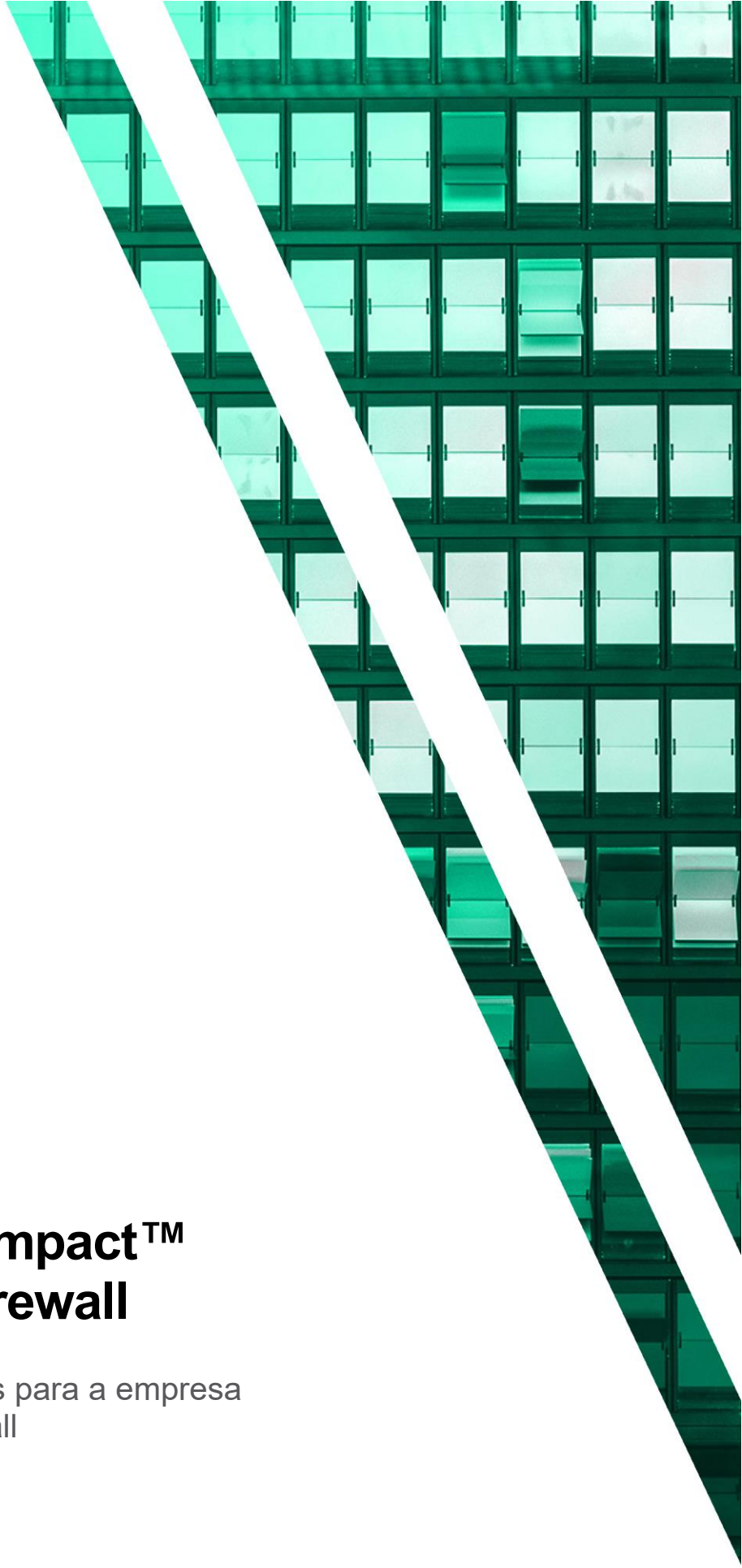
FORRESTER®



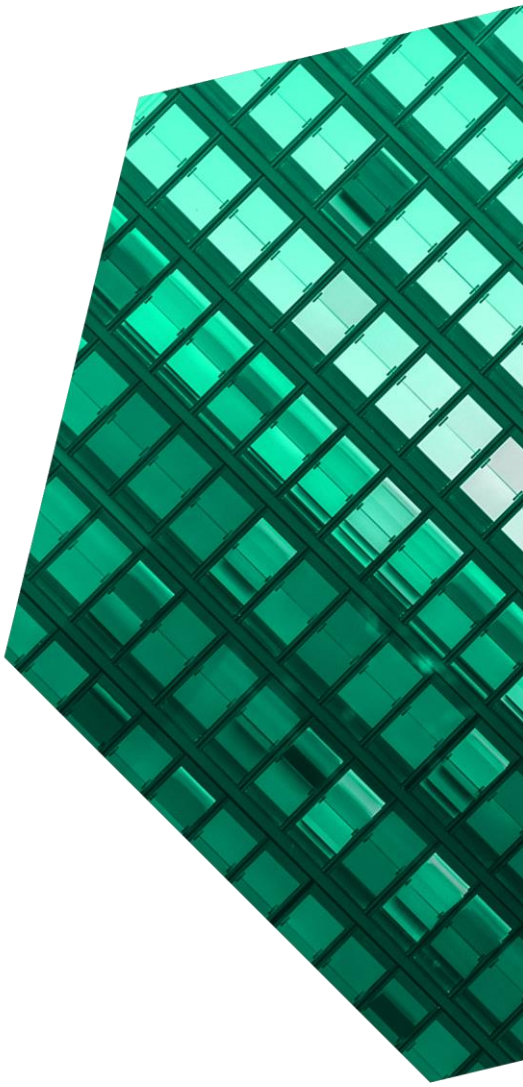
O Total Economic Impact™ da Cisco Secure Firewall

Redução de custos e vantagens para a empresa
Viabilizados pela Secure Firewall

MARÇO DE 2022

Índice

Equipa de consultoria: *Henry Huang*
Nick Mayberry



SOBRE A FORRESTER CONSULTING

A Forrester Consulting presta consultoria independente e objetiva com base em pesquisa para ajudar líderes empresariais a terem sucesso nas suas organizações. Para obter mais informações, aceda a forrester.com/consulting.

Resumo Executivo

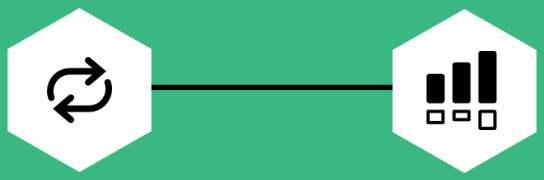
A Cisco Secure Firewall e o Firewall Management Center melhoram a visibilidade e o controlo das organizações sobre a segurança da sua rede. As organizações dos entrevistados pouparam até 95% de trabalho de profissionais de redes relacionado com firewalls e até 83% de trabalho de profissionais de segurança. Também reduziram o risco de uma intrusão material até 80%, ao mesmo tempo que melhoraram a produtividade do utilizador final, através da minimização da perturbação da rede e do VPN. A postura relativa a segurança melhorou mesmo reduzindo a implementação da firewall em 25%.

A Cisco Secure Firewall é uma solução de segurança de rede, layer 7, de próxima geração que protege as organizações contra ameaças externas e internas, enquanto alivia a sobrecarga das equipas de redes e segurança tanto para a gestão da firewall como das ameaças. As organizações podem gerir a Cisco Secure Firewall com o Firewall Management Center (FMC), uma gestão centralizada para defesa de ameaças e administração da firewall, que confere às equipas de redes e segurança visibilidade acrescida numa perspetiva holística unificada, mesmo na camada da aplicação e das ameaças detetadas no tráfego encriptado. Além disso, proporciona um controlo acrescido com o sistema de prevenção de intrusão (IPS) Snort 3 e de otimização de software para filtragem de URL e defesa contra malware.

A licença Cisco Secure Firewall inclui o uso da SecureX, a plataforma integrada da Cisco que permite às organizações consolidar dados das ameaças a partir do portfólio Cisco Secure e de ferramentas de segurança de terceiros, numa vista global única dos dados contextualmente enriquecidos concebida para facilitar a investigação e resposta rápidas.

A Cisco encomendou à Forrester Consulting a realização de um estudo Total Economic Impact™ (TEI) e a análise do potencial retorno do investimento (ROI) que as empresas podem realizar com a implementação da Secure Firewall.[1] O objetivo deste estudo é facultar aos leitores uma estrutura para avaliar o potencial impacto financeiro da Secure Firewall nas suas organizações.

PRINCIPAIS ESTATÍSTICAS



Retorno do investimento (ROI)
195%

Valor atual líquido (NPV)
$12,29 M

Para melhor compreender os benefícios, custos e riscos associados a este investimento, a Forrester entrevistou dez decisores em oito organizações com experiência de utilização da Secure Firewall. Para efeitos deste estudo, a Forrester agregou as experiências dos entrevistados e combinou os resultados numa única organização composta.

Antes de utilizar a Secure Firewall, estes entrevistados referiram como as suas organizações careciam de visibilidade e capacidade de gestão necessária para administrar adequadamente e proteger eficazmente as suas redes. Sem esta visibilidade e uma interface gráfica de utilizador (GUI) eficiente, os entrevistados referiram que os fluxos de rede, como a implementação da firewall, criação de políticas, atualizações da firewall e atualizações das políticas demoravam bastante tempo. Foi concedido tempo adicional aos fluxos de trabalho de segurança, como a investigação e resposta a ameaças e administração através do acesso remoto. Os entrevistados também referiram o fraco desempenho da rede durante os períodos de elevada procura e as complicações com a gestão de múltiplos fornecedores.

Depois do investimento na Secure Firewall, os entrevistados não só reduziram o tempo necessário para obter os resultados dos fluxos de rede e de segurança mencionados acima, como também melhoraram a segurança global das suas organizações. Ao mesmo tempo, as organizações melhoraram a produtividade dos funcionários com atualizações mais rápidas das políticas, inspeção melhorada do tráfego de rede e melhoria global do desempenho de rede, ao mesmo tempo que era realizada a desativação das soluções antigas e eliminados muitos dos custos associados ao tempo gasto na gestão.

