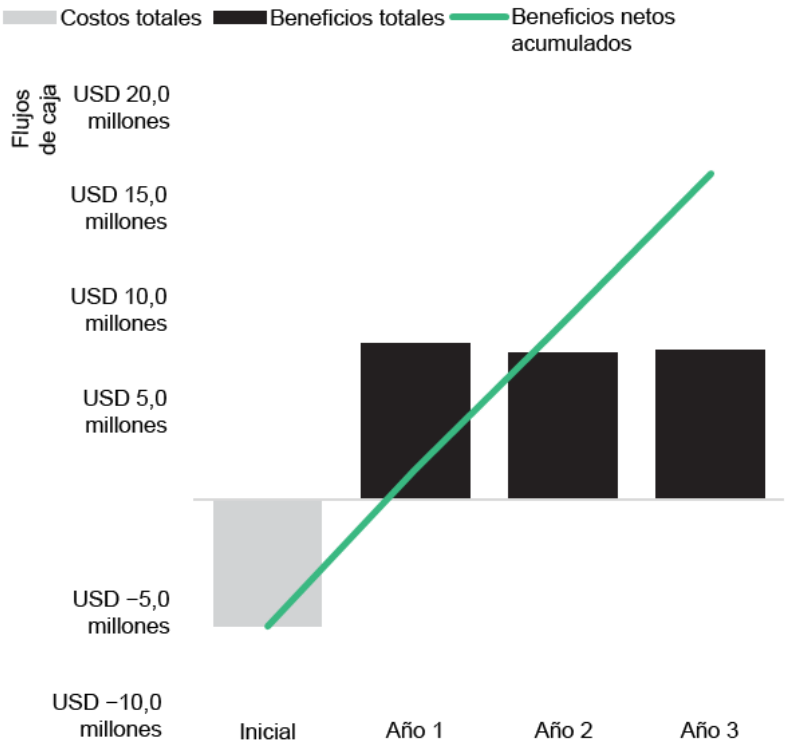
Resultados. Para tener en cuenta estos riesgos, Forrester ajustó este costo al alza en un 15 %, lo que dio lugar a un VP total, ajustado en función del riesgo a 3 años, de menos de USD 298.000.

Costos de implementación, creación de políticas y capacitación						
Ref.	**Métrica**	**Fuente**	**Inicial**	**Año 1**	**Año 2**	**Año 3**
G1	Instalaciones donde se desplegará	Organización compuesta	102			
G2	Horas promedio para la implementación física en cada instalación	Organización compuesta	6			
G3	Horas de creación de políticas	Entrevistas	30			
G4	Horas de implementación y administración de SecureX	Entrevistas	20	100	100	100
G5	Empleados que necesitan capacitación	Entrevistas	15	3	3	3
G6	Horas necesarias para capacitación	Entrevistas	2	2	2	2
G7	Tarifa horaria con todas las prestaciones de profesionales de NetSecOps	A5	USD 65	USD 65	USD 65	USD 65
Gt	Costos de implementación, creación de políticas y capacitación	((G1*(G2+G3))+,G4+(G5*G6))*G7	USD 241.930	USD 6.890	USD 6.890	USD 6.890
	Ajuste en función del riesgo	↑15 %				
Gtr	Costos de implementación, creación de políticas y capacitación (ajustados al riesgo)		USD 278.220	USD 7924	USD 7924	USD 7924
Total a tres años: USD 301.990			**Valor presente a tres años: USD 297.924**			

Resumen financiero

MÉTRICAS A TRES AÑOS CONSOLIDADAS AJUSTADAS EN FUNCIÓN DEL RIESGO

Gráfico de flujos de caja (ajustados en función del riesgo)



Los resultados financieros calculados en las secciones Beneficios y Costos pueden utilizarse para determinar el ROI, el VPN y el período de amortización de la inversión de la organización compuesta. Para este análisis, Forrester supone un porcentaje de descuento anual del 10 %.

Los valores relativos al ROI, el VPN y el período de amortización se determinan aplicando factores de ajuste en función del riesgo a los resultados no ajustados de las secciones de Beneficios y Costos.

