SANGFOR

SANGFOR NETWORK SECURE

NEXT GENERATION FIREWALL

Smarter AI-Powered Perimeter Defense

The World's First Fully Integrated NGFW + NGWAF + SoC Lite

- 모든 보안 운영을 위한 단일 관리 패널
- 시각화를 통한 보안 전문성 강화
- 적은 비용으로 더 많은 작업을 수행하세요. 효율적으로 최소 50%의 TCO 절감
- 새로운 사이버 위협을 차단하세요
- Sangfor XDDR Synergy로 랜섬웨어 예방 및 제거

Gartner

Visionary in 2022 Gartner® Magic Quadrant™ for Network Firewalls

FROST & SULLIVAN BEST PRACTICES AWARDS

2023 Asia-Pacific (APAC) Next-generation Firewall (NGFW) Company of the Year Award

CRO CYBER RATINGS.ORG

Recommended Ratings in CyberRatings.org's Enterprise Firewall Test

New World. New IT. New Security.

IT 분야는 계속해서 변화하고 있습니다. 인터넷 덕분에 클라우드 컴퓨팅, BYOD, IoT와 같은 IT 트렌드가 이전의 방식보다 훨씬 유연해졌습니다. 이제는 어디에서나, 언제든지 다양한 기기로 비즈니스 중요 애플리케이션과 서비스에 접근할 수 있습니다. 이런 유연한 트렌드가 계속 유지되는 이유는 그것이 가장 적합하기 때문입니다. 하지만 네트워크 보안도 이와 같은 속도로 발전하고 있을까요?

진화 과정에서 윤리가 중요한 역할을 하였으며, IT 분야에서도 마찬가지입니다. 정보는 새로운 중요한 자산이 되었고, 재정 정보나 중요한 기업 정보 같은 민감한 데이터는 자연스럽게 위협의 대상이 되고 있습니다. 기업 방화벽의 90% 이상이 곧 NGFW로 바뀔 것으로 보입니다. 이는 기존 방화벽을 대체하는 것이지만, 많은 조직들이 보다 발전된 보안 방법인 웹 애플리케이션 방화벽(WAF)으로 넘어가는 것을 등한시하고 있습니다. WAF와 같은 보안 수단은 추가 비용이 들고 경제적 이득이 적다고 여겨지지만, NGFW만으로는 끊임없이 발전하는 사이버 위협에 대응하기에는 부족합니다. 2017년에는 WannaCry라는 새로운 랜섬웨어가 전 세계 99개국을 감염시켜 정부, 학교, 병원 등을 공격했습니다. 이 사건이 랜섬웨어를 사람들에게 널리 알렸습니다.

랜섬웨어는 사이버 범죄자들이 파일(또는 컴퓨터)을 인질로 잡고 돈을 지불하라고 요구하면서 파일을 암호화하는 악성 소프트웨어입니다. 랜섬웨어가 처음 발견된 이후로 빠르게 확산되어 많은 사용자들, 회사와 개인 모두가 감염되고 있습니다. 랜섬웨어는 많은 회사의 생산성과 명성에 심각한 영향을 미치며, 결국 돈을 지불해야 하는 경우가 많습니다. XBash와 같이 데이터 시스템 파괴와 암호화폐 채굴에 집중된 더 많은 변종들이 퍼지고 있습니다. 애플리케이션 보안은 이제 선택사항이 아닙니다. 공격이 늘어나고 규제 압력이 커짐에 따라, 조직은 애플리케이션과 API를 보호하기 위한 효과적인 프로세스와 능력을 확립해야 합니다 (출처: OWASP, 2017). 위험 인식과 비용 문제로 진정한 조직 보안의 진화가 지연되는 동안, 많은 기업들은 실제 필요에 대한 고려 없이 단순히 제공되는 것을 받아들이고 있습니다.

Sangfor Network Secure

Sangfor Network Secure(이전에 Sangfor NGAF로 알려짐)는 고급 지속 위협(APT), 맬웨어, 랜섬웨어, IoT 위협, 웹 기반 공격에 대한 보호를 제공하는 통합 보안 솔루션입니다. 이 솔루션은 방화벽, 애플리케이션 제어, URL 필터링, 침입 방지 시스템(IPS), 안티맬웨어, 클라우드 샌드박스, WAF 등의 보안 기능을 통합합니다. Sangfor Network Secure는 Sangfor Engine Zero(AI 기반 맬웨어 검사 엔진)와 Neural-X(위협 인텔리전스 및 분석 플랫폼)의 힘을 활용하여 아직 어떤 보안 데이터베이스에도 추가되지 않은 신종 위협을 감지하고 격리합니다. 이로 인해 제로데이 공격에 특히 효과적입니다.

