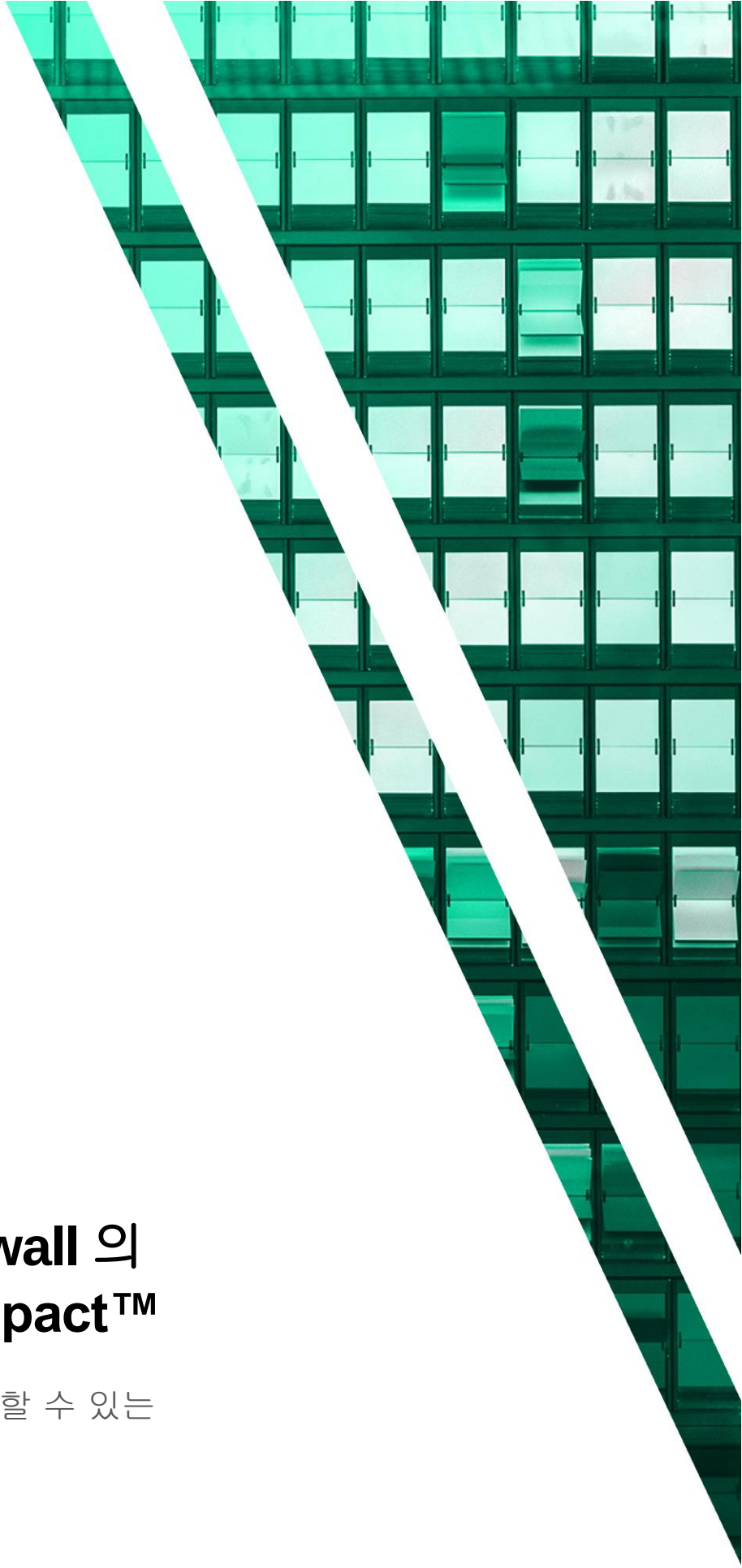
FORRESTER®



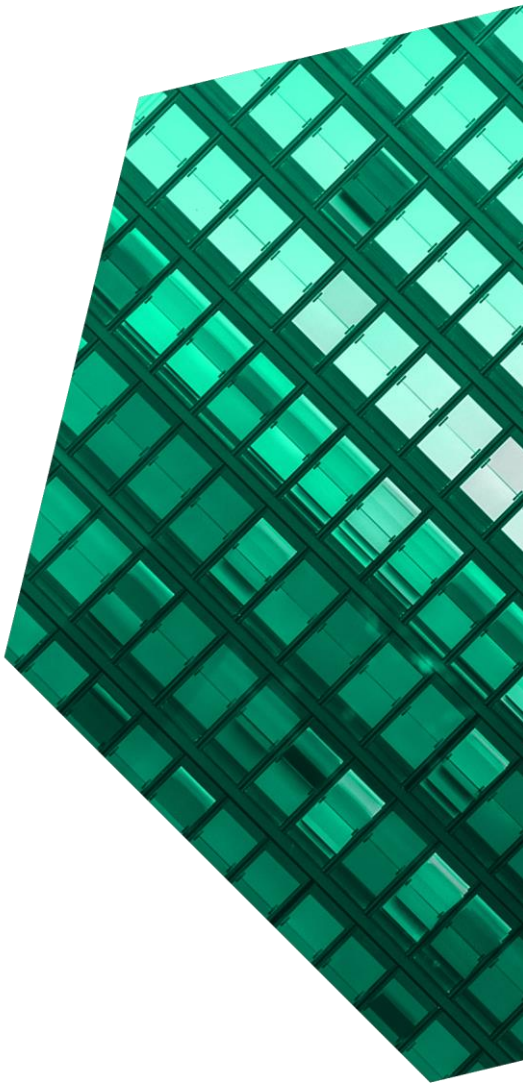
Cisco Secure Firewall 의 Total Economic Impact™

Cisco Secure Firewall 로 실현할 수 있는 비용 절감 및 비즈니스 이익

2022 년 3 월

목차

컨설팅팀: Henry Huang
Nick Mayberry



FORRESTER CONSULTING 소개

Forrester Consulting 은 독립적이고 객관적인 연구 기반 컨설팅을 제공하여 조직 내 경영진의 성공을 돕습니다. 자세한 내용은 forrester.com/consulting 을 참조하십시오.

© Forrester Research, Inc. All rights reserved. 무단 복제는 엄격히 금지됩니다. 가능한 가장 정확한 자료를 기반합니다. 제시된 의견은 당시의 판단을 반영하는 것으로서, 시간에 따라 변경될 수 있습니다. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, Total Economic Impact 는 Forrester Research, Inc.의 상표입니다. 기타 모든 상표는 각 해당 회사의 자산입니다.

개요

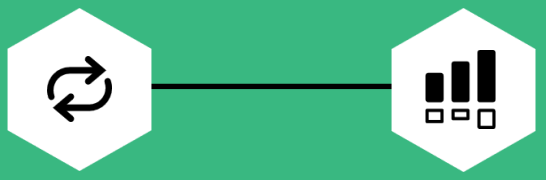
Cisco Secure Firewall 과 Firewall Management Center 는 네트워크 보안에 대한 조직의 가시성과 통제 능력을 개선해 줍니다. 인터뷰 대상자의 조직은 방화벽 관련 네트워크 전문 작업 중 최대 95%, 관련 보안 전문 작업 중 최대 83%를 절약했습니다. 이들 조직은 네트워크 및 VPN 중단을 최소화하여 최종 사용자 생산성을 높이는 동시에 중대한 보안 침해 리스크를 최대 80%까지 줄였습니다. 방화벽 배포를 25% 줄이면서도 보안 상태는 강화되었습니다.

Cisco Secure Firewall 은 외부 및 내부 위협으로부터 조직을 보호하는 동시에 방화벽과 위협 관리 모두에 대한 네트워크 팀과 보안 팀의 부담을 덜어주는 차세대 레이어 7 네트워크 보안 솔루션입니다. 조직에서는 네트워크 팀과 보안 팀에 애플리케이션 계층에서도 더욱 통합되고 종합적인 관점에서 네트워크 활동을 모니터링하고 암호화된 트래픽에서 탐지된 위협도 볼 수 있는 추가적인 가시성을 제공하는 중앙 집중식 방화벽 관리 및 위협 방어 허브인 FMC(Firewall Management Center)로 Cisco Secure Firewall 을 관리할 수 있습니다. 또한 Snort 3 IPS(침입 방지 시스템)로 향상된 제어 기능과 URL 필터링 및 맬웨어 방어를 위한 소프트웨어의 기능 향상을 제공합니다.

Cisco Secure Firewall 라이선싱에는 조직이 Cisco Secure 포트폴리오와 타사 보안 도구에서 얻은 위협 데이터를 신속한 조사와 대응을 촉진할 목적으로 설계된 단일 뷰로 통합하여 상황에 맞는 풍부한 데이터를 한 곳에서 전체적으로 볼 수 있게 해주는 Cisco 의 통합 플랫폼 SecureX 사용 권한이 포함됩니다.

Cisco 는 Total Economic Impact™(TEI)에 대한 연구와 더불어 기업들이 Secure Firewall 을 배포하여 실현할 수 있는 투자 수익률(ROI)에 대한 조사를 Forrester Consulting 에 의뢰했습니다.[1] 이 연구의 목적은 독자들에게 기업 내 Secure Firewall 의 잠재적인 재무 효과를 평가하는 프레임워크를 제공하는 것입니다.

주요 통계



투자 수익률(ROI)
195%

순 현재 가치(NPV)
$12.29M

이를 통해 얻게 되는 이익, 비용 및 리스크를 보다 효과적으로 파악하기 위해, Forrester 는 Secure Firewall 사용 경험이 있는 8 개 기업의 의사 결정권자 10 명을 대상으로 인터뷰했습니다. 이 연구의 목적상, Forrester 는 인터뷰 대상자의 경험을 취합하고 그 결과를 하나의 가상 기업으로 결합했습니다.

이들 인터뷰 대상자는 Secure Firewall 을 사용하기 전에는 각자의 조직에서 네트워크를 적절히 관리하고 효과적으로 보호하는 데 필요한 가시성과 관리 효율성이 얼마나 부족했는지를 언급했습니다. 이러한 가시성과 효율적인 GUI(그래픽 사용자 인터페이스)가 둘 다 없던 시절에는 방화벽 배포, 정책 생성, 방화벽 업그레이드, 정책 업데이트와 같은 네트워크 작업 흐름에 상당한 시간이 걸렸다고 합니다. 위협 조사 및 대응, 원격 액세스 관리와 같은 보안 작업 흐름에도 시간을 추가로 썼습니다. 인터뷰 대상자들은 수요가 많은 기간에는 네트워크 성능이 저하되었고 여러 벤더 솔루션을 관리하는 복잡성에 대해서도 언급했습니다.

Secure Firewall 에 투자한 후에는 위에서 언급한 네트워크 및 보안 작업 흐름에 걸리는 시간이 단축되었을 뿐 아니라, 조직의 전반적인 보안도 강화되었다고 합니다. 그와 동시에, 조직에서는 더 신속한 정책 업데이트, 향상된 네트워크 트래픽 검사, 전반적인 네트워크 성능의 개선으로 직원 생산성을 높이는 한편, 레거시 솔루션을 더 이상 사용하지 하고 그와 관련된 관리 시간 비용을 크게 줄이는 성과도 거두었습니다.