Benefícios totais

$18,6 milhões

PRINCIPAIS CONCLUSÕES

Benefícios quantificados. O valor atual (PV) dos benefícios quantificados ajustado ao risco inclui:

- **Fluxos de trabalho de operação da rede reduzidos até 95%.** Graças às mais recentes funcionalidades da Cisco Secure Firewall e à facilidade de gestão através do Firewall Management Center, as organizações dos entrevistados reduziram o tempo a:
  - implementar uma firewall em 36%
  - atualizar uma firewall em 90%
  - atualizar as políticas da firewall em 95%, em comparação com as firewalls Adaptive Security Appliances (ASA) 5500-X tradicionais
  - atualizar as políticas das firewall em 80%, em comparação com versões anteriores das políticas com base na Firewall Threat Defense (FTD)
  - atualizar firewalls virtuais em 80%.
- **Redução do tempo do fluxo de trabalho de resposta e investigação de segurança até 83%.** Os entrevistados também referiram poupanças substanciais no trabalho dos profissionais de segurança decorrentes da combinação da Cisco Secure Firewall e Firewall Management Center em que a informação era melhor organizada para consumo e análise. Os entrevistados referiram a redução do tempo de investigação de potenciais ameaças em 49% e do tempo de resposta a ameaças em 83%. Usando o SecureX em conjunto com a Secure Firewall e o FMC permitiu às organizações poupar até 77% do tempo restante na investigação e resposta.

"Prestamos muita atenção à segurança e queremos alavancar os produtos para proteger a empresa. Foi por isso que escolhemos a Cisco. Cresceram na segurança. Para eles, a segurança não é apenas um add-on."
Engenheiro de redes sénior, fabrico

- **Redução do risco de intrusão em 80%.** A visibilidade e controlo combinados proporcionados pela Cisco Secure Firewall e pelo Firewall Management Center possibilitaram às organizações dos entrevistados reduzir o risco de potenciais intrusões materiais e os custos que lhes estão associados. Estas soluções reduziram o risco de uma intrusão em 80%, em comparação com as firewalls ASA 5500-X tradicionais e em 15% em comparação com firewalls com base em FTD. A SecureX permitiu à organização dos entrevistados reduzir o risco remanescente e os custos de uma intrusão até mais 23%.

- **Aumento da produtividade do utilizador final avaliada em aproximadamente $2 milhões anualmente.** A implementação da Cisco Secure Firewall e do Firewall Management Center melhorou a produtividade das organizações dos entrevistados de duas formas. Primeiro, possibilitou que os profissionais de rede resolvessem erros de atualização de políticas disruptivas 80% mais rápido. Segundo, reduziu a gravidade da degradação do desempenho de rede, devolvendo quase 9 horas de trabalho, anualmente, a cada utilizador final afetado.
- **Reduziu os custos com as ferramentas antigas desativadas.** Os entrevistados também referiram que a Cisco Secure Firewall lhes permitiu desativar soluções de segurança antigas e dispendiosas que tinham implementado anteriormente. Os entrevistados referiram poupar centenas de milhares de dólares anualmente em IPS autónomos, milhões de dólares a evitar o custo de substituição das suas soluções de segurança atuais e outros 25% de custos dado que a Cisco Secure Firewall proporciona o mesmo nível de proteção com menos firewalls.

Benefícios não quantificados. Os benefícios não quantificados para este estudo incluem:

- **Produtividade do VPN e melhorias de segurança.** A Cisco Secure Firewall também permitiu melhor produtividade e segurança com o acesso remoto VPN através de load balancing, autenticação local e autenticação usando múltiplos certificados. Os utilizadores finais também estabeleceram melhores ligações por VPN enquanto as organizações conseguiram melhor controlo do acesso.
- **Operações melhoradas para o trabalho a partir de casa.** Os controlos da Cisco Secure Firewall também ajudaram a manter as operações em bom funcionamento quando o uso do VPN explodiu aquando da transição dos funcionários para o trabalho a partir de casa. Os profissionais de redes podem alavancar a limitação do débito e melhoramentos na redundância para melhorar a experiência e a produtividade dos funcionários mesmo nos picos da procura.
- **Facilidade de transição para a nuvem.** Por último, os entrevistados partilharam que a Cisco Secure Firewall tornou as suas iniciativas na nuvem mais fáceis de alcançar, ao facultar uma plataforma que protege o tráfego dentro dos locais, entre locais e entre a organização e múltiplas plataformas na nuvem. Especificamente, a Cisco oferece políticas padronizadas e meios validados para implementação da Secure Firewall através de marketplaces de plataformas na nuvem.

Custos. Os custos PV ajustados ao risco incluem:

- **Custos de licenciamento.** Embora os custos de licenciamento fossem os custos mais elevados incorridos pelas organizações dos entrevistados, a celebração do Contrato Cisco Enterprise poupou centenas de milhares de dólares em funcionalidades e soluções adicionais que as organizações careciam antes, mas melhorou a postura de segurança da organização. O direito à licença SecureX está incluída com a Secure Firewall.
- **Custos de implementação, criação de políticas e formação.** Os entrevistados referiram ter custos internos para a implementação das firewalls e para a criação de políticas para as mesmas. Estima-se que a implementação da firewall demore 6 horas por local, enquanto se espera que a criação da política demore 30 horas. A SecureX requer 20 horas de trabalho adicionais para implementar e 100 horas anualmente para a gestão numa base contínua. Alguns entrevistados referiram também a necessidade de dar formação aos seus profissionais de redes e segurança para o uso da Cisco Secure Firewall e do Firewall Management Center. Os custos internos de formação ascenderam a 2 horas por funcionário formado, tendo os entrevistados referido ter aproveitado os vídeos de formação feitos por especialistas em segurança da Cisco e que são do domínio público.

As entrevistas e a análise financeira dos decisores concluíram que a organização composta tem benefícios de $18,59 milhões ao longo de três anos versus custos de $6,3 milhões, o que soma uma valor atual líquido (NPV) de $12,29 milhões e um ROI de 195%.

ROI
195%

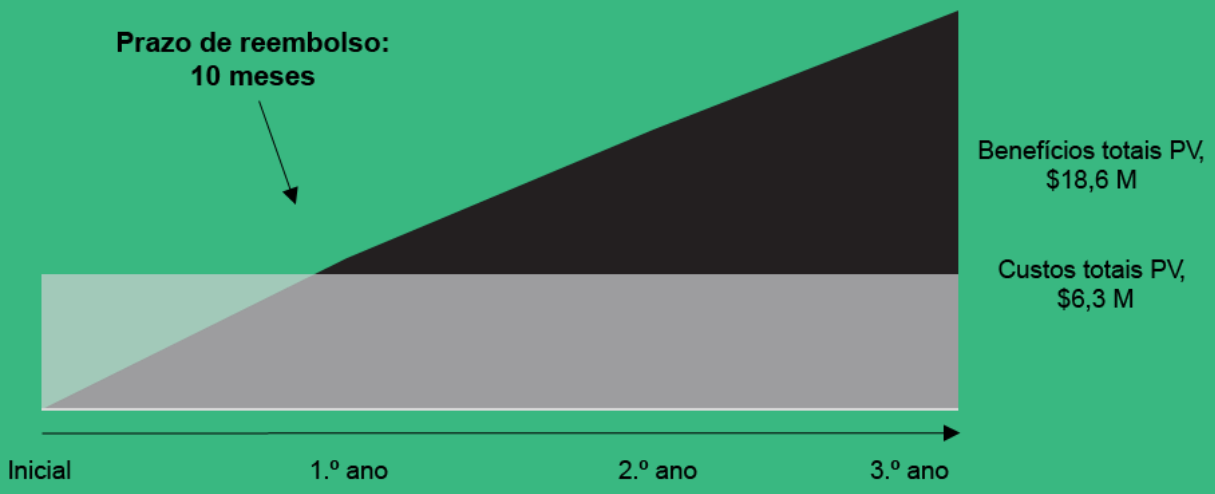
PV DOS BENEFÍCIOS
$18,59 M

VALOR ATUAL LÍQUIDO
$12,29 M

RETORNO
10 meses

Benefício (três anos)

Resumo financeiro



ESTRUTURA E METODOLOGIA DO TEI

A partir da informação prestada nas entrevistas, a Forrester criou uma estrutura do Total Economic Impact™ para as organizações que estejam a considerar um investimento na Cisco Secure Firewall.

O objetivo da estrutura é identificar o custo, benefício, flexibilidade e fatores de risco que afetam a decisão de investimento. A Forrester optou por um abordagem com múltiplos passos para avaliar o impacto que a Secure Firewall pode ter numa organização.

CONSIDERAÇÕES

Os leitores devem estar cientes do seguinte:

este estudo foi encomendado pela Cisco e é realizado pela Forrester Consulting. Não se destina a ser utilizado para fins de análise concorrencial.

A Forrester não faz estimativas quanto ao potencial retorno do investimento (ROI) que outras organizações possam vir a ter. A Forrester recomenda vivamente que os leitores usem as suas próprias estimativas dentro da estrutura constante do relatório para determinar a adequação de um investimento na Secure Firewall.

A Cisco reviu e deu feedback à Forrester, mas a Forrester mantém o controlo editorial sobre o estudo e as suas conclusões e não aceita alterações ao estudo que contradigam as conclusões da Forrester ou ocultem o significado do estudo.

A Cisco facultou os nomes dos clientes para as entrevistas, mas não participou nas entrevistas.

DUE DILIGENCE
Entrevistou partes interessadas da Cisco e analistas da Forrester a fim de recolher dados relativos à Secure Firewall.

ENTREVISTAS AOS DECISORES
Entrevistou dez decisores em organizações que usam a Secure Firewall para obter dados referentes a custos, benefícios e riscos.

ORGANIZAÇÃO COMPOSTA
Concebeu uma organização composta com base nas características das organizações dos entrevistados.

ESTRUTURA DO MODELO FINANCEIRO
Construiu um modelo financeiro representativo das entrevistas usando a metodologia TEI e ajustou o risco do modelo financeiro com base nos problemas e preocupações dos decisores.

CASO DE ESTUDO
Empregou quatro elementos fundamentais do TEI na modelação do impacto do investimento: benefícios, custos, flexibilidade e riscos. Dada a crescente sofisticação das análises do ROI relativas aos investimentos em TI, a metodologia TEI da Forrester oferece uma imagem completa do impacto económico total das decisões de aquisição. Consulte o Apêndice A para informação adicional sobre a metodologia TEI.