Smart World, Safe World with Sangfor Innovations

Neural-X는 Sangfor가 개발한 복잡한 네트워크 보안 요소의 중심에 있습니다. 클라우드 기반의 인텔리전스 및 분석 플랫폼으로, 인공지능(AI)에 의해 구동되는 Neural-X는 Sangfor의 네트워크, 엔드포인트, 그리고 보안-서비스 제공(Security-as-a-Service)의 보안 탐지 능력을 강화하고 확장합니다. Neural-X는 Engine Zero, 위협 인텔리전스, 딥러닝, 샌드박싱, 그리고 봇넷 감지를 포함하여 서로 연결된 수십 개의 구성요소를 포함하고 있으며, 이러한 구성요소들은 시스템을 안전하고 보안 유지하기 위해 매끄럽게 함께 작동하도록 설계되었습니다.

Sangfor Engine Zero

Sangfor Engine Zero는 강력한 인공지능 기술을 기반으로 한 맬웨어 탐지 엔진으로, 데이터 과학자, 보안 분석가, 그리고 화이트 해트 연구원들의 팀에 의해 지속적으로 강화되고 있습니다. 이 엔진은 Sangfor의 보안 제품과 Neural-X 클라우드 위협 인텔리전스 플랫폼에 내장된 여러 맬웨어 검사 엔진 중 하나입니다. 매우 효율적이며 최소한의 자원을 사용합니다. 이러한 효율성만이 네트워크 게이트웨이에서 알려진 공격과 제로데이 공격 모두에 대한 맬웨어 검사를 성능 저하 없이 제공할 수 있습니다. 최근 AV-Test가 실시한 랜섬웨어 테스트에서 Engine Zero로 구동되는 Sangfor Endpoint Secure는 모든 테스트에서 100%의 완벽한 성공률을 달성하여, 실제 세계의 고급 위협을 탐지할 수 있는 엔진의 능력을 입증했습니다.

Sangfor Neural-X

Neural-X는 Sangfor의 지능형 위협 탐지 및 방어의 핵심에 위치합니다. 위협 인텔리전스는 조직이 외부 출처로부터 알려진 및 신흥 위험을 이해하고 평가하며 방어할 수 있도록 조직화되고 분석된, 그리고 정제된 정보로 구성됩니다.

Deep Learning

딥러닝은 인간 뇌의 뉴런이 서로 연결되는 기능에서 영감을 받은 기계학습의 복잡한 요소입니다. 인공지능의 일부이며 기계학습의 발전으로 간주될 수 있습니다. 이름에서 알 수 있듯이, 딥러닝은 수백만 개의 데이터를 관찰하고 처리함으로써 스스로 학습할 수 있으며, 이를 통해 더 정확하고 빠른 예측을 할 수 있습니다. Neural-X가 딥러닝을 사용하는 방법 중 하나는 암호화된 도메인 이름을 기계가 읽을 수 있는 벡터로 분해하는 것입니다. 벡터 연관성의 심층 분석은 유사한 패밀리의 맬웨어에 의해 사용되는 도메인 이름을 감지합니다. 시간이 지남에 따라 딥러닝 기능은 독립적으로 작동하고 학습하기 시작하며 맬웨어에 대한 선제적 접근을 유지합니다.

Sangfor ZSand

Sangfor ZSand는 알려지지 않은 맬웨어를 감지하기 위해 설계된 가상 동적 실행 기술(샌드박싱)입니다. Sangfor ZSand는 의심되는 맬웨어를 안전하고 통제된 환경에서 실행시키고 이 파일들의 비정상적인 행동을 모니터링하여 미래의 인식 및 예방을 위해 기록합니다. 최근 테스트에서는 GandCrab, Zusy, GlobeImposter, LockCrypt 등의 랜섬웨어 패밀리를 정확하게 감지했습니다. ZSand는 모든 데이터를 Neural-X 위협 인텔리전스와 공유하여, 알려진 이전 서명이 없는 맬웨어를 식별하고 연구할 수 있게 하며, 이를 통해 미래의 제로데이 공격 위험을 줄이고 Neural-X 내에서의 탐지, 식별, 제거가 가능합니다.

Botnet Detection

해커들은 고정된 IP 주소를 버리고 동적 도메인 이름을 사용함으로써 더욱 정교해지고 있습니다. 이러한 암호화된 도메인 이름들은 비밀 알고리즘을 사용하여 컨트롤러와 연결된 감염된 컴퓨터의 네트워크인 봇넷을 구성합니다. DNS 쿼리가 일반 인터넷 사용자의 행동을 모방하기 때문에 봇넷을 탐지하기는 매우 어렵습니다. Neural-X는 고급 흐름 분석, 시각 계산, 그리고 딥러닝 기술을 사용하여 봇넷을 탐지합니다. 이는 VirusTotal과 같은 인기 있는 소스들에 비해 훨씬 많은 악성 도메인 이름을 발견할 수 있습니다. 지금까지 백만 개 이상의 악성 도메인 이름을 식별했으며 이 목록은 매일 성장하고 있습니다.