총이익

$18.6M

주요 연구 결과

정량화된 이익. 리스크 조정 후 현재 가치(PV)로 나타낸 정량적 이익:

- **네트워크 운영 작업 흐름을 최대 95% 줄였습니다.** Cisco Secure Firewall 의 최신 기능과 Firewall Management Center 를 통한 관리 용이성 덕분에, 인터뷰 대상자의 조직은 다음과 같이 작업 소요 시간을 줄였습니다.
  - 방화벽 배포 시간 36% 단축.
  - 방화벽 업데이트 시간 90% 단축.
  - 기존 ASA(Adaptive Security Appliances) 5500-X 방화벽에 비해 방화벽 정책 업데이트 시간 95% 단축.
  - FTD(Firewall Threat Defense) 기반 정책의 초기 버전에 비해 방화벽 정책 업데이트 시간 80% 단축.
  - 가상 방화벽 업데이트 시간 80% 단축.
- **보안 조사 및 대응 작업 흐름 시간을 최대 83% 단축했습니다.** 인터뷰 대상자들은 효과적으로 사용하고 분석할 수 있도록 정보가 더 적절히 구성된 Firewall Management Center 를 Cisco Secure Firewall 과 결합하여 보안 전문가의 작업에도 상당한 시간을 아낄 수 있었다고 했습니다. 그들은 잠재적 위협 조사 시간이 49%, 위협 대응 시간은 83% 줄었다고 밝혔습니다. 조직에서는 SecureX 를 Secure Firewall 및 FMC 와 함께 사용함으로써 조사와 대응에 소요된 남은 시간을 77%까지 절약할 수 있었습니다.

> **"우리는 보안에 매우 민감하며 적절한 제품을 활용해 회사의 보안을 지키고 싶습니다. 우리가 Cisco 와 함께한 이유죠. Cisco 는 보안을 가장 중시하는 환경에서 성장한 회사라, 보안이 단순한 추가 기능이 아니죠."**
> *제조 부문 선임 네트워크 엔지니어*

- **보안 침해 리스크를 최대 80% 줄였습니다.** Cisco Secure Firewall 과 Firewall Management Center 가 함께 제공하는 가시성과 제어 기능 덕분에 잠재적인 중대한 보안 침해 리스크와 관련 비용을 줄일 수 있었습니다. 이들 솔루션은 보안 침해 리스크를 기존의 ASA 5500-X 방화벽에 비해 80%, 초기 FTD 기반 방화벽에 비해서는 15% 줄였습니다. 이들 조직에서는 SecureX 를 사용해 보안 침해에 따른 나머지 리스크와 비용을 최대 23% 더 줄일 수 있었습니다.

- **연간 약 2 백만 달러의 가치에 해당하는 최종 사용자 생산성 향상 효과를 거두었습니다.** 인터뷰 대상 조직에서는 Cisco Secure Firewall 과 Firewall Management Center 를 배포해 두 가지 방식으로 생산성을 향상했습니다. 첫째, 네트워크 전문가들이 파괴적인 영향을 주는 정책 업데이트 오류를 80% 더 빠르게 수정할 수 있었습니다. 둘째, 네트워크 성능 저하의 심각성을 줄여 성능 저하의 영향을 받는 각 최종 사용자에게 매년 9 시간에 가까운 작업 시간을 되찾을 수 있었습니다.
- **폐기한 레거시 도구로 인한 비용을 절감했습니다.** 인터뷰 대상자들은 Cisco Secure Firewall 을 사용해 이전에 구현했던 값비싼 레거시 보안 솔루션을 폐기할 수 있었다는 점도 언급했습니다. 그래서 독립 실행형 IPS 에서 연간 수십만 달러, 기존 보안 솔루션의 교체 비용을 쓰지 않아도 됨으로써 수백만 달러, Cisco Secure Firewall 이 더 적은 수의 방화벽으로 같은 수준의 보호를 제공한 데 따라 추가로 25%의 비용을 절감했다고 합니다.

정량화할 수 없는 이익. 이 연구에서 정량화할 수 없는 이익은 다음과 같습니다.

- **VPN 생산성 및 보안 향상.** 또한 Cisco Secure Firewall 을 사용해 로드 밸런싱, 로컬 인증, 다중 인증서 인증을 통해 원격 액세스 VPN 생산성과 보안을 향상할 수 있었습니다. 최종 사용자들은 VPN 을 통해 더 나은 방법으로 연결을 설정할 수 있었고, 조직에서는 액세스를 더 잘 제어할 수 있었습니다.
- **재택 근무를 위한 업무 운영 개선.** Cisco Secure Firewall 제어는 직원이 재택 근무로 전환할 때 VPN 사용이 급증했을 때 업무 운영을 원활히 유지하는 데도 도움이 되었습니다. 네트워크 전문가는 최대 수요 시에도 직원 경험과 생산성 향상을 위해 속도 제한 및 중복성 개선을 활용할 수 있습니다.
- **클라우드로의 용이한 전환.** 마지막으로, 인터뷰 대상자들은 Cisco Secure Firewall 덕분에 사이트 내, 사이트 간, 조직과 여러 클라우드 플랫폼 간의 트래픽을 보호하는 단일 플랫폼을 제공함으로써 클라우드 이니셔티브를 더 쉽게 성취할 수 있다고 밝혔습니다. 특히, Cisco 는 클라우드 플랫폼 마켓플레이스를 통해 Secure Firewall 을 배포하는 표준화된 정책과 검증된 수단을 제공합니다.

비용. 리스크 조정 후 PV 비용에는 다음 항목이 포함됩니다.

- **라이선스 비용.** 라이선스 비용이 인터뷰 대상자의 조직에서 발생한 가장 큰 비용이었지만, Cisco 기업 계약을 체결함으로써 조직이 이전에는 부족했던 추가 기능과 솔루션에 수십만 달러를 절약하면서도 조직의 보안 상태는 한층 더 강화했습니다. Secure Firewall 에는 SecureX 라이선스 권한이 포함됩니다.
- **구현, 정책 생성 및 교육 비용.** 인터뷰 대상자들은 방화벽의 구현과 배포, 방화벽에 대한 정책 생성에 내부 비용이 든다고 말했습니다. 방화벽 배포에는 사이트당 6 시간이 소요될 것으로 예상되는 반면, 정책 생성에는 대략 30 시간이 걸립니다. SecureX 를 구현하려면 추가로 20 시간, 지속적 관리를 위해 연간 100 시간의 작업이 필요합니다. 일부 인터뷰 대상자는 Cisco Secure Firewall 과 Firewall Management Center 를 사용하기 위해 네트워크 및 보안 전문가를 교육할 필요가 있다고 언급했습니다. 인터뷰 대상자에 따르면 Cisco 보안 전문가가 출연하는 공개 교육 동영상을 활용할 경우 교육을 위한 내부 비용으로 직원당 2 시간의 시간 비용이 들었습니다.

의사 결정권자 인터뷰와 재무 분석 결과, 가상 기업이 3 년간 얻은 이익은 1,859 만 달러이고 비용은 630 만 달러가 들어, 1,229 만 달러의 최대 순현재가치(NPV)와 195%의 투자자본수익률을 달성하는 것으로 나타났습니다.

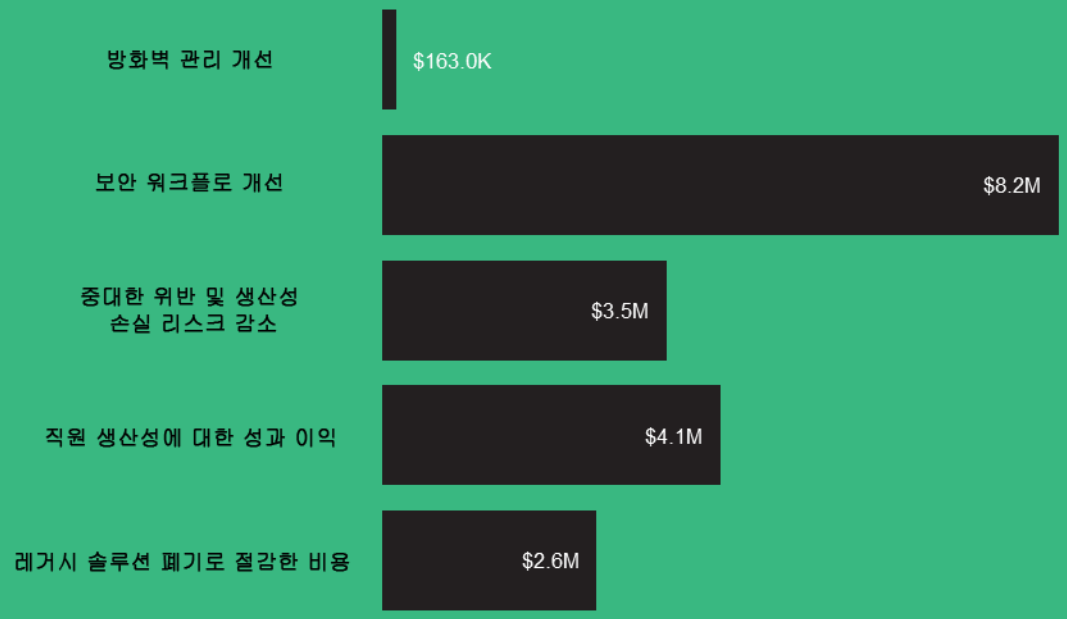
투자자본수익률(ROI)
195%

이익 PV
$18.59M

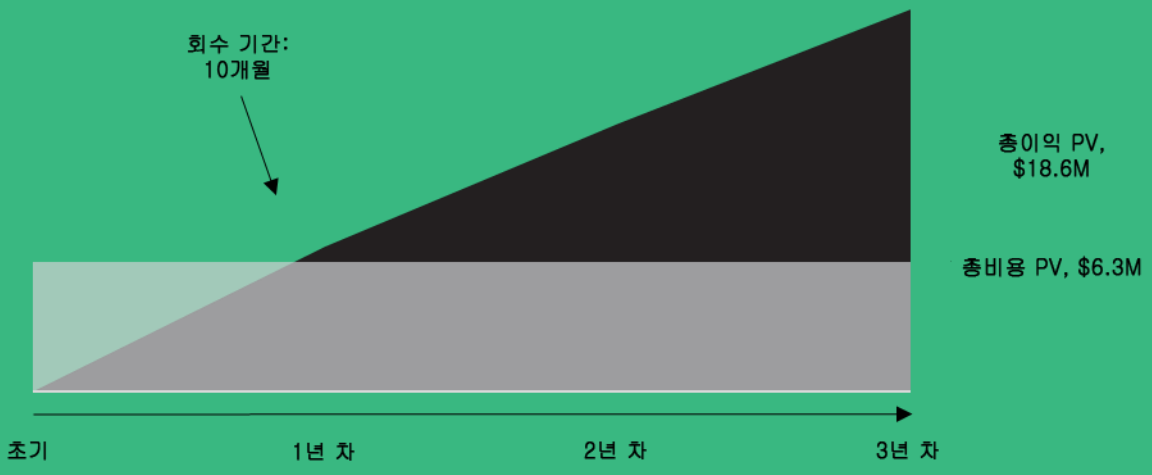
순현재가치(NPV)
$12.29M

원금 회수
10 개월

이익(3년)



재무 개요



TEI(총 경제적 영향)의 프레임워크 및 방법론

인터뷰에서 제공된 정보를 통해 Forrester 는 Cisco Secure Firewall 에 투자를 고려 중인 기업들을 대상으로 Total Economic Impact™ 프레임워크를 만들었습니다.

이 프레임워크의 목적은 투자 결정에 영향을 미치는 비용, 이익, 유연성 및 리스크 요소를 파악하는 것입니다. Forrester 는 다단계적인 접근 방식으로 Secure Firewall 이 기업에 미치는 효과를 평가했습니다.

실사

Cisco 이해 당사자 및 Forrester 분석가들과의 인터뷰를 통해 Secure Firewall 과 관련된 데이터를 수집했습니다.

의사 결정권자 인터뷰

Secure Firewall 을 사용 중인 기업의 의사 결정권자 10 명과의 인터뷰를 통해 비용, 이익 및 리스크 요소와 관련된 데이터를 수집했습니다.

가상 기업

인터뷰 대상 기업들의 특성을 기반으로 하나의 가상 기업을 만들었습니다.

재무 모델 프레임워크

TEI 방법론을 사용하여 인터뷰의 대표 재무 모델을 구성하고 의사 결정권자들의 문제와 관심을 기반으로 재무 모델의 리스크 조정을 수행했습니다.