Percurso do cliente Cisco Secure Firewall

Motivadores que levam ao investimento na Secure Firewall

Decisores entrevistados

Entrevistado	Indústria	Região	Total de funcionários
Gestor de serviços de engenharia	Serviços de TI	América do Norte	750
Engenheiro chefe de infraestrutura	Serviços financeiros	América do Norte	2800
Gestor adjunto dos serviços de telecomunicações e telefonia	Serviços financeiros	América do Norte	2800
Engenheiro principal de cibersegurança	Serviços de segurança	América do Norte	3000
Engenheiro de redes sénior	Fabrico	Global	5500
Gestor sénior de engenharia de redes	Tecnologia	Global	40 000
Engenheiro de segurança sénior	Tecnologia	Global	40 000
Chefe de equipa de operações de segurança	Ensino	América do Norte	46 000
Arquiteto de infraestruturas interno	Industrial	Global	205 000
Engenheiro de redes sénior	Tecnologia	Global	275 000

PRINCIPAIS DESAFIOS

Antes de implementar a Cisco Secure Firewall e o Firewall Management Center, as organizações dos entrevistados estavam maioritariamente a utilizar a firewall baseada na ASA 5500-X tradicional para proteger os seus ambientes. Alguns entrevistados tinham feito a troca das firewalls baseadas em ASA para as firewalls baseadas em FTD anteriores, uns anos antes, e referiram ter tido benefícios adicionais depois de fazerem a atualização para a versão mais recente da FTD no Cisco Secure Firewall e no Firewall Management Center.

Os entrevistados referiram como as suas organizações se debatiam com problemas comuns, incluindo:

- **Visibilidade limitada.** Os entrevistados referiram que os ambientes anteriores que dependiam de firewalls baseadas na ASA 5500-X proporcionavam visibilidade limitada sobre a sua segurança global. Um dos culpados era a falta de integração. Nos ambientes anteriores, as organizações dos entrevistados tinham dificuldade em integrar diversas soluções de segurança para o estabelecimento de uma gestão unificada e de políticas consistentes, enquanto também obtinham uma versão consolidada. Outra razão para a visibilidade limitada era que os ambientes anteriores dependiam de inspeções de portas como perspetiva principal para a rede. Os entrevistados referiram que isto os impedia de ter uma visão mais profunda dos dados com visibilidade limitada das aplicações e contexto histórico limitado.

> **"Anteriormente carecíamos de capacidades como o controlo de aplicações modernas. Não podíamos dizer como os nossos utilizadores usavam a rede e não podíamos responder a esta utilização adequadamente."**
> *Chefe de equipa de operações de segurança, ensino*

- **Custos elevados no que se refere ao tempo despendido na implementação e gestão das firewalls.** Os entrevistados também referiram que a implementação e a gestão das suas firewalls antigas eram morosas. Isto devia-se maioritariamente à falta de capacidade de fazer atualizações de diversos dispositivos ao mesmo tempo. O chefe da equipa de operações de segurança do setor da educação estimou que costuma demorar entre 45 minutos e uma hora a implementar uma simples regra da firewall. Adicionalmente, os entrevistados referiram que a falta de visibilidade dos ambientes anteriores significava que estavam a gastar um tempo desmesurado a correlacionar dados entre os diferentes sistemas para confirmar as posturas de segurança.

"A facilidade de administração e integração tem sido uma das vantagens da Cisco. Também beneficiamos do enriquecimento dos dados que os diferentes sistemas fornecem mais facilmente entre si. Também estabelecemos respostas autónomas a certas ameaças. Não podíamos fazer nada disto anteriormente."
Engenheiro principal de segurança, serviços de segurança

- **Fraco desempenho.** Os entrevistados também referiam que os seus sistemas anteriores tinham fraco desempenho. Por exemplo, o chefe da equipa de operações de segurança do setor do ensino referiu que quando a procura na sua infraestrutura de rede e segurança disparou, as soluções anteriores teriam "caído, reiniciando constantemente devido ao congestionamento da rede." Isto foi tão longe, que teve impacto na produtividade, como "os professores a não conseguirem utilizar a rede para reproduzir um vídeo ou demonstrar algo na aula."

- **Gestão de fornecedores.** Por último, os clientes referiram que ter múltiplos fornecedores no seu ambiente anterior criava dificuldades na gestão de fornecedores. O engenheiro chefe de infraestruturas da empresa de serviços financeiros referiu "Com múltiplos fornecedores, tudo tinha de ser feito várias vezes, acedendo a múltiplos planos de controlo para aplicar as mesmas alterações ou atualizações através de sistemas díspares."

ORGANIZAÇÃO COMPOSTA

Com base nas entrevistas, a Forrester elaborou a estrutura TEI, uma empresa composta e uma análise do ROI que ilustra as áreas afetadas financeiramente. A organização composta é representativa dos nove decisores que a Forrester entrevistou e é usada para apresentar a análise financeira agregada na próxima secção. A organização composta tem as seguintes características:

Descrição da organização composta. A organização composta é uma organização de tecnologia B2B com $5 mil milhões em receitas anuais e 16 000 funcionários. Serve clientes a nível global. A organização necessita de uma elevada disponibilidade nos seus data centers para garantir acesso aos seus dados ali armazenados. Estes data centers também requerem um aumento de segurança para proteger dados confidenciais do cliente de acesso ou ataque indesejados. Para além dos data centers, a organização está a fazer a transição para uma abordagem mais descentralizada com a utilização de múltiplas nuvens. Além disso, a organização está também a utilizar as Secure Firewalls para proteger os seus locais principais/escritórios das filiais.

Características da implementação. A organização composta já investiu em firewalls Cisco da próxima geração. Dois terços do seu stock de firewalls é composto por dispositivos Cisco Firepower, enquanto um terço é composto por firewalls ASA 5500-X. Está agora a fazer a transição das suas 102 firewalls dos escritórios domésticos, data center e do escritório para a última versão da Cisco Secure Firewall, atualizando os seus 68 dispositivos Firepower e substituindo os seus 34 dispositivos baseados em ASA.

Alguns entrevistados optaram por atualizar os dispositivos tradicionais existentes para software FTD sem alterar o hardware. Também implementa as firewalls virtuais Cisco Secure Firewall nos seus data centers para lidar com o tráfego este-oeste entre os data centers e os escritórios das filiais, bem como o tráfego entre data centers e múltiplas plataformas públicas de nuvem. Aproveita a inclusão da SecureX na sua licença Secure Firewall para melhorar ainda mais o trabalho da equipa de segurança na investigação e resposta a ameaças.

Principais pressupostos

- **$5 mil milhões em receitas**
- **16 000 funcionários**
- **Substituição de 34 firewalls com base em ASA**
- **Atualização de 68 firewalls Firepower para a mais recente Cisco Secure Firewall**

Análise dos benefícios

Dados dos benefícios quantificados conforme aplicados à organização composta

Benefícios totais

Ref.	Benefício	1.º ano	2.º ano	3.º ano	Total	Valor atual
Atr	Melhorias na gestão da firewall	$134 951	$25 556	$25 556	$186 064	$163 005
Btr	Melhorias nos fluxos de segurança	$2 669 879	$3 685 484	$3 685 484	$10 040 848	$8 241 976
Ctr	Reduzido risco de intrusão material e de perda de produtividade	$1 291 446	$1 393 402	$1 520 848	$4 205 696	$3 468 249
Dtr	Benefícios do desempenho para a produtividade dos funcionários	$1 656 403	$1 656 403	$1 656 403	$4 969 210	$4 119 230
Etr	Custos reduzidos das soluções legadas desativadas	$1 985 115	$503 513	$503 513	$2 992 142	$2 599 074
	Benefícios totais (ajustados ao risco)	$7 737 795	$7 264 360	$7 391 805	$22 393 959	$18 591 534

MELHORIAS NA GESTÃO DA FIREWALL

Evidência e dados. Os decisores entrevistados referiram a poupança de tempo e de custos relacionados com a gestão de firewalls, depois da implementação da Cisco Secure Firewall, independentemente de estarem a fazer a troca de firewalls antigas ou a atualização de versões anteriores da Firepower Threat Defense. Uma boa parte destas melhorias decorreram do facto de o Firewall Management Center ter ajudado os profissionais de redes ao disponibilizar uma gestão centralizada das firewalls através de um painel de controlo único que lhes permitiu ativar alterações em muitos dispositivos.

"A FMC oferece-nos um lugar para gerir e atualizar firewalls, em vez de andar a saltar entre diferentes firewalls como fazíamos anteriormente."
Gestor de serviços de engenharia, serviços de TI

As organizações dos entrevistados partilharam a poupança de tempo e de custos relacionados com a implementação da firewall. Com as firewalls baseadas em ASA tradicionais, os entrevistados referiram que a implementação da firewall tinha levado muito tempo, exigindo a escrita de regras de firewall específicas para o caso usado e a distribuição manual através do conjunto diversificado de políticas de firewall em vigor.

"A Cisco Secure Firewall permitiu-nos lançar e implementar novas firewalls. Não tivemos de dar formação aos funcionários à medida que desenvolvíamos as firewalls."
Gestor sénior da engenharia de redes, tecnologia

Depois da troca para a Cisco Secure Firewall e o Firewall Management Center, os entrevistados notaram uma poupança entre 30% e 40% no tempo necessário para a implementação das firewalls. A redução do tempo necessário foi atribuída à capacidade de automatizar a

implementação da Cisco Secure Firewall. Por exemplo, o gestor sénior de engenharia de redes do setor de tecnologia afirmou: “Automatizámos a implementação com a Cisco Secure Firewall. Temos processos automatizados para retirar da caixa, configurar o IP, configurar o chassis e aplicar a política.”

“A automatização integrada poupa-nos muito tempo. Mesmo no caso das atualizações. Já não tenho de ficar à espera e de estar atento ao processo de atualização, como acontecia com as ASAs. Posso afastar-me e o Firepower avisa-me se não voltar a ficar online em devido tempo.”
Gestor sénior da engenharia de redes, tecnologia

A automatização também ajudou os entrevistados relativamente à gestão e manutenção das suas Cisco Secure Firewalls após a implementação. A Cisco Secure Firewall inclui atualizações automatizadas integradas Os entrevistados reportaram que a atualização das firewalls baseadas em ASA podia levar várias horas, indo de firewall para firewall, carregando os ficheiros de atualização e reiniciando os sistemas. Ao usar a Cisco Secure Firewall a Firewall Management Center, os entrevistados reportaram que bastava clicar na interface para atualizar as firewalls e verificar decorridos 30 minutos para ver se as atualizações se encontravam concluídas.