Next Generation Web Application Firewall

Sangfor Network Secure는 SQL 인젝션, 웹 쉘, 크로스사이트 스크립팅(XSS), 역직렬화 결함을 포함한 네트워크 및 웹 기반 공격에 대응하기 위해 전용 차세대 웹 애플리케이션 방화벽(NGWAF)과 통합된 세계 최초의 차세대 방화벽(NGFW)입니다. Sangfor의 Web Intelligent & Semantic Engine (WISE)은 기계 학습 및 의미 분석을 사용하여 공격 행동을 면밀히 조사함으로써 탐지율을 높이고 기존 SNORT 기반 탐지 엔진과 비교할 때 오진율을 줄입니다. 공격 행동의 위협 모델이 설정되어 애플리케이션 관련 보안 위협의 효율적인 관리를 용이하게 합니다.

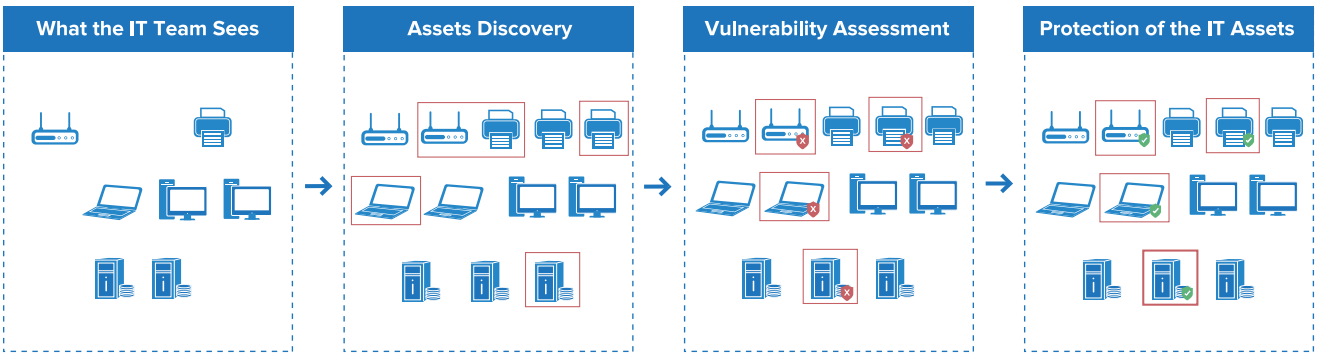
Sangfor's Concept of Security

네트워크 보안은 업계 및 지역에 따라 동등하게 발전하지 않았습니다. 다양한 산업과 지역의 보안 전문가들은 네트워크 보안에 대해 서로 다른 의견, 기대, 그리고 필요를 가지고 있습니다. 일부는 파일 및 데이터에 대한 무단 접근 방지로 정의하는 반면, 다른 이들은 맬웨어 감염 예방을 강조합니다. 그러나 이러한 전통적인 네트워크 보안 기능을 기반으로 하는 보안 솔루션은 사용자, 트래픽 및 IT 자산에 대한 가시성이 제한적이며, 실시간 또는 침해 후 탐지 기능이 부족합니다. 사이버 공격의 양과 복잡성이 증가함에 따라, 네트워크 보안은 신흥 위협을 따라잡기 위해 발전해야 합니다. Sangfor는 네트워크 보안의 혁신적이고 더 포괄적인 개념을 지지합니다. 우리는 그 이상을 제공하며, 공격 전이든 공격 후이든, 외부에서 발생하든 내부에서 발생하든, 현재든 미래든 모든 위협을 커버하는 종합적인 보안 솔루션을 제공합니다.

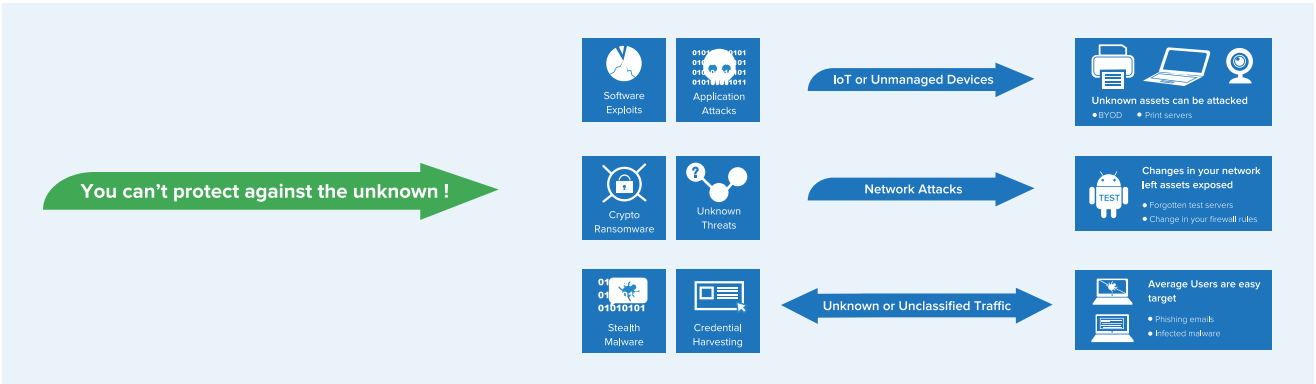
Sangfor의 혁신적인 네트워크 보안 접근 방식은 네 가지 기본 원칙에 기반을 두고 있습니다

1. Protect Business Assets

"Sangfor Network Secure는 비즈니스 자산을 발견하고 보호하는 데 뛰어나며, 설정된 비즈니스의 위험을 최소화하기 위해 자동으로 관리되지 않는 IT 자산을 발견하고 시스템 취약점, 약한 비밀번호, 무단 애플리케이션과 같은 위험을 식별합니다. 또한, Sangfor Network Secure는 가상 패치와 같은 치료적 기능을 통해 자산의 능동적 보호를 제공합니다."