사례 연구

투자 효과를 모델링할 때 TEI(총 경제적 영향)의 4 가지 기본 요소인 이익, 비용, 유연성 및 리스크를 사용했습니다. IT 투자와 관련된 ROI 분석이 점점 복잡해지고 있음을 고려해, Forrester 는 TEI 방법론을 통해 구매 결정에 대한 TEI(총 경제적 영향)를 한눈에 볼 수 있도록 만들었습니다. TEI 방법론에 대한 자세한 내용은 부록 A 를 참조하십시오.

공지

독자 유의 사항:

이 연구는 Cisco 의 의뢰를 받아 Forrester Consulting 에서 수행한 것으로 경쟁 제품과의 비교 분석 목적으로 사용될 수 없습니다.

Forrester 는 다른 기업들이 얻을 수 있는 잠재적인 ROI 에 대해 어떠한 가정도 하지 않습니다. Secure Firewall 에 대한 투자 여부는 이 연구에서 제공하는 정보를 기반으로 독자들이 자체적으로 판단하시기 바랍니다.

Cisco 는 Forrester 의 보고서를 검토하고 피드백을 제공했습니다. 그러나 Forrester 는 연구 및 결과에 관한 편집 권한을 보유하며, Forrester 의 조사 결과에 반하거나 연구의 의미를 모호하게 하는 변경 요구는 수락하지 않습니다.

Cisco 는 인터뷰 대상 고객들의 이름을 제공했지만 인터뷰에 참여하지는 않았습니다.

Cisco Secure Firewall 고객 여정

Secure Firewall 투자로 이어지는 주요 요인

인터뷰 대상 의사 결정권자

인터뷰 대상자	업종	지역	총 직원 수
엔지니어링 서비스 관리자	IT 서비스	북미	750
책임 인프라 엔지니어	금융 서비스	북미	2,800
통신 및 텔레포니 서비스 부 관리자	금융 서비스	북미	2,800
수석 사이버 보안 엔지니어	보안 서비스	북미	3,000
선임 네트워크 엔지니어	제조	글로벌	5,500
네트워크 엔지니어링 선임 관리자	기술	글로벌	40,000
선임 보안 엔지니어	기술	글로벌	40,000
보안 운영팀장	교육	북미	46,000
직원 인프라 아키텍트	산업	글로벌	205,000
선임 네트워크 엔지니어	기술	글로벌	275,000

주요 과제

Cisco Secure Firewall 및 Firewall Management Center 를 배포하기 전, 인터뷰 대상자들이 속한 조직에서는 환경 보호를 위해 기존의 ASA 5500-X 기반 방화벽 어플라이언스를 주로 활용하고 있었습니다. 일부 인터뷰 대상자는 몇 년 전에 기존의 ASA 기반 방화벽에서 초창기 FTD 기반 방화벽으로 전환했는데, Cisco Secure Firewall 및 Firewall Management Center 에서 최신 버전의 FTD 로 업그레이드한 후 추가적인 이익을 얻었다고 말했습니다.

인터뷰 대상자들은 각 조직이 공통적으로 어떤 어려움을 겪었는지에 대해 다음과 같이 언급했습니다.

- **제한적 가시성.** 인터뷰 대상자들은 ASA 5500-X 기반 방화벽에 의존했던 이전 환경에서는 전체 보안에 대한 가시성이 제한적이었다고 밝혔습니다. 통합이 부족하다는 점이 한 가지 원인이었습니다. 이전 환경에서는 인터뷰 대상자의 조직에서 다양한 보안 솔루션을 통합하여 통합 관리와 일관된 정책을 확립하는 동시에 한 가지 버전의 신뢰할 수 있는 정보를 얻기 어려웠습니다. 가시성 제한의 또 다른 이유는 이전 환경에서는 중앙에서 포트 검사에 의존해 네트워크를 보는 방식이었기 때문입니다. 인터뷰 대상자들은 그 점 때문에 애플리케이션에 대한 가시성과 과거 컨텍스트가 제한되어 데이터를 더 깊이 들여다볼 수 없었다고 했습니다.

> **"이전에는 현대적인 애플리케이션 제어와 같은 역량이 부족했습니다. 사용자가 네트워크를 어떻게 사용하고 있는지 알 수 없었고 이러한 사용에 적절히 대응하지 못했습니다."**
> *교육 부문 보안 운영팀장*

- **방화벽 구현과 관리에 드는 시간 비용이 많습니다.** 인터뷰 대상자들은 레거시 방화벽 배포와 관리에 시간이 많이 걸린다는 점도 지적했습니다. 이 중 대부분은 한 번에 여러 장치에 업데이트를 푸시하지 못했기 때문입니다. 교육 부문에서 일하는 보안 운영팀장은 간단한 방화벽 규칙을 배포하는 데 45 분에서 1 시간이나 걸렸던 것으로 추정했습니다. 또한 인터뷰 대상자들은 이전 환경의 가시성 부족으로 인해 보안 상태를 확인하려고 서로 다른 시스템 간의 데이터 상관 관계를 밝히는 데 지나치게 많은 시간을 써야 했다고 언급했습니다.

"관리 및 통합이 쉽다는 점이 Cisco 의 장점 중 하나였죠. 우리는 다양한 시스템이 서로에게 데이터를 더 쉽게 공급함에 따라 데이터가 풍부해진 이점도 누립니다. 또한 특정 위협에 대한 자율적 대응을 확립했습니다. 전에는 이런 일 중 어떤 것도 할 수 없었습니다."
보안 서비스 부문 수석 사이버 보안 엔지니어

- **낮은 성능.** 인터뷰 대상자들은 이전 시스템의 낮은 성능 부분도 지적했습니다. 예를 들어, 교육 부문의 보안 운영팀장은 네트워크 및 보안 인프라에 대한 수요가 급증할 때 이전 솔루션이라면 "갑자기 중단된 후 끊임없이 재부팅하면서 패킷을 삭제할 것"이라고 말했습니다. 이는 "네트워크를 활용해 동영상을 재생하거나 수업 시간에 뭔가를 시연하는 교수는 그렇게 할 수 없다"는 것과 같이, 생산성에 영향을 미치기까지 했습니다.

- **벤더 관리.** 마지막으로, 고객은 이전 환경에서는 벤더가 여럿이면 벤더 관리가 골칫거리였다고 했습니다. 금융 서비스 회사의 책임 인프라 엔지니어는 "벤더가 여럿이면 모든 일을 여러 번 해야 했기에, 여러 컨트롤 플레인에 액세스하여 서로 다른 시스템에서 똑같은 변경 사항이나 업데이트를 적용해야 했습니다"라고 말했습니다.

가상 기업

Forrester 는 인터뷰를 근거로 TEI 프레임워크, 가상 기업, 재무 영향 ROI 분석을 구성했습니다. 이 가상 기업은 Forrester 가 인터뷰한 9 명의 의사 결정권자를 나타내며, 다음 장에 이 조직의 재무 분석 결과가 나와 있습니다. 가상 기업의 특징은 다음과 같습니다.

가상 기업에 대한 설명. 이 가상 기업은 연간 매출이 50 억 달러이고 직원이 16,000 명인 B2B 기술 조직입니다. 전 세계 곳곳에 고객이 있습니다. 이 조직은 데이터 센터에 저장된 데이터에 대한 일관된 클라이언트 액세스를 보장하도록 데이터 센터에서 고가용성이 필수적입니다. 또한 이러한 데이터 센터는 원치 않는 액세스나 공격으로부터 중요한 클라이언트 데이터를 보호하기 위해 보안을 강화해야 합니다. 데이터 센터 외에도, 이 조직에서는 멀티클라우드를 사용하여 보다 분산된 접근 방식으로 옮겨가고 있습니다. 또한 이 조직에서는 Secure Firewall 을 사용하여 엣지 사이트/지사 사무실을 보호하고 있기도 합니다.

배포 특성. 가상 기업은 Cisco 차세대 방화벽에 이미 투자했습니다. 방화벽 재고의 2/3 는 Cisco Firepower 장치로 구성되어 있고, 1/3 은 ASA 5500-X 방화벽으로 구성되어 있습니다. 가상 기업은 현재 102 개의 홈 오피스, 데이터 센터, 본사에 있는 방화벽을 전부 최신 버전의 Cisco Secure Firewall 로 전환하고, 68 개의 Firepower 장치를 업데이트하며, 34 개의 ASA 기반 장치를 교체하는 중입니다. 일부 인터뷰 대상자는 하드웨어를 교체하지 않고 기존의 전통적 장치를 FTD 소프트웨어로 업데이트하기로 했습니다. 가상 기업은 또한 데이터 센터에 Cisco Secure Firewall 가상 방화벽을 배포하여 데이터 센터와 지사 간의 East-West 트래픽은 물론이고 데이터 센터와 여러 공용 클라우드 플랫폼 간의 트래픽도 처리합니다. SecureX 가 Secure Firewall 라이선스에 포함된 점을 이용해 보안팀의 위협 조사 및 대응 작업을 더욱 강화합니다.

주요 가정

- 매출 **50** 억 달러
- 직원 **16,000** 명
- **ASA** 기반 방화벽 **34** 개 교체
- **Firepower** 방화벽 **68** 개를 최신 **Cisco Secure Firewall** 로 업데이트

이익 분석

가상 기업에 적용된 정량화된 이익 데이터

총이익						
참조	이익	1 년 차	2 년 차	3 년 차	합계	현재 가치
Atr	방화벽 관리 개선	$134,951	$25,556	$25,556	$186,064	$163,005
Btr	보안 워크플로 개선	$2,669,879	$3,685,484	$3,685,484	$10,040,848	$8,241,976
Ctr	중대한 위반 및 생산성 손실 리스크 감소	$1,291,446	$1,393,402	$1,520,848	$4,205,696	$3,468,249
Dtr	직원 생산성에 대한 성과 이익	$1,656,403	$1,656,403	$1,656,403	$4,969,210	$4,119,230
Etr	레거시 솔루션 폐기로 절감한 비용	$1,985,115	$503,513	$503,513	$2,992,142	$2,599,074
	총이익(리스크 조정 후)	$7,737,795	$7,264,360	$7,391,805	$22,393,959	$18,591,534

방화벽 관리 개선

근거와 데이터. 레거시 방화벽에서 전환하든 초기 버전의 Firepower Threat Defense 에서 업데이트하든 상관없이, 인터뷰에 참여한 의사 결정권자들은 Cisco Secure Firewall 을 배포한 후 방화벽 관리와 관련된 시간과 비용을 절약했다고 언급했습니다. 이러한 개선의 상당 부분은 네트워킹 전문가가 Firewall Management Center 를 사용해 단일 창을 통해 다수의 장치로 변경 사항을 푸시할 수 있는 방화벽의 중앙 집중식 관리 기능의 지원을 받는다는 사실에서 비롯되었습니다.

"FMC 는 우리가 이전에 하던 방식대로 서로 다른 여러 방화벽을 따로 관리하는 대신 한 곳에서 방화벽을 관리하고 업그레이드할 수 있도록 되어 있습니다."
IT 서비스 부문 엔지니어링 서비스 관리자

인터뷰 대상자의 조직에서는 방화벽 배포와 관련된 시간과 비용을 절감했다고 합니다. 인터뷰 대상자들은 기존의 ASA 기반 방화벽을 사용할 때는 방화벽 배포에 상당한 시간이 걸렸는데, 사용 사례별 방화벽 규칙을 작성해 다양한 방화벽 정책에 수동으로 배포해야 했다고 말했습니다.

"우리는 Cisco Secure Firewall 을 사용해 새로운 방화벽을 신속하게 구축하고 배포할 수 있었습니다. 방화벽을 확장하면서 직원을 늘릴 필요가 없었죠."
기술 부문 네트워크 엔지니어링 선임 관리자

Cisco Secure Firewall 과 Firewall Management Center 로 전환한 후, 인터뷰 대상자들은 방화벽 배포 시간을 30~40% 정도 단축했다고 합니다. 시간 단축은 Cisco Secure Firewall 의 배포 자동화에 따른 효과였습니다. 예를 들어, 기술 업계의 네트워크 엔지니어링 선임 관리자는 이렇게 말했습니다.