“Estamos a assistir a 60% a 70% de poupança em horas extraordinárias na gestão de políticas depois de mudar da ASA para a Cisco Secure Firewall.”
Gestor de serviços de engenharia, serviços de TI

Com a Cisco Secure Firewall e o Firewall Management Center, os entrevistados referiram que as políticas podiam ser organizadas em categorias e zonas sem necessidade de listas de controlo de acesso longas (ACLs) usando um sistema orientado para o objeto. Agora as políticas podiam também ser implementadas automaticamente e atualizadas, em contraste com a atualização manual de cada dispositivo.

“A Cisco Secure Firewall autoimplementa 90% da política por si. Já não temos de lidar com configurações isoladas.”
Gestor sénior da engenharia de redes, tecnologia

Os entrevistados referiram poupanças de tempo adicionais depois de atualizar da FTD inicial para a FTD mais recente com o Cisco Secure Firepower. Por exemplo, o engenheiro chefe para as infraestruturas do setor de serviços financeiros referiu que, com a FTD inicial, a implementação da política levou entre 10 e 15 minutos, mas com a implementação da FTD o tempo caiu para cerca de 3 minutos.

“A gestão de políticas com a Cisco Secure Firewall é simples e fácil. O GUI do Firewall Management Center é leve, claro e intuitivo.”
Gestor sénior da engenharia de redes, tecnologia

Um dos entrevistados não estava a utilizar o Firewall Management Center, mas a gestão do software como um serviço (SaaS) na nuvem do Cisco Defense Orchestrator (CDO). Relativamente ao CDO, o arquiteto de infraestrutura interno do setor industrial partilhou: “A adoção do CDO foi feita sem qualquer esforço. Porque os nossos engenheiros já estavam familiarizados com o [Cisco Security Manager (CSM)], já conseguiam funcionar com a interface da linha de comandos e criar macros. Foi muito mais fácil do que mudar de fornecedor, caso em que seria complexo ter de aprender conceitos das camadas superiores.”

Modelação e pressupostos. O modelo da organização composta da Forrester:

- trinta e quatro firewalls ASA 5500-X tradicionais são substituídas pelas Cisco Secure Firewalls
- a organização composta evita as 55 horas de trabalho que levaria a implementar e criar políticas para cada substituição da firewall tradicional
- a organização composta evita 90% de 30 minutos que demorava a atualizar cada firewall todos os trimestres
- a organização composta atualiza a política da firewall em média uma vez por dia. Ao mudar para a Cisco Secure Firewall, evita 95% da 1 hora que costumava demorar a fazer cada uma destas atualizações.
- o valor médio hora de um profissional de operações de segurança de redes (NetSecOps) é de $65.
- sessenta e oito firewalls FTD são atualizadas para a versão mais recente da Cisco Secure Firewall. Por cada atualização diária da política, a organização composta poupa 80% do tempo que demorava nas firewalls FTD de gerações anteriores.
- adicionalmente, a organização composta poupa 80% do tempo que demorava a atualizar as políticas de firewall virtuais.

Riscos. A melhoria na gestão da firewall pode variar consoante:

- o tipo e o número de firewalls existentes
- o número de firewalls substituídas pelas Cisco Secure Firewalls e o ritmo desta implementação
- a decisão de implementar as firewalls virtuais nos data centers para lidar com o tráfego este-oeste e da nuvem pública.

Resultados. Tendo em conta estes riscos, a Forrester ajustou este benefício em baixa para 10%, com um PV total ao longo de três anos com ajuste de risco (com um desconto de 10%) de cerca de $163 000.

Melhorias na gestão da firewall					
Ref.	**Métrica**	**Fonte**	**1.º ano**	**2.º ano**	**3.º ano**
A1	Número de firewalls da próxima geração que substituem as firewalls antigas	Organização composta; 1/3 de um total de 102	34	0	0
A2	Horas evitadas na implementação de cada firewall	Entrevistas	55,00	55,00	55,00
A3	Horas evitadas na atualização de cada firewall ASA	90%*17 horas trimestralmente	61,2	61,2	61,2
A4	Horas evitadas na atualização manual das políticas para as firewalls ASA	95%*1 hora, diariamente*33% do ambiente	114	114	114
A5	Valor hora para um profissional de NetSecOps	Organização composta	$65	$65	$65
A6	Subtotal: Redução do tempo para implementar e atualizar para firewalls da próxima geração a partir de firewalls de 4 camadas antigas	((A1*A2)+(A3+A4))*A5	$132 938	$11 388	$11 388
A7	Número de firewalls FTD atualizadas	Organização composta; 2/3 de um total de 102	68	68	68
A8	Número de horas que anteriormente demorava a implementar políticas com o FTD anterior	Entrevistas	0,25	0,25	0,25
A9	Redução do tempo de implementação da política relativamente à atualização para o FTD mais recente	Entrevistas; de 15 minutos para 3 minutos	80%	80%	80%
A10	Subtotal: redução do tempo para implementar políticas no Firepower relativamente às firewalls 7 camadas mais antigas	365*A8*A9*A5*A7/102	$3163	$3163	$3163
A11	Número total de firewalls virtuais	Organização composta	100	100	100
A12	Número de horas evitadas anualmente para atualizar as políticas das firewall virtuais	80%*266 horas anualmente	213	213	213
A13	Subtotal: Redução do tempo para gerir firewalls virtuais	A12*A5	$13 845	$13 845	$13 845
At	Melhorias na gestão da firewall	A6+A10+A13	$149 946	$28 396	$28 396
	Ajustamento do risco	↓10%			
Atr	Melhorias na gestão da firewall (ajustados ao risco)		$134 951	$25 556	$25 556
	Total de três anos: $186 064			**Valor atual a três anos: $163 005**	

MELHORIAS NOS FLUXOS DE TRABALHO DE SEGURANÇA

Evidência e dados. A implementação da Cisco Secure Firewall e a utilização do FMC também ajudou os entrevistados a agilizar os fluxos de trabalho de segurança. Os decisores referiram que os dispositivos com base em ASA exigiam múltiplas ferramentas separadas para seguir e registar eventos através das firewalls. Com o FMC, os dados da Cisco Secure Firewall foram consolidados num só lugar em que os indicadores de risco (IOC) e as intrusões bloqueadas podiam ser seguidos e nivelados coerentemente por cima para uma solução de gestão do evento e da informação de segurança (SIEM). Com o FMC, os entrevistados conseguiram a capacidade de rever ligações, eventos e telemetria como um todo, de uma forma mais correlacionada através de toda a rede.

> **"As investigações costumavam assemelhar-se à construção de um puzzle com apenas uma peça."**
> *Chefe de equipa de operações de segurança, educação*

Com a consolidação através do Firewall Management Center, os entrevistados reportaram a redução dos custos do trabalho de investigação de segurança. Por exemplo, o engenheiro principal de cibersegurança do setor dos serviços de segurança referiu a redução do tempo de investigação de horas para 3 a 5 minutos com a ajuda da Secure Firewall e do Firewall Management Center. Anteriormente, este entrevistado referiu ter de passar por múltiplos sistemas incluindo um SIEM e uma consola de e-mail, iniciar sessão e coordenar dados. Agora, podem iniciar sessão no FMC e procurar IOCs específicos naquele ambiente.

"O Firewall Management Center funciona como uma consola única para gerir todas as Cisco Secure Firewalls. Facilita a administração e poupa tempo a investigar e a agrupar eventos e a tomar decisões relativas a atividade maliciosa."
Gestor de serviços de engenharia, serviços de TI

Os entrevistados também notaram uma redução nos seus tempos de resposta. Por exemplo, o chefe da equipa de operações de segurança do setor do ensino reportou ter de enviar pedidos para o apoio ao cliente múltiplas vezes, uma semana antes de investir na Cisco Secure Firewall. O suporte rastreava o utilizador e realizava um teste de malware, cujo scan poderia demorar horas. Depois a equipa do entrevistado procedia à limpeza do sistema ou mesmo à recriação da imagem. Este processo podia demorar um dia inteiro. Com a Cisco Secure Firewall, este entrevistado envia um pedido similar, uma vez por mês, e vai diretamente para o FMC para resolver o problema, o que demora cerca de uma hora.

"Os custos gerais das nossas firewalls antigas era elevada quando se tratava da execução da resposta a incidentes de segurança; levava muito tempo e custava muito dinheiro. Com o Firepower, estamos a assistir a enormes poupanças e a dar menos respostas a incidentes dado que há mais a serem bloqueados."
Chefe de equipa de operações de segurança, ensino

Os entrevistados que transitaram de uma versão anterior do FTD para uma versão atualizada também obtiveram benefícios relacionados com a investigação de segurança e os fluxos de trabalho de resposta. Como foi reportado pelo engenheiro chefe de infraestruturas do setor dos serviços financeiros, uma versão anterior do FTD ainda permitia uma vista agregada dos alertas de segurança através do Firewall Management Center mas depois da atualização as definições e as capacidades de acionar melhoraram. Este entrevistado também referiu que as outras integrações com produtos Cisco, incluindo o AMP e Umbrella, ainda proporcionaram mais benefícios da correlação adicional.

"O FMC dá-nos grande visibilidade. Agora, com esta visibilidade, gastamos mais tempo à procura e a certificar-nos de que tudo está a correr bem. Mas, mesmo assim, gastamos menos tempo do que anteriormente na resposta a incidentes."
Chefe de equipa de operações de segurança, ensino

As organizações que aproveitaram a inclusão da SecureX na sua licença Secure Firewall conseguiram melhorar ainda mais a eficiência operacional das equipas de segurança através da visibilidade e personalização. Por exemplo, o chefe da equipa de operações de segurança do setor do ensino também referiu que a SecureX permitia painéis de controlo personalizáveis, pelo que a equipa tinha não só visibilidade adicional do ambiente, como mostrava também aos diferentes utilizadores a informação mais importante para as suas responsabilidades.