2. Comprehensive Threat Protection



"Sangfor Network Secure는 방화벽, 침입 방지 시스템(IPS), 안티바이러스(AV), 안티맬웨어, 고급 지속 위협(APT) 보호, IoT 보안, URL 필터링, 클라우드 샌드박스, 웹 애플리케이션 방화벽을 포함한 다양한 보안 기능을 통합한 융합 보안 솔루션입니다. 이러한 기능들은 랜섬웨어, APT 공격, 웹 익스플로잇과 같은 광범위한 보안 위협에 대한 포괄적인 보호를 보장합니다.

새로운 맬웨어와 제로데이 공격에 대한 보호는 지금까지 어떤 서명 데이터베이스에도 포함되지 않았기 때문에 가장 중요합니다. 더욱이, 이러한 고급 위협은 대개 고도로 전문화되고 자원이 풍부한 위협 행위자들의 소유이며, 상당한 피해를 입힐 수 있는 능력을 가지고 있습니다.

Sangfor는 Engine Zero, NGWAF, 봇넷 감지 등 보안 혁신에 인공지능을 적용하여 이러한 위협에 효과적으로 대응합니다. 예를 들어, Engine Zero는 수백만 개의 맬웨어 샘플을 사용하여 진화하는 맬웨어의 특성을 학습하기 위해 지속적으로 훈련받고 있으며, 이를 통해 높은 정확도로 새로운 맬웨어와 제로데이 공격을 인식할 수 있습니다.

모든 Sangfor 탐지 엔진은 Sangfor의 클라우드 기반 Neural-X 플랫폼에서 제공하는 위협 인텔리전스 서비스를 공유하며, 기계 학습을 통해 알려지지 않은 서명 없이 새로운 위협을 정확하게 감지할 수 있어 조직의 예방적 방어를 강화합니다."

Real-Time Threat Intelligence Monitor

Intelligence Sources

• 20,000개가 넘는 연결된 네트워크 게이트웨이에서는 악성 URL, IP, 도메인 이름, 맬웨어 해시를 포함하는 IOC를 제공하며, 참여하는 게이트웨이의 수는 매년 두 배씩 증가하고 있습니다.

• 제3자 위협 인텔리전스 피드.

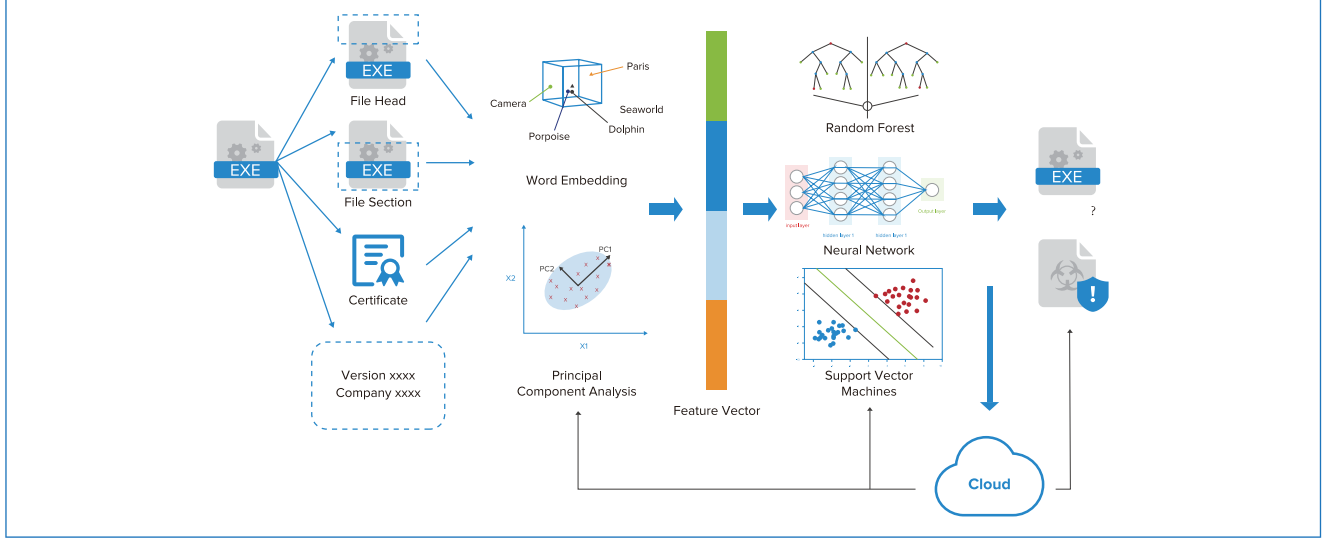
• Sangfor 보안 연구개발(R&D) 팀은 화이트 해트 및 블랙 해트 커뮤니티를 적극적으로 모니터링합니다.