"우리는 Cisco Secure Firewall 로 배포를 자동화했어요. 방화벽 시스템을 완성하고 IP 를 설정하고 섀시를 구성하고 정책을 적용하는 과정을 자동화한 거죠."

"기본 제공되는 자동화 기능이 시간을 가장 많이 절약해줘요. 업그레이드 시간은 훨씬 더 줄었죠. 이젠 더 이상 ASA 를 사용하던 시절처럼 업그레이드 프로세스 내내 지켜보고 있을 필요가 없어요. 자리를 비워도 되고, 설령 충분한 시간 내에 온라인 상태로 복귀하지 않더라도 Firepower 가 알려줘요."
기술 부문 네트워크 엔지니어링 선임 관리자

자동화는 배포 후 Cisco Secure Firewall 을 관리하고 유지하는 문제에서도 인터뷰 대상자에게 큰 도움이 되었습니다. Cisco Secure Firewall 에는 자동화된 업그레이드 기능이 기본으로 제공됩니다. 인터뷰 대상자들은 ASA 기반 방화벽을 업그레이드할 때는 방화벽 사이를 옮겨 다니고 업데이트 파일을 업로드하고 시스템을 다시 부팅하느라 많은 시간이 걸릴 수도 있었다고 합니다. 하지만 Cisco Secure Firewall 과 Firewall Management Center 를 도입한 후로는 인터페이스에서 몇 번만 클릭해 방화벽을 업그레이드한 다음 30 분 후에 업그레이드가 성공했는지 확인하기만 하면 된다고 말했습니다.

인터뷰 대상자들은 Cisco Secure Firewall 과 Firewall Management Center 를 도입함에 따라 객체 지향 시스템을 사용해 긴 ACL(액세스 제어 목록) 없이도 정책을 카테고리와 영역으로 나누어 구성할 수 있다고 했습니다. 또한 각 장치를 수동으로 업데이트하는 것과는 반대로, 지금은 정책을 자동으로 배포하고 업데이트할 수도 있습니다.

"Cisco Secure Firewall 은 정책의 90%를 자동으로 배포해 줍니다. 우리는 더 이상 일회성 구성 문제를 다루지 않는답니다."
기술 부문 네트워크 엔지니어링 선임 관리자

인터뷰 대상자들은 Cisco Secure Firepower 를 사용해 초기 FTD 에서 후기 FTD 로 업그레이드한 후 시간을 추가로 절약했다고 언급했습니다. 예를 들어 금융 서비스 부문의 책임 인프라 엔지니어는 초기 FTD 에서는 정책 배포에 10~15 분이 걸렸지만 업그레이드된 FTD 에서는 배포 시간이 약 3 분으로 줄었다고 합니다.

"ASA 에서 Cisco Secure Firewall 로 옮긴 후 시간이 지나면서 정책 관리 비용이 60%~70% 절감되는 효과를 누리고 있어요."
IT 서비스 부문 엔지니어링 서비스 관리자

"Cisco Secure Firewall 을 사용하면 간단하고 쉽게 정책을 관리할 수 있습니다. Firewall Management Center GUI 는 가볍고 깔끔하며 직관적으로 작동하죠."
기술 부문 네트워크 엔지니어링 선임 관리자

인터뷰 대상자 중 한 명은 Firewall Management Center 가 아니라 클라우드 SaaS(Software-as-a-Service) CDO(Cisco Defense Orchestrator) 관리 기능을 사용하고 있었습니다. CDO 에 관해, 산업 부문의 직원 인프라 아키텍트는 이렇게 말했습니다. “CDO 채택 과정이 너무나 순조로웠습니다. 우리 회사 엔지니어들은 이미 CSM(Cisco Security Manager)에 익숙했기에, 명령줄 인터페이스를 조작하고 매크로를 빌드할 수 있었거든요. 다른 벤더로 전환하려면 새로운 상위 계층 개념을 배워야 하는 복잡한 문제가 있는데, 그에 비하면 훨씬 쉬운 일이었죠.”

모델링 및 가정. 가상 기업에 대해 Forrester 는 다음과 같이 모델링합니다.

- 기존의 ASA 5500-X 방화벽 34 개를 Cisco Secure Firewall 로 바꿉니다.
- 이 가상 기업에서는 교체된 기존의 방화벽 각각에 대해 정책을 만들고 배포하는 데 걸렸을 55 시간의 노동 시간을 절약합니다.
- 분기별로 각 방화벽을 업그레이드하는 데 걸렸던 30 분의 시간 중 90%를 절약합니다.
- 가상 기업은 평균적으로 하루에 한 번 방화벽 정책을 업데이트합니다. Cisco Secure Firewall 로 전환함으로써, 이러한 업데이트를 각각 수행할 때마다 1 시간씩 걸리던 시간 중 95%를 줄일 수 있습니다.
- 네트워크 보안 운영(NetSecOps) 전문가의 평균 총 부담 시급은 65 달러입니다.
- 68 개의 FTD 방화벽을 최신 버전의 Cisco Secure Firewall 로 업그레이드합니다. 각 일일 정책 업데이트에 대해 가상 기업은 초기 세대 FTD 방화벽에서 걸리는 시간의 80%를 절약합니다.
- 또한 가상 기업은 가상 방화벽 정책을 업데이트하는 데 걸리던 시간의 80%를 절약합니다.

리스크. 방화벽 관리 개선 사항은 다음 사항에 따라 다를 수 있습니다.

- 기존 방화벽의 종류와 개수.
- Cisco Secure Firewall 로 교체된 방화벽의 수와 배포 속도.
- 데이터 센터에 가상 방화벽을 배포하여 East-West 및 공용 클라우드 트래픽을 처리한다는 결정.

결과. 이러한 리스크를 감안해 혜택을 10% 낮춘 결과, 3 년에 걸친 리스크 조정 후 총 PV(10% 할인)가 약 163,000 달러로 산출되었습니다.

방화벽 관리 개선

참조	기준	출처	1 년 차	2 년 차	3 년 차
A1	레거시 방화벽을 대체하는 차세대 방화벽의 수	가상 기업, 총 102 개 중 1/3	34	0	0
A2	각 방화벽 배포에 대해 절감된 시간	인터뷰	55.00	55.00	55.00
A3	각 ASA 방화벽 업데이트에 대해 절감된 시간	분기당 90%*17 시간	61.2	61.2	61.2
A4	ASA 방화벽에 대한 정책의 수동 업데이트에 대해 절감된 시간	95%*1 시간, 하루에 한 번*환경의 33%	114	114	114
A5	NetSecOps 전문가의 시급	가상 기업	$65	$65	$65
A6	소계: 레거시 레이어 4 방화벽에서 차세대 방화벽으로 업그레이드하고 배포하는 시간 단축	((A1*A2)+(A3+A4))*A5	$132,938	$11,388	$11,388
A7	업데이트된 FTD 방화벽 수	가상 기업, 총 102 개 중 2/3	68	68	68
A8	이전에 초기 FTD 로 정책을 배포할 때 걸린 시간	인터뷰	0.25	0.25	0.25
A9	최신 FTD 로 업그레이드한 후 정책 배포에서 단축된 시간	인터뷰, 15 분에서 3 분으로 단축	80%	80%	80%
A10	소계: 이전의 레이어 7 방화벽에서 Firepower 에 정책을 배포하는 시간 단축	365*A8*A9*A5*A7/102	$3,163	$3,163	$3,163
A11	가상 방화벽 총 수	가상 기업	100	100	100
A12	가상 방화벽 정책 업데이트 시 연간 절약 시간	연간 80%*266 시간	213	213	213
A13	소계: 가상 방화벽 관리에서 단축된 시간	A12*A5	$13,845	$13,845	$13,845
At	방화벽 관리 개선	A6+A10+A13	$149,946	$28,396	$28,396
	리스크 조정	↓10%			
Atr	방화벽 관리 개선(리스크 조정 후)		$134,951	$25,556	$25,556
	3 년 총계: $186,064		**3 년 현재 가치: $163,005**		

보안 워크플로 개선

근거와 데이터. Cisco Secure Firewall 배포와 FMC 활용은 인터뷰 대상자가 보안 워크플로를 간소화하는 데도 도움이 되었습니다. 의사 결정권자들은 ASA 기반 장치가 방화벽 전체에서 이벤트를 추적하고 기록하기 위해 여러 개의 도구가 따로 필요했다고 언급했습니다. FMC 도입으로, Cisco Secure Firewall 데이터는 IOC(Indicators of Compromise: 침해 지표)와 차단된 침입을 추적하거나 SIEM(Security Information and Event Management: 보안 정보 및 이벤트 관리) 솔루션으로 일관되게 상향 조정할 수 있는 한 곳으로 통합되었습니다. 인터뷰 대상자들은 FMC 를 사용하면서 전체 네트워크에서 보다 상관관계가 높은 방식으로 연결, 이벤트, 원격 측정을 전체적으로 검토하는 능력을 얻었습니다.

> **"예전에는 보안 조사가 한 조각만으로 퍼즐을 만드는 것과 같은 느낌이었어요."**
> *교육 부문 보안 운영팀장*

인터뷰 대상자들은 Firewall Management Center 를 통한 통합으로 보안 조사 작업의 시간 비용이 줄었다고 답했습니다. 예를 들어, 보안 서비스 업계의 수석 사이버 보안 엔지니어는 Secure Firewall 과 Firewall Management Center 의 도움으로 조사 시간이 몇 시간 정도 걸리던 데서 3~5 분으로 줄었다고 합니다. 이 엔지니어는 이전에는 SIEM 및 이메일 콘솔을 포함한 여러 시스템을 거쳐 로그인하고 데이터를 조정해야 했다고 말합니다. 하지만 이제는 FMC 에 로그인하면 FMC 환경 내에서 특정 IOC 를 찾을 수 있습니다.

"Firewall Management Center 는 모든 Cisco Secure Firewall 을 관리하는 단일 콘솔 역할을 합니다. 관리가 쉬워졌고 이벤트 조사와 대조, 악의적인 활동에 관한 결정을 내리는 데 드는 시간이 줄었어요."
IT 서비스 부문 엔지니어링 서비스 관리자

인터뷰 대상자들은 대응 시간도 단축되었다고 말했습니다. 예를 들어, 교육 업계에 종사하는 이 보안 운영 팀장은 Cisco Secure Firewall 에 투자하기 전에는 매주 여러 번 고객 지원팀에 티켓을 보내야 했다고 합니다. 그러면 지원팀에서 사용자를 추적하고 맬웨어 테스트를 실행하는데, 검사 작업에 몇 시간이 걸릴 수도 있었습니다. 그런 다음, 해당 팀에서 시스템을 정리하거나 심지어 이미지를 다시 만들기도 했습니다. 이 과정은 길게는 하루 종일 걸릴 수도 있습니다. 이 인터뷰 대상자는 Cisco Secure Firewall 을 사용하여 비슷한 티켓을 한 달에 한 번 보내고 FMC 로 바로 이동하여 문제를 해결하는데, 약 1 시간 정도 걸립니다.

"기존 방화벽에서는 보안 사고 대응을 실행하는 데 필요한 오버헤드가 많았어요. 시간과 비용이 많이 들었죠. Firepower 를 사용하면서 침입 차단 효과가 커지면서 시간이 크게 절약되고 사고 대응이 훨씬 줄어든 모습이 보여요."
교육 부문 보안 운영팀장

FTD 의 초기 버전에서 업데이트된 버전으로 이동한 인터뷰 대상자들은 보안 조사 및 대응 워크플로와 관련된 이익도 누렸습니다. 금융 서비스 부문의 책임 인프라 엔지니어가 응답한 바와 같이, 이전 버전의 FTD 에서 여전히 Firewall Management Center 를 통해 보안 경고를 한눈에 볼 수는 있었지만, 업그레이드 후에는 경고에 대한 정의 및 트리거 기능이 향상되었습니다. 이 인터뷰 대상자는 또한 AMP 및 Umbrella 를 포함한 Cisco 제품과의 추가 통합이 추가적인 상관 관계를 통해 훨씬 더 많은 이익을 제공했다고 합니다.