Modelação e pressupostos. Os modelos da organização composta da Forrester:

- Total anual de alertas de segurança: 100 000.
- Vinte seis por cento destes exigiam a atenção do analista de segurança.
- Setenta por cento dos alertas que requerem atenção também requerem investigação.
- A Cisco Secure Firewall e o Firewall Management Center poupam 49% das 2,8 horas que costumavam demorar a investigar os alertas.
- Dez por cento dos alertas que requerem investigação exigem resposta.
- A Cisco Secure Firewall e o Firewall Management Center poupam 83% das 6 horas que costumavam demorar a responder.
- A SecureX possibilita poupanças de tempo adicionais aos fluxos de trabalho de investigação e resposta de 42% no 1º ano e de 77% nos 2º e 3º anos.

Riscos. A melhoria dos fluxos de trabalho de segurança pode variar consoante:

- O número de alertas anuais, alertas que requerem atenção, alertas que requerem investigação e alertas que requerem resposta.
- O valor hora dos profissionais de NetSecOps.

Resultados. Tendo em conta estes riscos, a Forrester ajustou este benefício em baixa para 15%, com um PV total ao longo de três anos com ajuste de risco de mais de $8,2 milhões.

Melhorias nos fluxos de trabalho de segurança					
Ref.	**Métrica**	**Fonte**	**1.º ano**	**2.º ano**	**3.º ano**
B1	Total anual de alertas	Organização composta	100 000	100 000	100 000
B2	Alertas que requerem a atenção do analista	Estudo da Forrester; 26%	26 000	26 000	26 000
B3	Percentagem de alertas que requerem investigação	Entrevistas	70%	70%	70%
B4	Média de horas anterior para investigar	Entrevistas	2,8	2,8	2,8
B5	Redução do tempo de investigação do FMC	Entrevistas	49%	49%	49%
B6	Alertas que requerem resposta	Entrevistas	260	260	260
B7	Média de horas anterior para responder	Entrevistas	6	6	6
B8	Redução do tempo de investigação do FMC	Entrevistas	83%	83%	83%
B9	Redução adicional da investigação e resposta da SecureX	Entrevistas	42%	77%	77%
B10	Valor hora dos profissionais de segurança	A5	$65	$65	$65
Bt	Melhorias nos fluxos de segurança	((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10	$3 141 034	$4 335 864	$4 335 864
	Ajustamento do risco	↓15%			
Btr	Melhorias nos fluxos de trabalho de segurança (ajustados ao risco)		$2 669 879	$3 685 484	$3 685 484
	Total de três anos: $10 040 848		**Valor atual a três anos: $8 241 976**		

RISCO REDUZIDO DE INTRUSÃO MATERIAL E DE PERDA DE PRODUTIVIDADE

Evidência e dados. Os entrevistados também reportaram a obtenção de benefícios financeiros associados à redução do risco de intrusão material e dos custos de produtividade conexos depois da implementação da Cisco Secure Firewall.

Uma forma através da qual a postura de segurança das organizações dos entrevistados melhorou deveu-se à visibilidade acrescida que a Cisco Secure Firewall e o Firewall Management Center facultou. Por exemplo, o chefe de operações de segurança do setor da educação referiu: "Comparada com as ASA tradicionais, a Cisco Secure Firewall dá-nos melhor visibilidade. Isto é especialmente importante dado que os utilizadores estão a trazer um número crescente de dispositivos móveis para a nossa rede e a aceder a serviços como a impressão através da rede. A atualização para o Firepower dá-nos

"Assistimos a uma ampla melhoria no número de ameaças e de IOC bloqueados. São na ordem de diferença de grandeza. Antes, a nossa empresa estava em risco todos os dias em que não executávamos a Secure Firewall. Agora temos visibilidade acrescida e os riscos reduziram-se incomensuravelmente. Agora sentimo-nos confortáveis."
Gestor de serviços de engenharia, serviços de TI

maior visibilidade e a capacidade de filtrar o tráfego de rede interno, bem como o tráfego norte-sul."

A melhoria do bloqueio automatizado melhorado também ajudou na redução do potencial risco de uma intrusão com sucesso. O gestor sénior de engenharia de redes do setor da tecnologia referiu: "Firepower é líder no setor de [sistemas de proteção de intrusão (IPS)]. Conseguimos aumentar a nossa postura de segurança e remediar problemas desde o início. Por cada potencial incidente que remediamos precocemente, poupamos dinheiro." Este mesmo cliente reportou uma melhoria de 80% no bloqueio quando transitou de um sistema com base na ASA para a Cisco Secure Firewall.

"Com a Secure Firewall, eliminámos imediatamente 80% das nossas ameaças sem necessidade de qualquer contagem adicional."
Gestor sénior da engenharia de redes, tecnologia

E, muito importante, os entrevistados também referiram a melhoria do bloqueio através da atualização das suas firewalls FTD para as versões mais recentes. O engenheiro de redes sénior da empresa de tecnologia partilhou que a atualização para a versão mais recente do FTD possibilitou entre 10% e 15% mais bloqueios automatizados que as versões anteriores.

Este mesmo entrevistado partilhou uma anedota sobre o impacto que o bloqueio automático podia ter: "Uma vez tivemos um potencial risco baseado em social engineering em que um hacker conseguiu obter um token de acesso de 24 horas através de um utilizador autenticado. Quando o hacker tentou usar [o token], a Cisco Secure Firewalls salvou-nos. Conseguimos verificar a postura e verificar se o atacante estava a usar uma máquina da empresa. A Secure Firewall negou automaticamente o acesso do hacker ao VPN. Sem esta, o hacker teria tido acesso à nossa rede empresarial e não tenho a certeza sobre quão grave poderia ter sido o impacto."

"A Cisco Secure Firewall é um serviço centralizado. Tem todas as capacidades de integração com outras ferramentas para fornecer os dados relevantes para auxiliar na segurança. Tem diferentes variedades, podemos abordar diferentes requisitos de produtividade e suporta a expansão vertical e horizontal. Tem todas as funcionalidades necessárias para resolver os riscos de segurança atuais e está continuamente a melhorar."
Engenheiro de redes sénior, internet

O engenheiro de redes sénior da empresa de tecnologia também referiu um benefício de segurança que a Secure Firewall oferece ao ser capaz de gerir o acesso ao nível da aplicação: "Estamos a assistir a um uso imenso do BitTorrent na nossa rede para convidados. Ao alavancar o FTD para bloquear o BitTorrent, estamos não só a prevenir potenciais ameaças a outros convidados, como também reduzimos a utilização do circuito em cerca de 400 Mbps."

Para além da deteção da camada da aplicação e do bloqueio, os entrevistados referiram que o uso pela Cisco Secure Firewall de feeds de ameaças automatizadas baseadas no Snort também reduziu o risco das suas organizações de uma intrusão material bem-sucedida. O engenheiro chefe da infraestrutura dos serviços financeiros afirmou: "Queríamos a Cisco Secure Firewall por causa da visibilidade acrescida e a resposta automatizada do Snort, procurar coisas como servidores sem patches expostos à internet e o bloqueio holístico de tráfego malicioso."

As organizações que aproveitaram a inclusão da SecureX na sua licença Secure Firewall conseguiram reduzir ainda mais o risco e os custos de intrusões materiais. Por exemplo, o engenheiro chefe da infraestrutura da organização de serviços financeiros afirmou que a

SecureX lhes possibilitou obter ainda mais visibilidade na identificação de problemas de segurança e na identificação da causa essencial de potenciais ameaças.

"A SecureX pode dar-nos uma visão única do nosso ambiente de segurança global. Com o FMC, obtemos uma vista de todas as nossas firewalls, com a SecureX obtemos uma vista do FMC, bem como de toda a nossa integração nas soluções de segurança da Cisco."
Chefe de equipa de operações de segurança, ensino

Modelação e pressupostos. Os modelos da organização composta da Forrester:

- um número anterior de intrusões materiais de segurança de três
- a média combinada de custos internos e externos de uma intrusão material são $968 480
- a percentagem de ataques externos, incidentes internos e ataques/incidentes envolvendo parceiros e terceiros é de 79%
- a Cisco Secure Firewall e o Firewall Management Center reduzem o risco de uma intrusão em 80% para a percentagem da organização anteriormente coberta pelas firewalls ASA tradicionais
- a Cisco Secure Firewall e o Firewall Management Center reduzem o risco de uma intrusão em 15% para a percentagem da organização anteriormente coberta pelas firewalls com base em FTD
- sessenta e seis por cento dos funcionários da organização composta são afetados por cada intrusão, recuperando 70% da sua produtividade graças à redução do risco de intrusão causada pela Cisco Secure Firewall e pelo Firewall Management Center
- o valor hora dos funcionários em geral é de $40.

Riscos. O risco reduzido de uma intrusão material pode variar consoante:

- o número de intrusões materiais anuais atualmente experienciadas
- os custos internos e externos totais de uma intrusão material
- a percentagem de ataques externos, incidentes internos e ataques/incidentes envolvendo parceiros e terceiros
- o tipo e o número de firewalls existentes
- o número de funcionários afetados por uma intrusão material, o seu valor hora e a sua capacidade recuperar a produtividade quando estas intrusões materiais se reduzem.

Resultados. Tendo em conta estes riscos, a Forrester ajustou este benefício em baixa para 15%, com um PV total ao longo de três anos com ajuste de risco de quase $3,5 milhões.

Risco reduzido de intrusão material e de perda de produtividade					
Ref.	**Métrica**	**Fonte**	**1.º ano**	**2.º ano**	**3.º ano**
C1	Número médio de intrusões materiais	Estudo da Forrester	3	3	3
C2	Custo médio por intrusão material	Estudo da Forrester	$968 480	$968 480	$968 480
C3	Percentagem de ataques externos, incidentes internos e ataques/incidentes envolvendo parceiros e terceiros.	Entrevistas	79%	79%	79%
C4	Percentagem da organização que transita da ASA para o Firepower	Organização composta	33%	33%	33%
C5	Percentagem de redução do risco do Firepower	Entrevistas	80%	80%	80%
C6	Percentagem da organização que transita do Firepower antigo para o Firepower atualizado	Organização composta	67%	67%	67%
C7	Percentagem de redução do risco do Firepower atualizado	Entrevistas	15%	15%	15%
C8	Redução adicional com o SecureX	Entrevistas	14%	18%	23%
C9	Subtotal: Risco reduzido de intrusão	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	$1 162 951	$1 254 763	$1 369 528
C10	Número de utilizadores afetados por cada intrusão	Estudo da Forrester	10 600	10 600	10 600
C11	Valor hora médio dos funcionários em geral	Organização composta	$40	$40	$40
C12	Captação da taxa de produtividade	Organização composta	70%	70%	70%
C13	Subtotal: Produtividade melhorada decorrente do risco reduzido de intrusões	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8)	$356 397	$384 534	$419 705
Ct	Reduzido risco de intrusão material e de perda de produtividade	C9+C13	$1 519 348	$1 639 297	$1 789 232
	Ajustamento do risco	↓15%			
Ctr	Risco reduzido de intrusão material e de perda de produtividade		$1 291 446	$1 393 402	$1 520 848
	Total de três anos: $4 205 696			**Valor atual de três anos: $3 468 249**	

BENEFÍCIOS DO DESEMPENHO PARA A PRODUTIVIDADE DOS FUNCIONÁRIOS

Evidência e dados. A Cisco Secure Firewall permitiu às organizações dos entrevistados melhorar amplamente a produtividade dos funcionários de duas maneiras: 1) fornecendo visibilidade e controlo ao nível da aplicação que melhoraram o desempenho de rede e 2) limitando as sequelas dos períodos de inatividade causados pelas atualizações de políticas.