Real Case Scenario

Sangfor Network Secure가 인터넷에 연결된 서버에서 비정상적인 아웃바운드 연결을 감지하면, 해당 의심스러운 DNS 주소를 Neural-X에 검증을 위해 보냅니다. 위협 인텔리전스가 이 특정 DNS를 알려진 명령 및 제어(C2) 서버로 분류했다면, 해당 서버는 침해되었을 가능성이 큽니다. Network Secure는 이러한 C2 통신을 차단하도록 프로그래밍될 수 있으며, 추가 피해가 발생하지 않도록 하고 보안 운영자에게 추가 조사 및 처리를 위해 경고할 수 있습니다.

Engine Zero AI Powered Detection Engine

AI Detection Engine



Engine Zero vs Traditional Detection Technologies

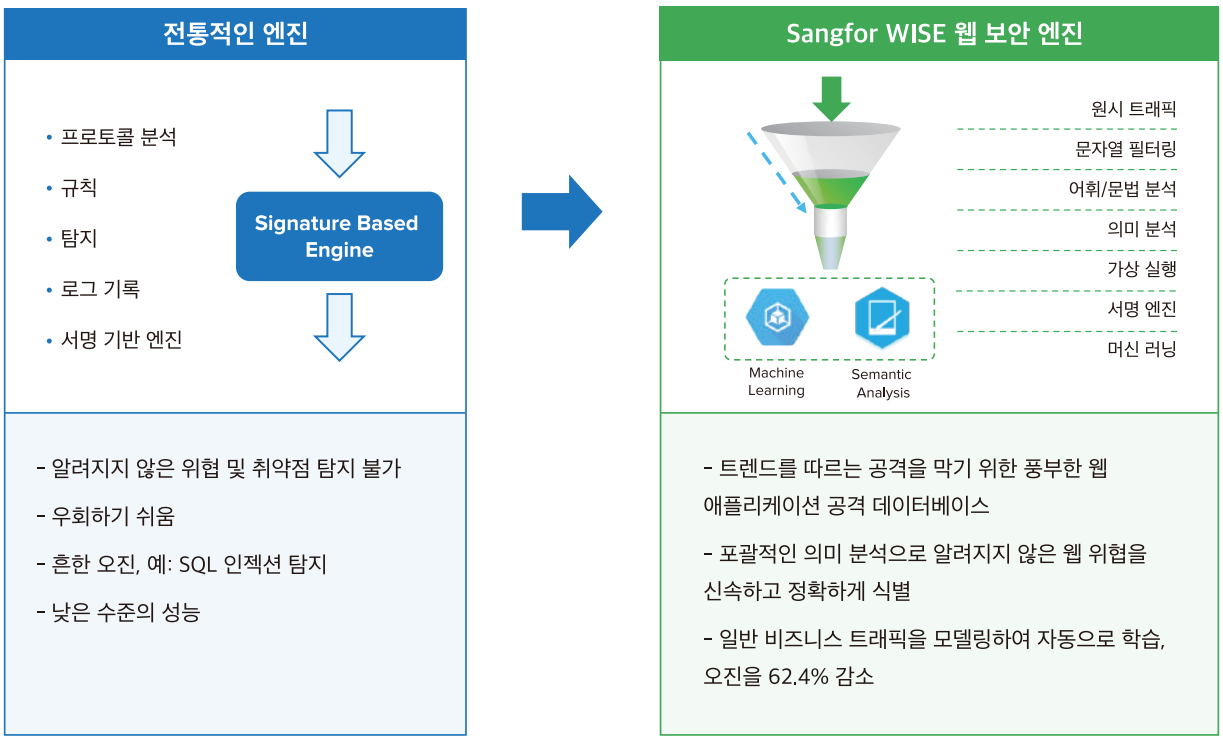
전통적인 탐지 기술에는 주로 서명 기반 탐지(해시, 바이러스 서명 등), 규칙 매칭, 가상 실행, 그리고 샌드박스가 포함됩니다. 이러한 기술들의 위협 탐지 능력은 서명 기반 탐지에서 샌드박스까지 점진적으로 향상됩니다. 하지만, 탐지 기술이 고도화될수록 성능은 일반적으로 저하되고 비용은 증가합니다. 이러한 전통적인 기술들과 비교할 때, Engine Zero는 다음과 같은 장점을 가지고 있습니다:

- **Strong generalization:** 기계 학습의 일반화 덕분에, Engine Zero는 사전 지식 없이도 미확인 바이러스나 기존 바이러스의 새로운 변종을 식별할 수 있습니다. 하지만 전통적인 솔루션은 먼저 샘플을 확보해야 하므로 새로운 악성 소프트웨어가 생성된 시점과 이를 탐지할 수 있는 시점 사이에 지연이 발생합니다.
- **Rapid speed:** 서명 기반 탐지에 가까운 거의 선형적인 스캔 속도.