"FMC 는 뛰어난 가시성을 제공해요. 이제는 이러한 가시성 덕분에 모든 것이 정상인지 살펴보고 확인하는 데 더 많은 시간을 쓰고 있어요. 그래도 사고 대응에 쓰던 시간보다는 줄었답니다."
교육 부문 보안 운영팀장

SecureX 가 Secure Firewall 라이선싱에 포함된 이점을 활용한 조직에서는 가시성과 사용자 지정을 통해 보안팀의 운영 효율성을 더욱 개선했습니다. 예를 들어, 교육 부문의 보안 운영팀장은 SecureX 가 개인화되고 사용자 지정 가능한 대시보드를 허용하므로, 환경에 대한 팀의 가시성이 더욱 향상되었을 뿐 아니라 다양한 사용자에게 자신의 책임에 대해 가장 중요한 정보를 보여줄 수도 있다고 말했습니다.

모델링 및 가정. 가상 기업에 대해 Forrester 는 다음과 같이 모델링합니다.

- 연간 총 보안 경고 수 100,000 건.
- 그중 26%는 보안 분석가의 주의가 필요합니다.
- 주의가 필요한 경고 중 70%는 조사도 필요합니다.
- Cisco Secure Firewall 과 Firewall Management Center 는 경고를 조사하는 데 걸렸던 2.8 시간 중 49%를 절감해 줍니다.
- 조사가 필요한 경고의 10%는 대응이 필요합니다.
- Cisco Secure Firewall 과 Firewall Management Center 는 대응하는 데 걸렸던 6 시간 중 83%를 절감해 줍니다.
- SecureX 를 사용하면 조사 및 대응 워크플로에 걸리는 시간을 1 년 차에 42%, 2 년 차와 3 년 차에 77% 추가로 단축할 수 있습니다.

리스크. 보안 워크플로에 대한 개선 사항은 다음 사항에 따라 다를 수 있습니다.

- 연간 경고, 주의가 필요한 경고, 조사가 필요한 경고, 대응이 필요한 경고의 수.
- NetSecOps 전문가의 총 부담 시급.

결과. 이러한 리스크를 감안해 이익을 15% 감소시킨 결과, 3 년간 리스크 조정 후 총 PV 가 820 만 달러 이상이 산출되었습니다.

보안 워크플로 개선					
참조	**기준**	**출처**	**1 년 차**	**2 년 차**	**3 년 차**
B1	연간 경고 총 수	가상 기업	100,000	100,000	100,000
B2	분석가의 주의가 필요한 경고 수	Forrester 연구, 26%	26,000	26,000	26,000
B3	조사가 필요한 경고의 비율	인터뷰	70%	70%	70%
B4	이전의 평균 조사 시간	인터뷰	2.8	2.8	2.8
B5	FMC 에서의 조사 시간 단축	인터뷰	49%	49%	49%
B6	대응이 필요한 경고 수	인터뷰	260	260	260
B7	이전의 평균 대응 시간	인터뷰	6	6	6
B8	FMC 에서의 대응 시간 단축	인터뷰	83%	83%	83%
B9	SecureX 에서의 조사 및 대응에 대한 추가적인 절감	인터뷰	42%	77%	77%
B10	보안 전문가의 총 부담 시급	A5	$65	$65	$65
Bt	보안 워크플로 개선	((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10	$3,141,034	$4,335,864	$4,335,864
	리스크 조정	↓15%			
Btr	보안 워크플로 개선(리스크 조정 후)		$2,669,879	$3,685,484	$3,685,484
	3 년 총계: $10,040,848		**3 년 현재 가치: $8,241,976**		

중대한 위반 및 생산성 손실 리스크 감소

근거와 데이터. 인터뷰 대상자들은 또한 Cisco Secure Firewall 을 배포한 후 중대한 위반 리스크 및 관련 생산성 비용 감소와 관련된 재정적 이익을 봤다고 했습니다.

인터뷰 대상 조직의 보안 상태를 개선한 한 가지 수단은 Cisco Secure Firewall 및 Firewall Management Center 가 제공하는 추가적 가시성에서 비롯된 것이었습니다. 예를 들어, 교육 부문의 보안 운영팀장은 이렇게 언급했습니다. "기존 ASA 에 비해 Cisco Secure Firewall 은 더 나은 가시성을 제공합니다. 사용자들이 점점 더 많은 휴대기기를 네트워크에 접속해 사용하고 네트워크를 통한 인쇄와 같은 서비스에 액세스함에 따라 이 점이 특히 중요합니다. Firepower 로 업그레이드하면 가시성과 내부 네트워크 트래픽뿐 아니라 남-북 트래픽의 필터링 능력이 향상됩니다."

> **"우리는 위협 및 IOC 차단 건수가 대폭 개선되는 효과를 보았습니다. 엄청난 차이가 나죠. Secure Firewall 을 실행하지 않았던 예전에는 매일 비즈니스가 위험한 상황에 처했습니다. 이제는 가시성이 향상되어 리스크가 헤아릴 수 없을 정도로 감소했습니다. 지금은 마음이 놓입니다."**
> *IT 서비스 부문 엔지니어링 서비스 관리자*

개선된 자동 차단은 성공적인 보안 위반의 잠재적 리스크를 줄이는 데도 도움이 되었습니다. 기술 부문의 네트워크 엔지니어링 선임 관리자는 이렇게 말했습니다. “Firepower 는 IPS(침입 방지 시스템)의 업계 리더입니다. 보안 상태를 강화하고 즉시 문제를 해결할 수 있었습니다. 모든 잠재적 사고에 대해 조기에 문제를 수정해 비용을 절감합니다.” 해당 고객은 ASA 기반 시스템에서 Cisco Secure Firewall 로 이전함으로써 차단 능력이 80% 향상되었다고 알려주었습니다.

“우리는 Secure Firewall 을 사용해 인원을 증원할 필요 없이 위협의 80%를 즉시 제거했습니다.”
기술 부문 네트워크 엔지니어링 선임 관리자

인터뷰 대상자들이 FTD 방화벽을 최신 버전으로 업데이트하여 차단 기능도 강화했다고 언급한 점이 중요합니다. 이 기술 회사의 선임 네트워크 엔지니어는 최신 버전의 FTD 로 업그레이드하면 이전 버전보다 10%에서 15% 더 많이 자동화된 차단이 가능해졌다고 합니다.

이 인터뷰 대상자는 자동 차단이 미칠 수 있는 영향에 대한 일화도 공유해 주었습니다. “우리는 소셜 엔지니어링을 기반으로 한 피해를 당할 뻔한 적이 있는데, 해커가 인증된 사용자로부터 24 시간 액세스 토큰을 얻어내 벌인 일이었죠. 해커가 토큰을 사용하려 할 때 Cisco Secure Firewall 이 그걸 막아주었어요. 우리는 보안 상태를 점검해 공격자가 회사 컴퓨터를 사용 중인지 확인할 수 있었거든요. Secure Firewall 이 해커 VPN 액세스를 자동으로 거부했기에 피해를 막을 수 있었어요. Secure Firewall 이 없었다면 해커가 우리 회사 네트워크에 액세스했을 것이고, 그러면 우리가 어떤 끔찍한 피해를 당했을지 알 수 없어요.”

“Cisco Secure Firewall 은 원스톱 서비스입니다. 다른 도구와의 모든 통합 기능을 보유하고 있어 보안에 도움이 되는 적절한 데이터를 제공해 줍니다. 다양한 요구에 부응하죠. 다양한 처리량 요구 사항을 충족시킬 수 있고 수직적 확장과 수평적 확장을 모두 지원해요. 오늘날의 보안 리스크를 해결하는 데 필요한 모든 기능을 갖춘 이 제품은 계속 개선되고 있습니다.”
인터넷 부문 선임 네트워크 엔지니어

기술 회사의 이 선임 네트워크 엔지니어는 Secure Firewall 이 애플리케이션 수준에서 액세스를 관리할 수 있다는 점에서 생기는 보안상의 이점도 언급했습니다. “우리 회사 게스트 네트워크에서 BitTorrent 가 엄청나게 사용되고 있다는 걸 알았어요. 우리는 FTD 를 활용해 BitTorrent 를 차단함으로써 다른 게스트에 대한 잠재적 위협을 방지할 뿐 아니라 회선 사용률을 약 400Mbps 줄였습니다.”

인터뷰 대상자들은 애플리케이션 계층 감지 및 차단 외에도 Cisco Secure Firewall 이 Snort 기반의 자동화된 위협 피드를 사용해 침입에 성공한 중대 보안 위반에 따른 조직의 리스크도 감소했다고 말했습니다. 금융 서비스 부문의 책임 인프라 엔지니어는 이렇게 말했습니다. “우리는 패치가 적용되지 않은 채로 인터넷에 노출된 서버와 같은

것을 찾거나 악성 트래픽을 전면적으로 차단하는 Snort 의 추가적 가시성과 자동화된 대응을 위해 Cisco Secure Firewall 을 원했습니다."

SecureX 가 Secure Firewall 라이선스에 포함된 점을 이용한 조직에서는 중대한 위반의 리스크와 비용을 더욱 줄였습니다. 예를 들어, 금융 서비스 조직의 책임 인프라 엔지니어는 SecureX 를 사용해 보안 문제 식별과 잠재적 위협의 근본 원인 파악을 위해 훨씬 더 많은 가시성을 확보할 수 있었다고 언급했습니다.

"SecureX 를 통해 한 곳에서 전체 보안 환경을 파악할 수 있습니다. 우리는 FMC 를 사용해 모든 방화벽을 살펴보고 SecureX 를 사용해 FMC 뿐 아니라 모든 통합 Cisco 보안 솔루션을 확인합니다."
교육 부문 보안 운영팀장

모델링 및 가정. 가상 기업에 대해 Forrester 는 다음과 같이 모델링합니다.

- 이전의 중대 보안 위반 건수는 연간 3 건.
- 중대 위반으로 인한 내부 및 외부 평균 총비용은 968,480 달러입니다.
- 외부 공격, 내부 사고, 그리고 파트너 및 타사와 관련된 공격/사고의 비율은 79%입니다.
- Cisco Secure Firewall 과 Firewall Management Center 는 이전에는 전통적인 ASA 방화벽으로 보호하던 조직의 비율에 대해 위반 리스크를 80% 줄여줍니다.
- Cisco Secure Firewall 과 Firewall Management Center 는 이전에는 FTD 기반 방화벽으로 보호하던 조직의 비율에 대해 위반 리스크를 15% 줄여줍니다.
- 가상 기업의 직원 중 66%가 각 보안 위반의 영향을 받아 Cisco Secure Firewall 및 Firewall Management Center 의 침해 리스크 감소 덕분에 생산성의 70%를 회복합니다.
- 일반 직원의 총 부담 시급은 40 달러입니다.

리스크. 중대한 보안 위반의 리스크 감소는 다음 사항에 따라 다를 수 있습니다.

- 현재 겪고 있는 연간 중대 보안 위반 건수.
- 중대 위반으로 인한 내부 및 외부 총비용.
- 외부 공격, 내부 사고, 그리고 파트너 및 타사와 관련된 공격/사고의 비율.
- 기존 방화벽의 종류와 개수.
- 중대한 보안 위반의 영향을 받는 직원의 수, 그들의 총 부담 시급, 이러한 중대 위반 감소 시의 생산성 회복 능력.