Os entrevistados referiram que o desempenho da sua rede se degradava menos frequentemente depois da implementação da Cisco Secure Firewall graças à sua capacidade de controlar o acesso à rede na camada da aplicação. Anteriormente, os clientes reportavam que as suas redes abrandavam e o desempenho se degradava frequentemente ao ponto de afetarem a produtividade dos funcionários quando havia uma elevada procura de aplicações específicas, especialmente as relacionadas com ficheiros de vídeo. O chefe de equipa de operações de segurança do setor do ensino partilhou: “Embora a rede abrandasse diariamente de forma notória, a degradação era tão má que afetava a produtividade uma vez a cada duas semanas. Isto acontecia sobretudo quando tínhamos um aumento súbito de atividade, como no caso de milhares de utilizadores a verem um vídeo.”

Como a Cisco Secure Firewall permitiu às organizações dos entrevistados estabelecer a política de segurança em múltiplas camadas, incluindo a camada da aplicação, os entrevistados tinham uma maior controlo granular sobre as permissões de rede. Como resultado, estas empresas podiam controlar melhor quando e que aplicações podiam aceder às suas redes, prevenindo a sobrecarga da rede a partir de aplicações com elevada largura de banda, melhorando o desempenho da rede e aumentando a produtividade dos seus funcionários.

"A Cisco Secure Firewall dá-nos muito maior visibilidade sobre como a rede está a ser utilizada e a possibilidade de controlar este uso. Temos atualmente 4000 sistemas diferentes monitorizados, assim, se quisesse, podia ver quão utilizada tinha sido [uma aplicação social popular com base em vídeo] na última semana. Podíamos estabelecer regras para proibir este tipo de tráfego se for necessário."
Chefe de equipa de operações de segurança, ensino

Outros entrevistados referiram que as suas empresas aumentaram a produtividade dos funcionários ao limitar o impacto negativo que os erros humanos por vezes criavam nas atualizações de políticas. Por exemplo, o gestor de serviços de engenharia da empresa de serviços de TI referiu que, porque as políticas podiam ser criadas e atualizadas muito mais rapidamente com o Firewall Management Center, também recebiam feedback sobre se as atualizações tinham sucesso mais rapidamente.

Antes desta empresa ter implementado a Secure Firewall, demoraria 15 minutos a atualizar uma política e outros 15 minutos para saber se tinha sido corretamente definida. Se não, demoraria mais 15 minutos a sair e a voltar para atualizar a política uma segunda vez. Ocasionalmente, uma política atualizada erradamente teria um impacto negativo na produtividade dos funcionários, especialmente em ambientes de produção.

Depois de atualizar para a versão mais recente do FTD com a Cisco Secure Firewall, o gestor dos serviços de engenharia notou uma redução do tempo de atualização da política e feedback para 3 minutos para sair e 3 minutos para voltar reduzindo o tempo total de atualização, feedback e resolução de problemas em 80% de 60 minutos para 12 minutos.

Modelação e pressupostos. Os modelos da organização composta da Forrester:

- demora uma hora a resolver uma atualização errada da política (15 minutos para enviar a atualização errada, 15 minutos para receber o feedback e 30 minutos para atualizar e receber feedback depois de resolvida a situação)
- a Cisco Secure Firewall e o Firewall Management Center reduzem o tempo que demora a resolver políticas erradas em 80%
- uma percentagem assumida de 2% da organização é, em média, afetada por atualizações erradas de políticas
- a rede costumava incorrer em grave degradação que afetava a produtividade dos funcionários durante 20 minutos aproximadamente, a cada duas semanas
- trinta e três por cento dos funcionários que as firewalls ASA tradicionais costumavam cobrir foram afetados pela degradação da rede.

Riscos. Os benefícios do desempenho para a produtividade dos funcionários podem variar consoante:

- a percentagem de funcionários afetados por atualizações erradas da política
- a frequência e a extensão da degradação da rede que afeta a produtividade dos funcionários
- o número de funcionários afetados pela degradação da rede

Resultados. Tendo em conta estes riscos, a Forrester ajustou este benefício em baixa para 10%, com um PV total ao longo de três anos ajustado ao risco de mais de $4,1 milhões.

Benefícios do desempenho para a produtividade dos funcionários

Ref.	Métrica	Fonte	1.º ano	2.º ano	3.º ano
D1	Número de horas que anteriormente demorava a implementar políticas com o FTD anterior	Entrevistas	1	1	1
D2	Número de horas que demora agora a implementação de políticas com o FTD atualizado	Entrevistas	0,2	0,2	0,2
D3	Número médio de funcionários afetados	Organização composta	320	320	320
D4	Valor hora médio dos funcionários em geral	C10	$40	$40	$40
D5	Taxa de recuperação da produtividade	Organização composta	25%	25%	25%
D6	Subtotal: Produtividade melhorada do feedback da política anterior	365*(D1-D2)*D3*D4*D5	$934 400	$934 400	$934 400
D7	Frequência da degradação do desempenho devido ao abuso da utilização da rede	Entrevistas	26	26	26
D8	Extensão média da degradação do desempenho em horas	Entrevistas	0,33	0,33	0,33
D9	Número de funcionários afetados (apenas migrações ASA)	Organização composta	5280	5280	5280
D10	Valor hora médio dos funcionários em geral	C11	$40	$40	$40
D11	Taxa de recuperação da produtividade	Organização composta	50%	50%	50%
D12	Subtotal: Produtividade melhorada dos funcionários do utilizador final	D7*D8*D9*D10*D11	$906 048	$906 048	$906 048
Dt	Benefícios do desempenho para a produtividade dos funcionários	D6+D12	$1 840 448	$1 840 448	$1 840 448
	Ajustamento do risco	↓10%			
Dtr	Benefícios do desempenho para a produtividade dos funcionários (risco ajustado)		$1 656 403	$1 656 403	$1 656 403
	Total de três anos: $4 969 210			**Valor atual de três anos: $4 119 230**	

CUSTOS REDUZIDOS E EVITADOS DAS SOLUÇÕES ANTERIORES

Evidência e dados. Ao migrar a sua infraestrutura de segurança de rede para a versão mais recente da Cisco Secure Firewall, as organizações dos entrevistados reduziram e evitaram os custos associados à infraestrutura da sua rede antiga. Não sendo de admirar que os entrevistados tenham reportado ter evitado os custos do relicenciamento das suas firewalls tradicionais baseadas na ASA, bem como quaisquer firewalls baseadas em FTD anteriores, com a substituição destas pelas Cisco Secure Firewalls.

Para além das substituições das firewall físicas e virtuais, as organizações dos entrevistados que transitaram de ambientes com base ASA desativaram as suas soluções IPS autónomas dado que a Cisco Secure Firewall inclui IPS.

“Com as firewalls ASA tradicionais, também necessitávamos de investir em unidades IPS para colocar entre os links e a firewall. Com Cisco Secure Firewall, a IPS está integrada. Já não precisamos de gerir duas soluções diferentes com dois ecossistemas diferentes e não estamos dependentes dos engenheiros IPS.”
Gestor sénior da engenharia de redes, tecnologia

Mais importante, os entrevistados referiram poupanças adicionais quando atualizaram as firewalls das suas organizações do FTD anterior para a Cisco Secure Firewall. Por causa da eficiência destas firewalls mais recentes, os entrevistados reportaram necessitar entre 20% e 25% menos firewalls para alcançar os mesmos resultados.

“Transitar de um FTD anterior para o FTD mais recente na Cisco Secure Firewall, assistimos a uma melhor eficiência do processamento. A Cisco Secure Firewall é entre 20% e 25% mais eficiente que as iterações anteriores, o que significa que necessitamos de menos firewalls.”
Engenheiro de redes sénior, internet

Modelação e pressupostos. Os modelos da organização composta da Forrester:

- uma redução dos custos de licenciamento da IPS autónoma, devido à substituição das firewalls ASA tradicionais pelas Cisco Secure Firewalls, de $171 600 anualmente
- evitadas as taxas de manutenção das IPS autónomas equivalente a 20% das taxas de licenciamento
- uma redução dos custos de gestão continuados relacionados com as IPS de 80%, de 30 minutos para 2 FTE semanalmente
- evitados os custos de substituição das firewalls existentes por outras de tipo similar superiores a $1,3 milhões no 1º ano
- evitados os custos de substituição das firewalls de $300 000 anualmente
- evitados os custos de mais 25% das firewalls físicas graças à eficiência das Cisco Secure Firewalls.

“Desativámos finalmente as nossas unidades IPS dispendiosas e com desempenho inferior quando implementámos a Cisco Secure Firewall.”
Engenheiro chefe de infraestruturas, serviços financeiros

Riscos. A redução dos custos da solução antiga variará consoante :

- o número e o tipo das firewalls existentes
- a capacidade para desativar as soluções IPS autónomas.

Resultados. Tendo em conta estes riscos, a Forrester ajustou este benefício em baixa para 10%, com um PV total ao longo de três anos, com ajuste de risco de quase $2,6 milhões.