  낮은 메모리 점유율: 리소스 비용 측면에서 Engine Zero는 200MB 미만의 메모리만 점유하여, 기존의 전통적인 엔진들보다 더 적은 메모리를 사용합니다.
- **A high degree of automation:** Engine Zero의 AI 모델은 인간의 개입 없이 자동으로 학습하고 특징을 추출할 수 있습니다. 이 모델은 클라우드에서 진화하며, 탐지 및 자동화 능력이 지속적으로 향상됩니다. 하지만 전통적인 탐지 기술은 전문가가 수작업으로 바이러스 지문과 서명을 추출해야 하므로 비용이 많이 들고 탐지가 누락될 가능성이 있습니다. "새로운" 바이러스는 전통적인 안티바이러스 벤더가 바이러스 데이터베이스를 업데이트하기 전에 이미 오랫동안 존재했을 수 있습니다.

전통적인 탐지 솔루션의 부족함에도 불구하고, 이들은 여전히 독특한 가치를 가지고 있습니다. 예를 들어, 블랙리스트와 화이트리스트 메커니즘을 사용하여 신속하게 대응할 수 있습니다. 따라서 Engine Zero는 고급 AI와 전통적인 탐지 기술을 결합하여 뛰어난 성능과 높은 탐지 정확도를 제공합니다.

The Only NGFW with Enterprise-Grade WAF



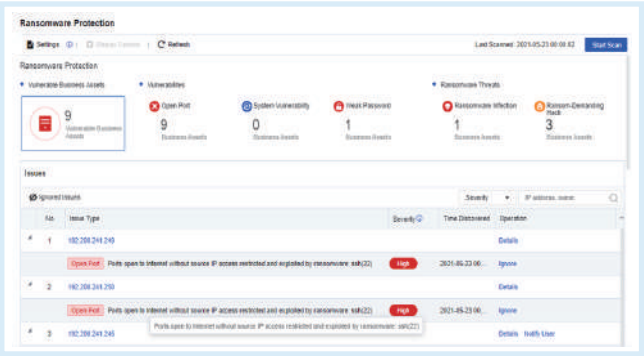
3. Simplified Security Operation

전담 IT 보안 팀이 없는 소규모 또는 중규모 조직은 매주 수천 건의 경고를 받고, IT 부서는 조사와 분석에 많은 시간을 할애하게 되어 운영 비용이 증가합니다. 이것은 IT 운영자에게 악몽과 같은 상황이며, 보안 사고의 근본 원인을 파악하고 피해를 최소화하며 미래의 공격으로부터 보호하기 위한 조치를 취해야 합니다. 또한, 지능적이거나 자동화된 보고 도구 없이 전통적인 보안 솔루션을 여전히 사용하는 조직은 큰 불리함을 가지며, 360도 가시성과 명확한 분석 및 보고가 없으면 효과적인 보안은 점점 더 어려워집니다.

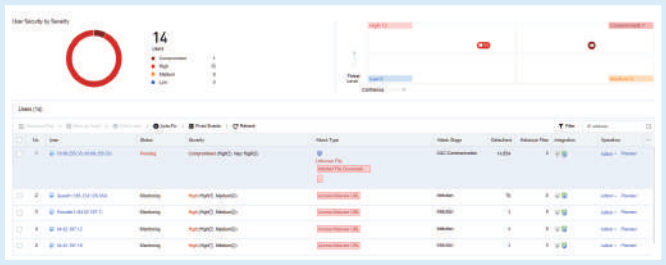
Sangfor Network Secure는 쉬운 배치와 간소화된 운영 및 유지 관리 기능을 통해 신뢰할 수 있고 수월한 보안을 제공하여 효과적이고 안전한 IT 환경을 가능하게 합니다. 내장된 구성 마법사는 보안 정책 배포를 간소화하며, 통합된 SoC Lite 모듈은 비즈니스 시스템에서 엔드포인트까지 조직의 전반적인 보안을 종단간 가시화합니다. Sangfor Network Secure는 수천 개의 경고 사이에서 실제로 위험한 보안 이벤트를 식별함으로써 일상적인 보안 운영을 간소화하고, 최상의 해결책에 대한 지침과 제안을 제공합니다. 랜섬웨어와 같은 유행하는 위협에 대한 전용 대시보드도 제공되어 관리자가 시기적절한 업데이트를 받을 수 있도록 돕습니다.

또한, 광범위한 자산과 IoT 가시성 구성요소는 IT 부서와 비즈니스 소유자가 비즈니스 시스템의 보안 상태를 적극적으로 확인할 수 있도록 하여, 자산의 온라인/오프라인 상태와 불법 네트워크 접근의 존재 등을 빠르게 파악할 수 있게 합니다. 이러한 검사는 IT 운영자가 허점을 닫고 정보에 입각한 결정을 내릴 수 있게 도와줍니다. 또한, Sangfor Network Secure는 수천 개의 정책 중 중복, 충돌, 오류 설정을 신속하게 식별할 수 있는 내장형 스마트 정책 최적화기를 특징으로 하고 있습니다.