결과. 이러한 리스크를 감안해 이익을 15%를 감소시킨 결과, 3 년간 리스크 조정 후 총 PV 가 350 만 달러 가까이 산출되었습니다.

중대한 위반 및 생산성 손실 리스크 감소

참조	기준	출처	1 년 차	2 년 차	3 년 차
C1	중대한 보안 위반의 평균 건수	Forrester 연구	3	3	3
C2	중대 위반당 평균 비용	Forrester 연구	$968,480	$968,480	$968,480
C3	외부 공격, 내부 사고, 그리고 파트너 및 타사와 관련된 공격/사고의 비율	인터뷰	79%	79%	79%
C4	ASA 에서 Firepower 로 이전하는 조직의 비율	가상 기업	33%	33%	33%
C5	Firepower 에서의 리스크 감소 비율	인터뷰	80%	80%	80%
C6	초기 Firepower 에서 업그레이드된 Firepower 로 이전하는 조직의 비율	가상 기업	67%	67%	67%
C7	업그레이드된 Firepower 에서의 리스크 감소 비율	인터뷰	15%	15%	15%
C8	SecureX 를 사용한 추가 감소	인터뷰	14%	18%	23%
C9	소계: 보안 위반 리스크 감소	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	$1,162,951	$1,254,763	$1,369,528
C10	각 보안 위반의 영향을 받는 사용자 수	Forrester 연구	10,600	10,600	10,600
C11	일반 직원의 평균 총 부담 시급	가상 기업	$40	$40	$40
C12	생산성 회복률	가상 기업	70%	70%	70%
C13	소계: 보안 위반 리스크 감소를 통한 생산성 향상	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8	$356,397	$384,534	$419,705
Ct	중대한 위반 및 생산성 손실 리스크 감소	C9+C13	$1,519,348	$1,639,297	$1,789,232
	리스크 조정	↓15%			
Ctr	중대한 위반 및 생산성 손실 리스크 감소(리스크 조정 후)		$1,291,446	$1,393,402	$1,520,848
	3 년 총계: $4,205,696		**3 년 현재 가치: $3,468,249**		

직원 생산성에 대한 성과 이익

근거와 데이터. 인터뷰 대상자의 조직에서는 Cisco Secure Firewall 을 사용해 1) 네트워크 성능을 향상한 애플리케이션 수준 가시성 및 제어 기능 제공, 2) 정책 업데이트에 따른 다운타임의 여파 제한이라는 두 가지 수단을 통해 직원 생산성을 광범위하게 개선할 수 있었습니다.

인터뷰 대상자들은 Cisco Secure Firewall 을 구현한 후 애플리케이션 계층에서 네트워크 액세스를 제어하는 기능 덕분에 네트워크 성능 저하 빈도가 줄었다고 말했습니다. 이전에는 고객들이 특정 애플리케이션, 특히 비디오 미디어와 관련된 애플리케이션에 대한 수요가 높을 때 네트워크가 자주 느려지고 직원 생산성에 영향을 미치는 수준까지 성능이 저하되었다는 불만을 제기했습니다. 교육 부문의 보안 운영팀장은 이런 의견을 피력했습니다. "네트워크 속도가 현저히 느려지는 일이야 매일 있었지만, 성능 저하가 너무 심해 2 주에 한 번꼴로 실제로 생산성에 영향을 미칠 정도였죠. 이런 문제는 수천 명의 사용자가 비디오를 시청할 때와 같이 활동량이 급증할 때 주로 발생했습니다."

인터뷰 대상자는 조직에서 Cisco Secure Firewall 을 사용해 애플리케이션 계층을 포함한 여러 계층에서 네트워크 보안 정책을 설정할 수 있게 되면서 네트워크 권한을 더욱 세부적으로 제어할 수 있었습니다. 결과적으로 이들 회사는 네트워크에 액세스할 수 있는 애플리케이션과 그 시점을 더 잘 제어하여 고대역폭 애플리케이션으로 인한 네트워크 과부하를 방지하고 네트워크 성능을 개선하며 직원의 생산성을 높일 수 있습니다.

"Cisco Secure Firewall 은 네트워크 사용 방식과 이러한 사용을 제어하는 능력에 대한 가시성을 훨씬 높여줍니다. 우리는 현재 4,000 개의 다양한 시스템을 모니터링하고 있어, 원하면 지난주에 인기 동영상 기반 소셜 앱의 사용량을 확인할 수 있습니다. 필요하면 이러한 유형의 트래픽을 허용하지 않도록 규칙을 수정할 수 있습니다."
교육 부문 보안 운영팀장

다른 인터뷰 대상자들은 회사에서 정책 업데이트 시의 인적 오류로 인해 때때로 발생하는 부정적인 영향을 제한함으로써 직원 생산성을 높였다고 답했습니다. 예를 들어 IT 서비스 회사의 엔지니어링 서비스 관리자의 말에 따르면, Firewall Management Center 로 정책을 훨씬 더 빠르게 만들고 업데이트할 수 있으므로 업데이트 성공 여부에 대한 피드백도 더 빨리 받았다고 합니다.

이 회사가 Secure Firewall 을 구현하기 전에는 정책 업데이트에 15 분이 걸리고 정책이 올바로 설정되었는지 확인하는 데 추가로 15 분이 더 걸렸습니다. 올바로 설정되지 않은 경우에는 정책을 두 번째로 업데이트하는 데 다시 15 분이 소요됩니다. 경우에 따라 정책을 잘못 업데이트하면 특히 프로덕션 환경에서 직원 생산성에 부정적인 영향을 미치게 됩니다.

Cisco Secure Firewall 을 사용하여 FTD 의 최신 버전으로 업그레이드한 후, 엔지니어링 서비스 관리자는 정책 업데이트와 피드백에 걸리는 시간을 3 분으로 줄이고 다시 시작하는 데 3 분으로 줄여 업데이트, 피드백, 문제 해결에 소요되는 총 시간을 60 분에서 12 분으로 80% 단축했습니다.

모델링 및 가정. 가상 기업에 대해 Forrester 는 다음과 같이 모델링합니다.

- 잘못 업데이트된 정책을 수정하는 데 온전히 1 시간이 걸립니다(잘못된 업데이트를 보내는 데 15 분, 피드백을 받는 데 15 분, 수정된 후 업데이트하고 피드백을 받는 데 30 분).
- Cisco Secure Firewall 과 Firewall Management Center 는 잘못된 정책의 수정 소요 시간을 80% 단축합니다.
- 평균적으로 조직의 2%가 잘못된 정책 업데이트의 영향을 받는 것으로 가정합니다.
- 네트워크에서는 대략 2 주에 한 번꼴로 20 분간 직원 생산성에 영향을 미친 심각한 성능 저하를 일으키곤 했습니다.
- 기존 ASA 방화벽에서 보호하던 직원의 33%가 네트워크 성능 저하의 영향을 받았습니다.

리스크. 직원 생산성에 대한 성과 이익은 다음 사항에 따라 다를 수 있습니다.

- 잘못된 정책 업데이트의 영향을 받는 직원의 비율.
- 직원 생산성에 영향을 미치는 네트워크 성능 저하의 빈도와 기간.
- 네트워크 성능 저하의 영향을 받는 직원의 수.

결과. Forrester 는 이러한 리스크를 감안하여 이익을 10% 하향 조정함으로써 3 년간 리스크 조정 후 총 PV 가 410 만 달러 이상으로 산출되었습니다.

직원 생산성에 대한 성과 이익

참조	기준	출처	1 년 차	2 년 차	3 년 차
D1	이전에 초기 FTD 로 정책을 조정할 때 걸린 시간	인터뷰	1	1	1
D2	업데이트된 FTD 로 정책을 새로 조정하는 시간	인터뷰	0.2	0.2	0.2
D3	영향을 받는 평균 직원 수	가상 기업	320	320	320
D4	일반 직원의 평균 총 부담 시급	C10	$40	$40	$40
D5	생산성 회복률	가상 기업	25%	25%	25%
D6	소계: 더 이른 정책 피드백을 통한 생산성 향상	365*(D1-D2)*D3*D4*D5	$934,400	$934,400	$934,400
D7	네트워크 남용으로 인한 성능 저하 빈도	인터뷰	26	26	26
D8	성능 저하 평균 기간(시간)	인터뷰	0.33	0.33	0.33
D9	영향을 받는 직원 수(ASA 마이그레이션만 해당)	가상 기업	5,280	5,280	5,280
D10	일반 직원의 평균 총 부담 시급	C11	$40	$40	$40
D11	생산성 회복률	가상 기업	50%	50%	50%
D12	소계: 최종 사용자 직원의 생산성 향상	D7*D8*D9*D10*D11	$906,048	$906,048	$906,048
Dt	직원 생산성에 대한 성과 이익	D6+D12	$1,840,448	$1,840,448	$1,840,448
	리스크 조정	↓10%			
Dtr	직원 생산성에 대한 성과 이익(리스크 조정 후)		$1,656,403	$1,656,403	$1,656,403
	3 년 총계: $4,969,210		**3 년 현재 가치: $4,119,230**		

이전 솔루션 비용 절감 및 방지

근거와 데이터. 인터뷰 대상자의 조직은 네트워크 보안 인프라를 Cisco Secure Firewall 의 최신 버전으로 마이그레이션함으로써 레거시 네트워크 인프라와 관련된 비용을 절감하고 방지했습니다. 놀랄 일도 아니지만, Cisco Secure Firewall 이 기존의 ASA 기반 방화벽뿐 아니라 초기 FTD 기반 방화벽도 대체함으로써 인터뷰 대상자들은 이들에 대한 라이선스를 다시 발급받는 비용을 내지 않게 되었다고 합니다.

물리적 방화벽과 가상 방화벽 교체 외에도, Cisco Secure Firewall 에는 IPS 가 포함되므로 ASA 기반 환경에서 새 환경으로 전환하는 인터뷰 대상자의 조직에서는 독립 실행형 IPS 솔루션을 폐기했습니다.

"기존 ASA 방화벽을 사용할 때는 링크와 방화벽 사이에 배치할 IPS 장치에도 투자해야 했습니다. Cisco Secure Firewall 에는 IPS 가 내장되어 있어요. 더 이상 두 가지 다른 에코시스템으로 두 가지 다른 솔루션을 관리하지 않으며, IPS 엔지니어에 의존하지도 않습니다."
기술 부문 네트워크 엔지니어링 선임 관리자

중요한 점은 인터뷰 대상자들이 조직의 방화벽을 초기 FTD 에서 Cisco Secure Firewall 로 업그레이드할 때 추가 절감 효과를 얻었다고 언급한 점입니다. 이러한 최신 방화벽의 효율성 덕분에, 인터뷰 대상자들은 전과 동일한 결과를 얻기 위해 사용하는 방화벽 수가 20%~25% 줄었다고 합니다.

"Cisco Secure Firewall 의 초기 FTD 에서 최신 FTD 로 전환하면서 처리 효율성이 나아졌어요. Cisco Secure Firewall 은 이전 버전보다 20%~25% 정도 더 효율성이 뛰어난데, 이는 곧 필요한 방화벽 수가 적다는 뜻입니다."
인터넷 부문 선임 네트워크 엔지니어

모델링 및 가정. 가상 기업에 대해 Forrester 는 다음과 같이 모델링합니다.

- 기존 ASA 방화벽을 Cisco Secure Firewall 로 바꿈으로써 독립 실행형 IPS 라이선싱 비용이 연간 171,600 달러 감소합니다.
- 라이선스 요금의 20%에 해당하는 독립 실행형 IPS 유지 관리 비용을 쓸 필요가 없습니다.
- 매주 FTE 2 명에 대해 지속적으로 발생하는 30 분의 80%에 해당하는 IPS 관련 관리 비용이 절감됩니다.
- 1 년 차에 기존 방화벽을 유사한 유형의 방화벽으로 바꾸는 데 드는 130 만 달러 이상의 비용이 발생하지 않았습니다.
- 연간 300,000 달러의 가상 방화벽 교체 비용을 방지했습니다.
- Cisco Secure Firewall 의 효율성 덕분에 물리적 방화벽의 25%에 해당하는 비용을 추가로 절감했습니다.