Redução dos custos das soluções desativadas antigas					
Ref.	**Métrica**	**Fonte**	**1.º ano**	**2.º ano**	**3.º ano**
E1	Reduzido os custos do IPS antigo	Entrevistas	$171 600	$171 600	$171 600
E2	Reduzido o custo das taxas de manutenção	E1*20%	$34 320	$34 320	$34 320
E3	Reduzidos os custos da gestão continuada do IPS antigo	Entrevistas	$53 539	$53 539	$53 539
E4	Evitados os custos de firewalls para o ciclo de substituição	Organização composta	$1 616 980	$300 000	$300 000
E5	Evitados os custos de eficiência da firewall adicional	Organização composta	$329 245	$0	$0
Et	Custos reduzidos com a desativação de soluções antigas	E1+E2+E3+E4+E5	$2 205 684	$559 459	$559 459
	Ajustamento do risco	↓10%			
Etr	Custos reduzidos com a desativação de soluções antigas (risco ajustado)		$1 985 115	$503 513	$503 513
	Total de três anos: $2 992 142		**Valor atual de três anos: $2 599 074**		

BENEFÍCIOS NÃO QUANTIFICADOS

Benefícios adicionais que os clientes experienciaram mas não conseguiram quantificar incluem:

- **Melhorias na segurança e produtividade do VPN.** Os entrevistados também referiram que a Cisco Secure Firewall possibilitou melhor produtividade e segurança com o acesso remoto à VPN. Com uma carga equilibrada, a Secure Firewall distribuiu sessões entre os dispositivos agrupados, fornecendo desempenho, resiliência e produtividade do utilizador final. De modo similar, a autenticação local com a Secure Firewall possibilitou que os utilizadores permanecessem produtivos se um servidor AAA ficasse inacessível. Para segurança, a Cisco Secure Firewall possibilita a autenticação com múltiplos certificados, para que as organizações possam assegurar que o dispositivo remoto foi atribuído pela empresa, para além da validação dos próprios utilizadores finais.
- **Conformidade melhorada.** Os entrevistados também partilharam que a Cisco Secure Firewall e o Firewall Management Center forneciam um benefício não qualificável para os fluxos de trabalho de conformidade. O engenheiro chefe de infraestruturas da empresa de serviços financeiros referiu que, antes de implementar a Secure Firewall e o FMC, o relatório de conformidade era mais difícil. As soluções anteriores careciam de uma função de relatório simples. Porém, a Secure Firewall e o FMC possibilitaram que a sua organização executasse relatórios que fossem mais abrangentes relativamente aos componentes e mais detalhados quanto às atividades e vistas. Os entrevistados também mencionaram que a Cisco Secure Firewall suporta encriptação transport layer security (TLS) 1.3 standard. Por exemplo, o engenheiro de redes sénior da empresa de internet referiu que a sua equipa não estava atualmente a desencriptar esses fluxos devido à carga administrativa. Depois de investir na Cisco Secure Firewall, a desencriptação TLS 1.3 tornou-se mais fácil e mais eficiente.

“Anteriormente, não tínhamos os resultados de relatório para uma série de componentes de configuração diferentes, mas agora podemos ter relatórios mais detalhados com um espetro mais amplo com maior facilidade. Por exemplo, acabei de receber um relatório de todas as alterações ao controlo de acesso, que fiz no último ano. Apresenta o resultado de todas as vistas de página e as alterações que foram feitas.”
Engenheiro chefe de infraestruturas, serviços financeiros

- Melhoria da **experiência dos funcionários.** Os entrevistados também referiram haver uma melhoria na experiência dos funcionários das suas organizações. Por exemplo, o engenheiro de redes sénior da empresa de internet afirmou: “A capacidade de controlar melhor o acesso à aplicação nas nossas redes melhorou a satisfação dos funcionários. As nossas equipas de TI locais costumavam ter dificuldades em encontrar os utilizadores para lhes pedir que deixassem de utilizar determinadas aplicações ou para lhes bloquear o acesso. Com a Secure Firewall e o FMC, agora podemos fazer exatamente isso remotamente.”

FLEXIBILIDADE

O valor da flexibilidade é único para cada cliente. Há múltiplos cenários em que um cliente podia implementar uma Secure Firewall e mais tarde compreender a existência de usos e oportunidades comerciais adicionais, incluindo:

- **Integrações Cisco Security adicionais.** Para além dos benefícios da SecureX, os entrevistados referiram que o Ecossistema da Cisco de ofertas de segurança oferecia a flexibilidade para incentivar ainda mais as suas posturas de segurança organizacional. Por exemplo, o gestor dos serviços de engenharia da empresa de serviços de TI partilhou: “A Cisco Security tem um conjunto profundo de soluções de segurança integradas, que é também algo com que outros fornecedores se debatem. Não é apenas a Secure Firewall, são todas as outras peças que se integram bem em conjunto e nos permitem criar as nossas defesas.”
- **Operações melhoradas para o trabalho a partir de casa.** Os controlos da Cisco Secure Firewall também ajudaram a manter as operações em bom funcionamento quando o uso do VPN explodiu aquando da transição para o trabalho a partir de casa por parte dos funcionários. O engenheiro de redes sénior da empresa de internet referiu que “Durante a pandemia as nossas ligações VPN simultâneas aumentaram de uma média de 100 000 para perto de 350 000 globalmente. De modo a manter a viabilidade da nossa rede, usámos a Cisco Secure Firewall para definir limites de variação, facilitando as operações.”
- **Facilidade de transição para a nuvem.** Por último, os entrevistados partilharam que a Cisco Secure Firewall facilitou a realização das suas iniciativas na nuvem. O gestor de serviços de engenharia da organização de serviços de TI disse “Precisávamos de uma plataforma única para chegar ao local, a locais remotos e também para a nuvem, mas tinha de ser fácil de implementar. Assim, com as plataformas na nuvem, basta colocar uma firewall FTD, instalá-la e ligá-la depois no Firewall Management Center. Não levou tempo nenhum a configurar e implementar. E podíamos avançar com uma política padronizada para as mesmas.”

A flexibilidade seria também quantificada quando avaliada como parte de um projeto específico (descrito com mais detalhe no Apêndice A).

Análise dos custos

Dados dos custos quantificados conforme foram aplicados à organização composta

Custos totais							
Ref.	**Custo**	**Inicial**	**1.º ano**	**2.º ano**	**3.º ano**	**Total**	**Valor atual**
Ftr	Custos de licenciamento	$6 000 690	$0	$0	$0	$6 000 690	$6 000 690
Gtr	Custos de implementação, criação de política e formação	$278 220	$7924	$7924	$7924	$301 990	$297 924
	Custos totais (ajustados ao risco)	$6 278 910	$7924	$7924	$7924	$6 302 680	$6 298 614

CUSTOS DE LICENCIAMENTO

Evidência e dados. Os clientes referiram que suportaram diversos custos diferentes associados ao seu investimento na Secure Firewall, incluindo:

- custos da firewall física, que variou consoante o desempenho
- firewalls virtuais implementadas para o data center ou data centers para lidar com o tráfego este-oeste
- custos de das licenças de Threat Protection, Malware Defense e filtragem do URL
- licenças do Firewall Management Center.

"Esforçámo-nos por encontrar qualquer outra opção com a profundidade da arquitetura, conjunto de ferramentas e funcionalidades que a Cisco Secure Firewall tem em conjunto numa caixa. Mas, para além disso, a relação preço-desempenho também era persuasiva."
Engenheiro chefe de infraestruturas, serviços financeiros

Os clientes referiram que conseguiram implementar a Cisco SecureX sem custos adicionais por estar incluída nas suas licenças Secure Firewall.

Modelação e pressupostos. Para a organização composta, com 100 escritórios e quatro data centers físicos, que exigiam redundância, o modelo da Forrester é o seguinte:

- todas as licenças ao preço de tabela, durante três anos
- o custo de uma firewall para a sede da empresa é de $328 443 a sede da empresa requer uma firewall grande ao nível de uma grande empresa, com um débito até 75 Gbps.
- o custo das firewalls para o data center é de $978 067. Em cada data center, a organização composta implementa um clustering de perímetro de data center ou conjunto de elevada disponibilidade para lidar com o tráfego norte-sul para dentro e para fora do data center.
- O custo de 100 firewalls virtuais é de $2 628 561. Estas firewalls virtuais lidam com o tráfego este-oeste dentro dos data centers e também entre os data centers e as plataformas da nuvem pública.
- As firewalls físicas e virtuais nos data centers têm todas uma licença Threat Protection com uma taxa de subscrição de três anos. Isto oferece segurança adicional, incluindo o Snort 3 para detetar e mitigar melhor os indicadores de risco e tráfego malicioso.
- O custo total das firewalls para 60 filiais é de $1 848 160. Sessenta escritórios requerem Secure Firewalls com um débito até 1,9 Gbps.

- O custo total de 39 filiais pequenas é de $137 779. Os 39 escritórios remanescentes apenas requeriam um débito até 650 Mbps.
- Todas as firewalls dos escritórios têm licenças de Threat Protection, Malware Defense e filtragem de URL adicionais com uma taxa de subscrição de três anos.
- O Firewall Management Center também está licenciado com uma dimensão apropriada para lidar com todas estas firewalls. O custo do Firewall Management Center é de $79 680.

Riscos. Os custos de licenciamento da Cisco Secure Firewall e do Firewall Management Center variam consoante:

- o número de firewalls virtuais desejado
- o número necessário de firewalls ao nível das grandes empresas
- a dimensão e o número dos data centers e necessidade de elevada disponibilidade
- a dimensão e o número de escritórios das filiais.

Resultados. Como a Forrester obteve o preço para a organização composta diretamente junto da Cisco, não ajustámos este custo ao risco, com um PV total ao longo de três anos (com um desconto de 10%) de $6 milhões.