Análisis de flujos de caja (cálculos ajustados en función del riesgo)

	Inicial	Año 1	Año 2	Año 3	Total	Valor presente
Costos totales	(USD 6.278.910)	(USD 7.924)	(USD 7.924)	(USD 7.924)	(USD 6.302.680)	(USD 6.298.614)
Beneficios totales	USD 0	USD 7.737.795	USD 7.264.360	USD 7.391.805	USD 22.393.959	USD 18.591.534
Beneficios netos	(USD 6.278.910)	USD 7.729.871	USD 7.256.436	USD 7.383.881	USD 16.091.279	USD 12.292.920
ROI						195 %
Plazo de amortización (meses)						10

Anexo A: Total Economic Impact

Total Economic Impact (TEI) es una metodología desarrollada por Forrester Research que permite mejorar los procesos de toma de decisiones tecnológicas de las empresas y ayuda a los proveedores a comunicar a sus clientes la propuesta de valor de sus productos y servicios. La metodología TEI ayuda a las empresas a demostrar, justificar y materializar el valor tangible de las iniciativas informáticas, tanto para la alta dirección como para otras partes implicadas clave de las entidades.

MÉTODO TOTAL ECONOMIC IMPACT

Los **beneficios** representan el valor que el producto ofrece a la empresa. El método TEI asigna el mismo valor al cálculo de los beneficios y los costos, lo que permite obtener una evaluación completa del efecto de la tecnología en toda la empresa.

Los **costos** abarcan todos los gastos necesarios para generar el valor propuesto o los beneficios del producto. La categoría de costos de TEI incluye los costos graduales sobre el entorno existente para los gastos continuados asociados a la solución.

La **flexibilidad** representa el valor estratégico que puede obtenerse de una inversión adicional futura que se realice sobre la inversión inicial ya realizada. Poder aprovechar dicho beneficio presenta un VP susceptible de cálculo.

Los **riesgos** determinan la incertidumbre en los cálculos de beneficios y costos habida cuenta de: 1) la probabilidad de que los cálculos de costos y beneficios se ajusten a las previsiones iniciales y 2) la probabilidad de que se haga un seguimiento de los cálculos a lo largo del tiempo. Los factores de riesgo del método TEI se basan en una “distribución triangular”.

La columna de inversión inicial contiene los costos incurridos en el “momento 0” o al comienzo del primer año; estos costos no se descuentan. El resto de los flujos de caja se descuentan usando la tasa de descuento al final del año. El valor presente (VP) se calcula para cada estimación de costos y beneficios totales. Los cálculos del VPN en las tablas resumidas representan la suma de la inversión inicial y los flujos de caja descontados en cada año. Las sumas y los cálculos del valor presente de las tablas Beneficios totales, Costos totales y Flujo de caja podrían no sumar 100 exactamente como consecuencia del redondeo.

VALOR PRESENTE (VP)

Valor presente o actual de las estimaciones de costos y beneficios (descontadas), dado un tipo de interés (tasa de descuento). El VP de costos y beneficios alimenta al valor actual neto total de los flujos de caja.

VALOR PRESENTE NETO (VPN)

Valor presente o actual de los futuros flujos de caja netos (descontados), dado un tipo de interés (tasa de descuento). Un VPN positivo en un proyecto suele indicar que se debe realizar la inversión, a menos que otros proyectos tengan valores presentes netos más elevados.

RETORNO DE LA INVERSIÓN (ROI)

El retorno previsto de un proyecto expresado en porcentaje. El ROI se calcula dividiendo los beneficios netos (beneficios menos costos) entre los costos.

TASA DE DESCUENTO

El tipo de interés que se utiliza en el análisis de los flujos de caja para reflejar el valor del dinero en el tiempo. Las empresas suelen utilizar tasas de descuento de entre el 8 % y el 16 %.

PLAZO DE AMORTIZACIÓN

El punto de equilibrio de una inversión. El punto en el tiempo en el que los beneficios netos (beneficios menos costos) son iguales a la inversión o el costo inicial.

Anexo B: Notas finales

[1] Total Economic Impact (TEI) es una metodología desarrollada por Forrester Research que permite mejorar los procesos de toma de decisiones tecnológicas de las empresas y ayuda a los proveedores a comunicar a sus clientes la propuesta de valor de sus productos y servicios. La metodología TEI ayuda a las empresas a demostrar, justificar y materializar el valor tangible de las iniciativas informáticas, tanto para la alta dirección como para otras partes implicadas clave de las entidades.

FORRESTER®