리스크. 레거시 솔루션 비용 절감은 다음 사항에 따라 달라집니다.

- 기존 방화벽의 개수와 종류.
- 독립 실행형 IPS 솔루션 폐기 기능.

"우리는 마침내 Cisco Secure Firewall 을 배포할 때 더 비싸고 성능이 떨어지는 IPS 어플라이언스를 사용 중지했습니다."
금융 서비스 부문 책임 인프라 엔지니어

결과. 이러한 리스크를 감안하여 이익을 10% 줄인 결과, 3 년간 리스크 조정 후 총 PV 가 260 만 달러로 산출되었습니다.

레거시 솔루션 폐기로 절감한 비용

참조	기준	출처	1 년 차	2 년 차	3 년 차
E1	레거시 IPS 비용 절감	인터뷰	$171,600	$171,600	$171,600
E2	유지 관리 비용 절감	E1*20%	$34,320	$34,320	$34,320
E3	레거시 IPS 의 지속적인 관리 비용 절감	인터뷰	$53,539	$53,539	$53,539
E4	교체 주기의 방화벽 비용 방지	가상 기업	$1,616,980	$300,000	$300,000
E5	추가 방화벽 효율성으로 인한 비용 방지	가상 기업	$329,245	$0	$0
Et	레거시 솔루션 폐기로 절감한 비용	E1+E2+E3+E4+E5	$2,205,684	$559,459	$559,459
	리스크 조정	↓10%			
Etr	레거시 솔루션 폐기로 절감한 비용(리스크 조정 후)		$1,985,115	$503,513	$503,513
	3 년 총계: $2,992,142		**3 년 현재 가치: $2,599,074**		

정량화할 수 없는 이익

고객들이 경험했지만 정량화할 수 없는 추가 이익:

- **VPN 생산성 및 보안 향상.** 인터뷰 대상자들은 또한 Cisco Secure Firewall 을 사용해 원격 액세스 VPN 생산성과 보안을 향상했다는 점도 언급했습니다. Secure Firewall 은 로드 밸런싱을 통해 그룹화된 장치 간에 세션을 분산하여 성능, 복원력, 최종 사용자 생산성을 제공했습니다. 마찬가지로, 사용자는 Secure Firewall 을 사용한 로컬 인증을 통해 원격 AAA 서버에 액세스할 수 없게 된 경우에도 생산성을 유지할 수 있었습니다. Cisco Secure Firewall 은 보안을 위해 다중 인증서를 통한 인증을 지원하므로, 조직에서는 최종 사용자 자체를 검증하는 것 외에도 원격 장치가 회사에서 발급한 것인지 확인할 수 있습니다.

- **규정 준수 개선.** 또한 인터뷰 대상자는 Cisco Secure Firewall 과 Firewall Management Center 가 규정 준수 워크플로에 정량화할 수 없는 이익을 제공했다고 밝혔습니다. 금융 서비스 회사의 책임 인프라 엔지니어는 Secure Firewall 과 FMC 를 배포하기 전에는 규정 준수에 대해 보고하기 더 어려웠다고 밝혔습니다. 이전 솔루션에는 손쉬운 보고 기능이 없었습니다. 하지만 조직에서는 Secure Firewall 과 FMC 를 사용해 구성 요소를 더욱 폭넓게 포괄하고 활동과 보기에 관해 더욱 자세한 보고서를 실행할 수 있었습니다. 인터뷰 대상자들은 또한 Cisco Secure Firewall 이 TLS(전송 계층 보안) 1.3 암호화 표준을 지원한다고 말했습니다. 예를 들어, 인터넷 회사의 선임 네트워크 엔지니어는 자신이 팀에서 현재 관리 부담으로 인해 그와 같은 흐름을 해독하고 있지 않다고 밝혔습니다. Cisco Secure Firewall 에 투자한 후, TLS 1.3 암호 해독이 더 쉽고 효율적이 되었습니다.

"이전에는 다양한 다수의 구성 요소에 대한 보고 출력이 없었지만, 이제는 더 광범위하고 자세한 보고서를 더 쉽게 얻을 수 있습니다. 예를 들어, 작년에 제가 수행한 모든 액세스 제어 변경 사항에 대한 보고서를 받았습니다. 이 보고서는 모든 페이지 보기와 수행된 변경 사항의 출력을 보여줍니다."
금융 서비스 부문 책임 인프라 엔지니어

- 직원 **경험 향상.** 인터뷰 대상자들은 또한 조직의 직원 경험이 향상되었다고 말했습니다. 예를 들어, 인터넷 회사의 선임 네트워크 엔지니어는 이렇게 말했습니다. "네트워크에서 애플리케이션 액세스를 더 잘 제어할 수 있게 되어 직원 만족도가 향상되었습니다. 현지 IT 팀은 특정 앱 사용을 중단하거나 앱 액세스를 차단하도록 요구하기 위해 사용자를 추적하는 데 어려움을 겪곤 했습니다. Secure Firewall 과 FMC 를 사용하면 이제 원격으로 그 작업을 수행할 수 있습니다."

유연성

유연성의 가치는 고객마다 다릅니다. 고객이 Secure Firewall 을 구현한 후 추가적으로 이용하고 비즈니스 기회를 실현할 수 있는 시나리오는 다음과 같습니다.

- **추가 Cisco Security 통합.** SecureX 의 이점 외에도, 인터뷰 대상자들은 Cisco 의 보안 제품 에코시스템이 조직의 보안 상태를 더욱 강화하기 위한 유연성을 제공한다고 했습니다. 예를 들어, IT 서비스 회사의 엔지니어링 서비스 관리자는 이렇게 밝혔습니다. "Cisco Security 는 다른 벤더가 어려움을 겪고 있는 통합 보안 솔루션의 심층적인 스택을 갖추고 있습니다. 단순히 Secure Firewall 뿐 만이 아니라 다른 모든 부분이 함께 잘 통합되어 더 나은 방어 체계를 구축할 수 있습니다."
- **재택 근무를 위한 업무 운영 개선.** Cisco Secure Firewall 제어는 직원이 재택 근무로 전환할 때 VPN 사용이 급증했을 때 업무 운영을 원활히 유지하는 데도 도움이 되었습니다. 인터넷 회사의 선임 네트워크 엔지니어는 이렇게 말했습니다. "팬데믹 와중에 동시 VPN 연결이 전 세계적으로 평균 100,000 개에서 350,000 개에 가까이 증가했습니다. 우리는 네트워크의 실행 가능성을 유지하기 위해 Cisco Secure Firewall 을 사용해 속도 제한을 설정하고 운영을 원활하게 했습니다."
- **클라우드로의 용이한 전환.** 마지막으로, 인터뷰 대상자들은 Cisco Secure Firewall 을 통해 클라우드 이니셔티브를 더 쉽게 달성할 수 있다고 밝혔습니다. IT 서비스 조직의 엔지니어링 서비스 관리자는 이렇게 말했습니다. "현장, 원격 사이트 그리고 클라우드까지 닿기 위해 단일 플랫폼이 필요했지만, 배포하기 쉬워야 했습니다. 클라우드 플랫폼을 사용하면 그냥 FTD 박스를 놓고 바로 그 자리에 설치한 다음 Firewall Management Center 에 연결할 수 있습니다. 설정하고 배포하는 데 전혀 시간이 걸리지 않았습니다. 그리고 표준화된 정책을 그와 같은 박스로 푸시할 수 있습니다."

유연성은 특정 프로젝트의 일부로 평가해 정량화될 수도 있습니다(자세한 내용은 부록 A 참조).

비용 분석

가상 기업에 적용된 정량화된 비용 데이터

총비용

참조	비용	초기	1 년 차	2 년 차	3 년 차	합계	현재 가치
Ftr	라이선스 비용	$6,000,690	$0	$0	$0	$6,000,690	$6,000,690
Gtr	구현, 정책 생성 및 교육 비용	$278,220	$7,924	$7,924	$7,924	$301,990	$297,924
	총비용(리스크 조정 후)	$6,278,910	$7,924	$7,924	$7,924	$6,302,680	$6,298,614

라이선스 비용

근거와 데이터. 고객은 다음을 포함하여 Secure Firewall 투자와 관련해 발생하는 여러 가지 다양한 비용을 공유해 주었습니다.

- 필요한 처리량에 따라 다른 물리적 방화벽 비용.
- East-West 트래픽을 처리하기 위해 데이터 센터에 배포된 가상 방화벽.
- 위협 방지, 맬웨어 방어 및 URL 필터링 라이선스 비용.
- Firewall Management Center 라이선스.

"우리는 심층적인 아키텍처, 도구 집합, 기능을 갖춘 옵션을 찾으려 애썼습니다. Cisco Secure Firewall 은 이 모든 것을 하나의 박스에 포함하고 있었죠. 하지만 그에 더해 가성비도 매력적이었습니다."
금융 서비스 부문 책임 인프라 엔지니어

고객들은 Secure Firewall 라이선스에 Cisco SecureX 가 포함되어 있으므로 추가 비용 없이 Cisco SecureX 를 배포할 수 있다는 점을 언급했습니다.

모델링 및 가정. 100 개의 사무실과 이중화가 필요한 4 개의 물리적 데이터 센터가 있는 가상 기업의 경우 Forrester 는 다음과 같이 모델링합니다.

- 3 년 동안 모든 라이선스를 정가로 제공합니다.
- 회사 사무실용 방화벽 비용은 328,443 달러입니다. 회사 사무실에는 최대 75Gbps 의 처리량 성능을 가진 대규모 엔터프라이즈급 방화벽이 필요합니다.
- 데이터 센터 방화벽 비용은 978,067 달러입니다. 각 데이터 센터에서 가상 기업은 데이터 센터 안팎으로 오가는 남-북 트래픽을 처리하기 위해 두 개의 물리적 방화벽으로 구성된 데이터 센터 경계 클러스터링 또는 고가용성 번들을 배포합니다.
- 100 개의 가상 방화벽 비용은 2,628,561 달러입니다. 이러한 가상 방화벽은 데이터 센터 내에서, 그리고 데이터 센터와 공용 클라우드 플랫폼 사이에서도 East-West 트래픽을 처리합니다.
- 데이터 센터의 물리적 방화벽과 가상 방화벽에는 모두 3 년 구독 요금으로 추가 Threat Protection 라이선스가 있습니다. 이는 침해 트래픽 및 악성

트래픽의 지표를 더 잘 탐지하고 완화하기 위해 Snort 3 를 포함한 추가 보안을 제공합니다.

- 60 개 지사 방화벽의 총비용은 1,848,160 달러입니다. 60 개 사무실에는 최대 1.9Gbps 의 처리량을 제공하는 Secure Firewall 이 필요합니다.
- 39 개 소규모 지사 방화벽의 총비용은 137,779 달러입니다. 나머지 39 개 사무실에는 최대 650Mbps 의 처리량만 필요했습니다.
- 모든 사무실 방화벽에는 3 년 구독 요금으로 추가적인 Threat Protection, Malware Defense 및 URL 필터링 라이선스가 있습니다.
- 또한 Firewall Management Center 는 이러한 모든 방화벽을 다룰 수 있도록 적절한 규모에 맞춰 라이선스가 부여됩니다. Firewall Management Center 의 비용은 79,680 달러입니다.

리스크. Cisco Secure Firewall 와 Firewall Management Center 의 라이선스 비용은 다음에 따라 다릅니다.

- 원하는 가상 방화벽의 수.
- 필요한 엔터프라이즈급 방화벽의 수.
- 데이터 센터의 규모와 수, 고가용성에 대한 필요성.
- 지사 사무실의 규모와 수.