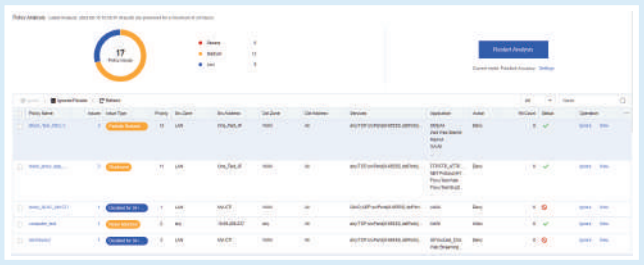
Asset Discover & Risk Management



Ransomware Threat Monitoring



User Security Overview



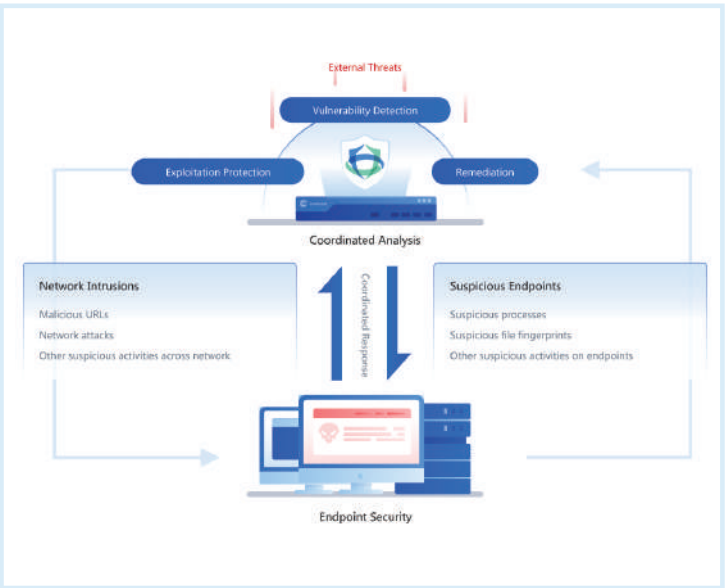
Smart Policy Optimizer

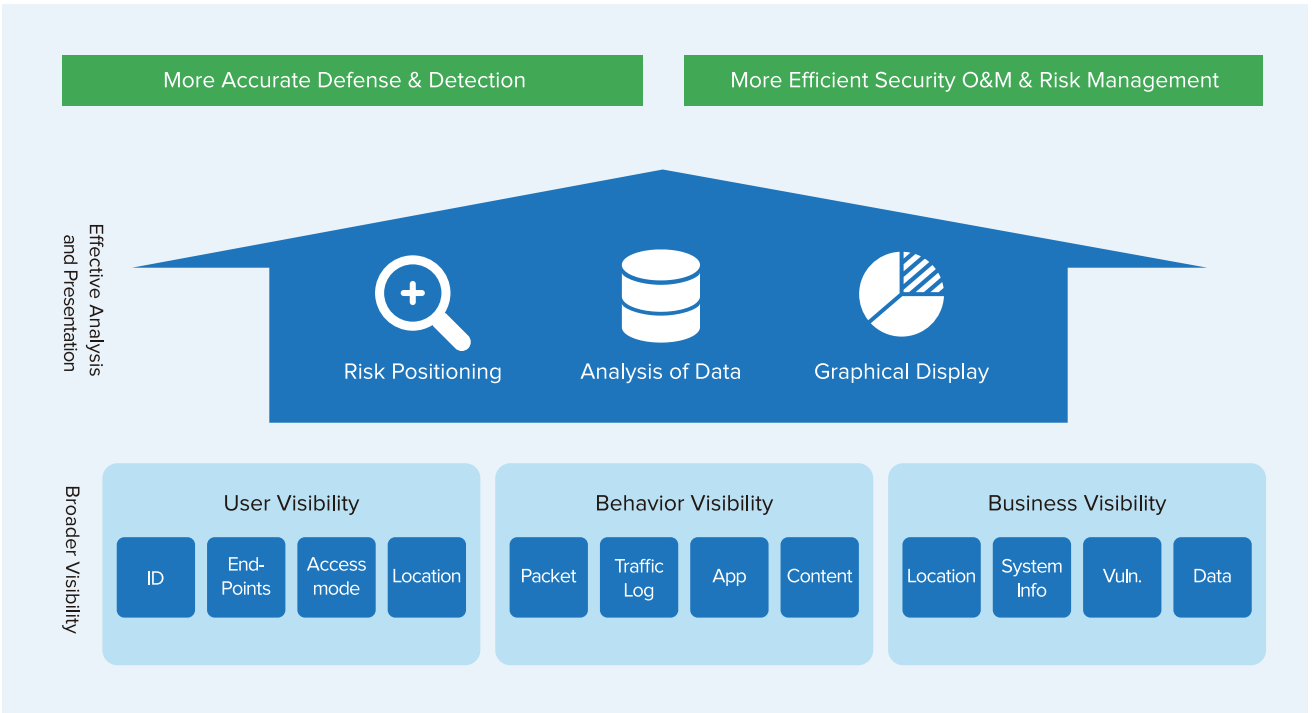
4. Security Synergy

복잡한 위협, 예를 들어 랜섬웨어와 암호 화폐 채굴 공격과 같은 경우, 침해된 엔드포인트와 공격자의 인프라 사이에서 명령 및 제어(C2) 통신을 확립하는 것은 킬 체인에서 필수적인 단계입니다. 그러나 방화벽 탐지나 수동 조사를 통해 C2 행동을 보이는 침해된 클라이언트를 정확하게 식별하는 것은, 특히 DHCP 환경에서, 매우 어려운 도전입니다. Sangfor는 이러한 도전을 인식하고 네트워크와 엔드포인트 보호를 조율함으로써 혁신적으로 이에 대응합니다.

Sangfor Network Secure & Endpoint Secure 통합은 네이티브 빌트인 API를 통해 강화된 원활한 협업을 가능하게 합니다. 이 통합을 통해 Sangfor Network Secure와 Endpoint Secure는 위협 인텔리전스와 관련 이벤트를 교환하여 C2 통신 및 기타 은밀한 행동을 탐지하는 데 도움을 줍니다. 이러한 조사 결과는 Network Secure의 단일 대시보드에서 통합되며, 이 대시보드는 위협, 악성 도메인, 피해 클라이언트의 이름 프로세스 및 권장 완화 전략에 대한 포괄적인 개요를 제공합니다. 보안 관리자는 악성 프로세스를 격리하거나 Network Secure 대시보드에서 직접 바이러스 검사를 시작할 수 있습니다.

Sangfor Network Secure와 Endpoint Secure 간에 생성된 시너지는 위협 탐지 및 대응을 크게 향상시키고 최소한의 투자로 운영을 간소화합니다.





Sangfor Network Secure Product Family

Performance

	NSF-1050A-I	NSF-1100A-I	NSF-3100A-I	NSF-7100A-I
Firewall Throughput [1,2]	10Gbps	20Gbps	30Gbps	70Gbps
Application Control Throughput [1,3]	6Gbps	12Gbps	20Gbps	40Gbps
NGFW throughput [1,4]	1.5Gbps	3Gbps	7Gbps	25Gbps
Threat Prevention Throughput [1,5]	820Mbps	1.5Gbps	3.6Gbps	15Gbps
Web Application Protect Throughput [1,6]	950Mbps	2.3Gbps	3.2Gbps	20Gbps
IPsec VPN Throughput [1,7]	600Mbps	1.5Gbps	3.5Gbps	10Gbps
Max IPsec VPN Tunnels	100	1000	4,000	20,000
Concurrent Connections	800,000	2,000,000	4,000,000	25,000.000