“Com o nosso contrato de segurança Cisco para as grandes empresas, o nosso custo total é mais barato do que seria se todos os componentes fossem adquiridos individualmente. Embora o Firepower constitua a maior parte daquele custo, estamos a poupar centenas de milhares de dólares obtendo proteção adicional com produtos que não tínhamos antes.”
Chefe de equipa de operações de segurança, ensino

Custos de licenciamento

Ref.	Métrica	Fonte	Inicial	1.º ano	2.º ano	3.º ano
F1	Custo das firewalls virtuais	Cisco	$2 628 561			
F2	Custo da firewall da sede da empresa	Cisco	$328 443			
F3	Custo das firewalls do data center físico	Cisco	$978 067			
F4	Custo das firewalls dos escritórios das filiais pequenas	Cisco	$137 779			
F5	Custo das firewalls dos escritórios das filiais grandes	Cisco	$1 848 160			
F6	Custo do Firewall Management Center	Cisco	$79 680			
Ft	Custos de licenciamento	F1+F2+F3+F4+F5+F6	$6 000 690	$0	$0	$0
	Ajustamento do risco	0%				
Ftr	Custos de licenciamento (ajustados ao risco)		$6 000 690	$0	$0	$0
	Total de três anos: $6 000 690			**Valor atual de três anos: $6 000 690**		

CUSTOS DE IMPLEMENTAÇÃO, CRIAÇÃO DE POLÍTICA E FORMAÇÃO

Evidência e dados. Os entrevistados partilharam ter experienciado custos internos de tempo e mão de obra associados à implementação das firewalls através dos seus data centers e escritórios. O primeiro destes custos envolveu a implementação física das firewalls em cada local. O segundo envolveu a implementação destas firewalls através da criação e implementação das políticas apropriadas através de cada conjunto de firewalls.

"A implementação foi realmente rápida e relativamente simples. A mudança real demorou três semanas, dado que já tínhamos o design e sabíamos como ligar tudo."
Chefe de equipa de operações de segurança, educação

Por último, os decisores entrevistados também referiram ter experienciado custos de tempo relacionados com a formação. A formação demorou 2 horas para qualquer funcionário que necessitasse dessa formação para implementar e gerir as Cisco Secure Firewalls. Alguns entrevistados referiram ter aproveitado os vídeos de formação, realizados por especialistas em segurança da Cisco e que são do domínio público.

Modelação e pressupostos. Os modelos da organização composta da Forrester:

- em média, é necessário um tempo de implementação de 6 horas em cada dois data centers e 100 escritórios
- em média a criação da política demora 30 horas por cada firewall
- a SecureX requer 20 horas de trabalho para a implementação inicial e outras 100 horas, anualmente, para fazer a gestão continuada
- inicialmente, quinze funcionários necessitam de formação com outros três funcionários a necessitar de formação anualmente devido à rotatividade dos funcionários.

Riscos. O custo da implementação e da criação da política varia consoante:

- o número de Cisco Secure Firewalls a implementar
- o número de funcionários que necessitam de formação inicialmente
- o índice de rotatividade dos funcionários
- o valor hora dos profissionais de NetSecOps.

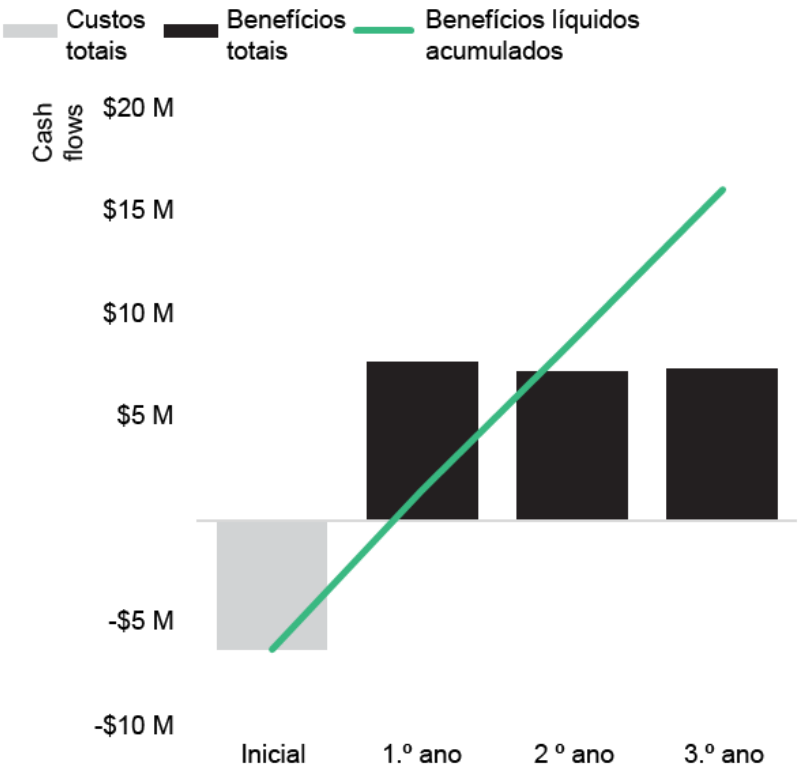
Resultados. Tendo em conta estes riscos, a Forrester ajustou este custo em alta para 15%, com um PV total ao longo de três anos com ajuste de risco abaixo dos $298 000.

Custos de implementação, criação de política e formação						
Ref.	**Métrica**	**Fonte**	**Inicial**	**1.º ano**	**2.º ano**	**3.º ano**
G1	Locais a implementar	Organização composta	102			
G2	Número médio de horas para a implementação física em cada local	Organização composta	6			
G3	Horas para a criação da política	Entrevistas	30			
G4	Horas para a implementação e gestão da SecureX	Entrevistas	20	100	100	100
G5	Funcionários que necessitam de formação	Entrevistas	15	3	3	3
G6	Horas necessárias para formação	Entrevistas	2	2	2	2
G7	Valor dos profissionais de NetSecOps.	A5	$65	$65	$65	$65
Gt	Custos de implementação, criação de política e formação	((G1*(G2+G3))+,G4+(G5*G6))*G7	$241 930	$6890	$6890	$6890
	Ajustamento do risco	↑15%				
Gtr	Custos de implementação, criação de política e formação (ajustado ao risco)		$278 220	$7924	$7924	$7924
Total de três anos: $301 990			**Valor atual de três anos: $297 924**			

Resumo financeiro

MÉTRICA CONSOLIDADA PARA TRÊS ANOS AJUSTADA AO RISCO

Quadro do Cash Flow (ajustado ao risco)



Os resultados financeiros calculados nas secções Benefícios e Custos podem ser usados para determinar o ROI, o NPV e o período de reembolso para o investimento da organização composta. A Forrester assume uma taxa de desconto anual de 10% para esta análise.

Estes valores do ROI ajustados ao risco, NPV e período de reembolso são determinados pela aplicação dos fatores de ajustamento do risco aos resultados não ajustados em cada secção Benefício e Custo.

Análise do Cash Flow (Estimativas ajustadas ao risco)

	Inicial	1.º ano	2.º ano	3.º ano	Total	Valor atual
Custos totais	($6 278 910)	($7924)	($7924)	($7924)	($6 302 680)	($6 298 614)
Benefícios totais	$0	$7 737 795	$7 264 360	$7 391 805	$22 393 959	$18 591 534
Benefícios líquidos	($6 278 910)	$7 729 871	$7 256 436	$7 383 881	$16 091 279	$12 292 920
ROI						195%
Período de reembolso (meses)						10

Apêndice A: Total Economic Impact

O Total Economic Impact é uma metodologia desenvolvida pela Forrester Research que otimiza os processos de tomada de decisão de tecnologia de uma empresa e auxilia os fornecedores na comunicação da proposta de valor dos seus produtos e serviços aos clientes. A metodologia TEI ajuda as empresas a demonstrar, justificar e realizar o valor tangível das iniciativas de TI à administração e a outras partes interessadas chave.

ABORDAGEM DO TOTAL ECONOMIC IMPACT

Benefícios representam o valor oferecido à empresa pelo produto. A metodologia TEI coloca igual peso na medida dos benefícios e na medida dos custos, permitindo um exame completo do efeito da tecnologia em toda a organização.

Custos consideram-se todas as despesas necessárias para oferecer o valor ou benefícios propostos do produto. A categoria custo no âmbito do TEI capta os custos crescentes através do ambiente existente para os custos continuados associados à solução.

Flexibilidade representa o valor estratégico que pode ser obtido para algum investimento futuro adicional acima do investimento inicial já efetuado. Tendo a capacidade de captar aquele benefício tem um PV que pode ser estimado.

Riscos medem a incerteza das estimativas de custo e benefício apresentadas: 1) a probabilidade das estimativas cumprirem as projeções originais e 2) a probabilidade das estimativas serem seguidas ao longo do tempo. Os fatores de risco do TEI baseiam-se na "distribuição triangular."

A coluna do investimento inicial inclui os custos incorridos na "hora 0" ou no início do 1º ano que não são descontados. Todos os outros cash flows são descontados usando a taxa de desconto no final do ano. Os cálculos do PV são feitos para cada estimativa do total do custo e benefício. Os cálculos do NPV nos quadros resumo são a soma do investimento inicial e dos cash flows descontados em cada ano. As somas e os cálculos do valor atual dos quadros dos Benefícios totais, Custos totais e Cash Flow podem não estar exatamente corretos, dado que podem ocorrer alguns arredondamentos.

VALOR ATUAL (PV)

As estimativas do valor atual ou presente do custo (descontado) e do benefício são calculadas com uma taxa de juro (a taxa de desconto). O PV dos custos e benefícios entra no NPV total dos cash flows.

VALOR ATUAL LÍQUIDO (NPV)

O valor atual ou presente dos cash flows líquidos futuros (descontado) é calculado com uma taxa de juro (a taxa de desconto). Um NPV positivo do projeto indica normalmente que o investimento deve ser feito, salvo se outros projetos tiverem NPVs mais elevados.

RETORNO DO INVESTIMENTO (ROI)

Um retorno esperado do projeto em termos percentuais. O ROI é calculado dividindo os benefícios líquidos (benefícios menos custos) pelos custos.

TAXA DE DESCONTO

A taxa de juro usada na análise do cash flow para ter em conta o valor temporal do dinheiro. As organizações usam habitualmente taxas de desconto entre 8% e 16%.

PERÍODO DE REEMBOLSO

O limiar de rentabilidade de um investimento. Este é o momento em que os benefícios líquidos (benefícios menos custos) igualam o investimento ou custo inicial.

Apêndice B: Notas finais

[1] O Total Economic Impact é uma metodologia desenvolvida pela Forrester Research que otimiza os processos de tomada de decisão sobre tecnologia de uma empresa e auxilia os fornecedores na comunicação da proposta de valor dos seus produtos e serviços aos clientes. A metodologia TEI ajuda as empresas a demonstrar, justificar e realizar o valor tangível das iniciativas de TI à administração e a outras partes interessadas chave.


FORRESTER®