결과. Forrester 는 Cisco 와 함께 가상 기업의 가격을 직접 책정했으므로 이 리스크 비용을 조정하지 않아, 3 년 총 PV(10% 할인)는 6 백만 달러입니다.

"Cisco 기업 보안 계약을 통해 총비용이 모든 것을 개별 주문하는 것 보다 더 저렴해집니다. Firepower 가 그 비용의 큰 부분을 차지하지만, 이전에는 없었던 제품으로 추가 보호 기능을 사용하여 수십만 달러를 절약하고 있습니다."
교육 부문 보안 운영팀장

라이선스 비용

참조	기준	출처	초기	1 년 차	2 년 차	3 년 차
F1	가상 방화벽 비용	Cisco	$2,628,561			
F2	회사 사무실 방화벽 비용	Cisco	$328,443			
F3	데이터 센터에 설치되는 물리적 방화벽 비용	Cisco	$978,067			
F4	소규모 지사 사무실 방화벽 비용	Cisco	$137,779			
F5	대규모 지사 사무실 방화벽 비용	Cisco	$1,848,160			
F6	Firewall Management Center 비용	Cisco	$79,680			
Ft	라이선스 비용	F1+F2+F3+F4+F5+F6	$6,000,690	$0	$0	$0
	리스크 조정	0%				
Ftr	라이선스 비용(리스크 조정 후)		$6,000,690	$0	$0	$0
	3 년 총계: $6,000,690			**3 년 현재 가치: $6,000,690**		

구현, 정책 생성 및 교육 비용

근거와 데이터. 인터뷰 대상자들은 데이터 센터와 사무실 전체에서 방화벽 배포 및 구현과 관련된 내부 소요 시간과 인건비가 발생했다고 밝혔습니다. 이러한 비용 중 첫 번째 비용은 각 사이트에 방화벽을 물리적으로 배포하는 비용이었습니다. 두 번째는 각 방화벽 세트에 적절한 정책을 만들고 배포하여 이러한 방화벽을 구현하는 비용이었습니다.

"구현과 배포는 정말 빠르고 비교적 간단했습니다. 이미 설계가 완료되었고 모든 것을 켜는 방법을 알고 있었기에, 실제 전환까지는 3 주가 걸렸습니다."
교육 부문 보안 운영팀장

마지막으로, 인터뷰 대상 의사 결정권자들은 교육과 관련된 시간 비용도 발생한다고 언급했습니다. Cisco Secure Firewall 을 배포하고 관리하기 위해 이러한 교육이 필요한 직원의 경우 교육에 약 2 시간이 걸렸습니다. 일부 인터뷰 대상자는 Cisco 보안 전문가가 출연하는 공개 교육 동영상을 활용한다고 말했습니다.

모델링 및 가정. 가상 기업에 대해 Forrester 는 다음과 같이 모델링합니다.

- 데이터 센터 두 곳과 사무실 100 개에 각각 평균 6 시간의 구현 시간이 필요합니다.
- 평균적으로 정책 생성에는 방화벽당 30 시간이 걸립니다.
- SecureX 를 구현하려면 20 시간, 지속적 관리를 위해 연간 100 시간의 작업이 추가로 필요합니다.
- 처음에는 15 명의 직원이 교육을 받아야 하는데, 직원 이직으로 인해 매년 3 명의 직원이 추가로 교육을 받아야 합니다.

리스크. 구현 및 정책 생성에 대한 비용은 다음 요인에 따라 달라집니다.

- 배포할 Cisco Secure Firewall 의 수.
- 초기에 교육을 받아야 하는 직원 수.
- 직원 이직률.
- NetSecOps 전문가의 총 부담 시급.

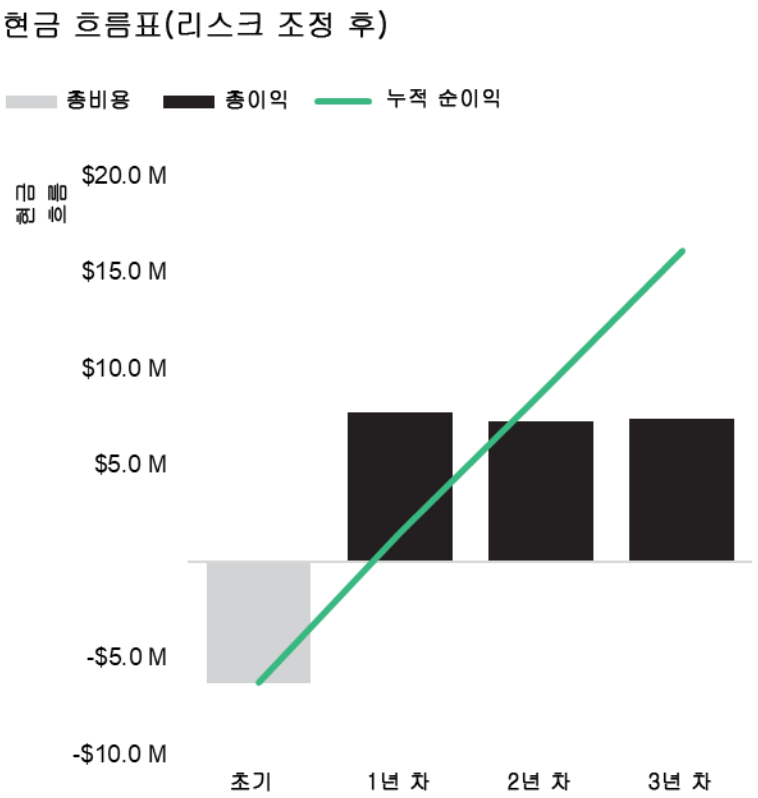
결과. 이러한 리스크를 감안해 Forrester 는 이 비용을 15% 증액하여 3 년 리스크 조정 후 총 298,000 달러 미만의 PV 를 산출했습니다.

구현, 정책 생성 및 교육 비용

참조	기준	출처	초기	1 년 차	2 년 차	3 년 차
G1	배포할 사이트 수	가상 기업	102			
G2	각 사이트의 물리적 구현 평균 시간	가상 기업	6			
G3	정책 생성 시간	인터뷰	30			
G4	SecureX 구현 및 관리 시간	인터뷰	20	100	100	100
G5	교육이 필요한 직원 수	인터뷰	15	3	3	3
G6	교육에 필요한 시간	인터뷰	2	2	2	2
G7	NetSecOps 전문가의 평균 총 부담 시급	A5	$65	$65	$65	$65
Gt	구현, 정책 생성 및 교육 비용	((G1*(G2+G3))+,G4+(G5*G6))*G7	$241,930	$6,890	$6,890	$6,890
	리스크 조정	↑15%				
Gtr	구현, 정책 생성 및 교육 비용(리스크 조정 후)		$278,220	$7,924	$7,924	$7,924
	3 년 총계: $301,990		**3 년 현재 가치: $297,924**			

재무 개요

3 년 리스크 조정 후 통합 지표



이익 및 비용 섹션에 계산된 재무 결과는 가상 기업의 투자에 대한 ROI, NPV 및 원금 회수 기간을 결정하는 데 사용할 수 있습니다. Forrester 가 이 분석에서 추정한 연간 할인율은 10%입니다.

이와 같은 리스크 조정 후 ROI, NPV 및 원금 회수 기간 값은 각 이익 및 비용 섹션의 조정 전 결과에 리스크 조정 요소를 적용하여 결정됩니다.

현금 흐름 분석(리스크 조정 후 추정치)

	초기	1 년 차	2 년 차	3 년 차	합계	현재 가치
총비용	($6,278,910)	($7,924)	($7,924)	($7,924)	($6,302,680)	($6,298,614)
총이익	$0	$7,737,795	$7,264,360	$7,391,805	$22,393,959	$18,591,534
순이익	($6,278,910)	$7,729,871	$7,256,436	$7,383,881	$16,091,279	$12,292,920
투자자본수익률(ROI)						195%
회수 기간(개월)						10

부록 A: Total Economic Impact

Total Economic Impact(총 경제적 영향)는 Forrester Research 에서 개발한 방법론으로, 기업이 기술 의사 결정 과정을 향상하고 자사의 제품 및 서비스가 제공하는 가치를 고객에게 효과적으로 전달할 수 있도록 지원합니다. TEI 방법론은 기업이 고위 경영진과 중요한 비즈니스 이해관계자들에게 IT 프로젝트의 가시적 가치를 입증하고 타당함을 제시하여 실현할 수 있도록 도움을 줍니다.

TOTAL ECONOMIC IMPACT 접근 방식

이익은 제품이 비즈니스에 제공하는 가치를 의미합니다. TEI(총 경제적 영향) 방법론은 이익과 비용을 측정하는 데 동일한 가중치를 적용해 기술이 기업 전반에 어떤 영향을 미치는지 전체적으로 파악할 수 있도록 해줍니다.

비용은 제품의 제안된 가치 또는 이익을 창출하는 데 소요되는 모든 비용으로 간주됩니다. TEI(총 경제적 영향)의 비용 범주에는 솔루션과 관련하여 지속적으로 발생하는 비용에 대한 기존 환경에 투입되는 증분 비용이 포함됩니다.

유연성은 초기 투자가 이미 이행된 상태에서 향후 추가 투자가 이루어질 경우 획득할 수 있는 전략적 가치를 의미합니다. 그 이익을 가질 수 있다는 것은 추정 가능한 PV 가 있다는 의미입니다.

리스크는 이익 및 비용 추정의 불확실성에 관한 지표입니다. 이때 1) 추정치가 원래의 예상치에 부합할 가능성, 그리고 2) 시간의 경과에 따라 추정치를 모니터링할 가능성을 고려합니다. TEI(총 경제적 영향) 리스크 요소는 “삼각 분포”에 기반합니다.

초기 투자 열에는 "0 시점", 즉 1 년 차 시작 시점에 발생한 할인되지 않은 비용이 포함됩니다. 그 밖의 현금 유동성에는 연말에 할인율을 적용합니다. PV 는 총비용 및 총이익 추정치 각각에 대해 계산합니다. 요약 표의 NPV 계산은 초기 투자 및 각 연도의 할인된 현금 유동성을 합한 것입니다. 총이익, 총비용 및 현금 흐름표의 합계 및 현재 가치 표들은 반올림이 적용된 경우가 있으므로 합계가 정확하게 100%가 되지 않을 수 있습니다.

현재 가치(PV)

이자율(할인율)을 감안한 (할인된) 예상 비용 및 이익의 현재 가치입니다. 비용 및 이익의 PV 는 현금 흐름의 총 NPV 에 반영됩니다.

순 현재 가치(NPV)

이자율(할인율)을 감안한 (할인된) 향후 순 현금흐름의 현재 가치입니다. 일반적으로 프로젝트 NPV 가 양수이면 다른 프로젝트의 NPV 가 더 높지 않은 한 해당 프로젝트에 대한 투자를 진행해야 한다는 의미입니다.

투자 수익률(ROI)

백분율로 표시되는 프로젝트의 기대 수익률입니다. ROI 는 순이익(이익 - 비용)을 비용으로 나누어 계산합니다.

할인율

현금 흐름 분석에서 금액의 시간적 가치를 고려하기 위해 사용하는 이자율입니다. 일반적으로 기업들은 8%~16%의 할인율을 사용합니다.

원금 회수 기간

투자에 대한 손익 분기점입니다. 순이익(비용을 차감한 이익)이 초기 투자 또는 비용과 동일해지는 시점입니다.

부록 B: 주석

[1] Total Economic Impact(TEI)는 Forrester Research 에서 개발한 방법론으로, 기업이 기술 의사 결정 과정을 향상하고 자사의 제품 및 서비스가 제공하는 가치를 고객에게 효과적으로 전달할 수 있도록 지원합니다. TEI 방법론은 기업의 경영진 및 중요한 비즈니스 이해관계자들에게 IT 프로젝트의 가시적 가치를 입증하고 타당함을 제시하여 실현할 수 있도록 도움을 줍니다.


FORRESTER®