New Connections	20,000	90,000	180,000	600,000
Virtual Domains (Recommended/Max)	1/6	3/6	5/10	24/48

Hardware Specification

	NSF-1050A-I	NSF-1100A-I	NSF-3100A-I	NSF-7100A-I
Form Factor	Desktop	1U	1U	2U
RAM	4GB	8GB	16GB	48GB
Storage	128GB SSD	128G SSD	256G SSD	128G + 960G SSD
Power Supply Type	Single AC	Dual AC	Dual AC	Dual AC
Power Consumption (Max)	24W	40W	150W	300W
Operation Temperature	0°C – 45°C			
Humidity	5% - 90% non-condensing			
System Weight	3.08kg	7.96kg	8.78kg	21kg
Length x Width x Height (mm)	175 x 275 x 44.5	400 x 430 x 44.5	450 x 440 x 44.5	600 x 440 x 89
Hardware Bypass (Copper)	N/A	2	4	2
10/100/1000 Base-T	8	8	16	4
1G SFP	2	N/A	N/A	4
10G SFP+	N/A	2	6	8
Network Slots (In Use/Total)	N/A	0/1	0/2	0/4
Management Interface	1	1	1	1
Serial Port	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45
USB Port	2	2	2	2
Certificates	CE, FCC, ROHS			

Remarks

1. All throughput performance data is measured in the laboratory. The performance may vary depending on the actual configuration & network environment.

2. Firewall Throughput is measured with 1518 Bytes UDP packets.

3. Application Control throughput is measured with firewall and Application Control enabled. 64K HTTP packets

4. NGFW Throughput is measured with Firewall, Application Control, Bandwidth Management and IPS enabled. 64K HTTP packets

5. Threat Prevention Throughput is measured with Firewall, Application Control, Bandwidth Management, IPS, and Anti-Virus enabled. 64K HTTP packets

6. Web Application Protect Throughput is measured with Firewall, Application Control, Bandwidth Management, IPS and WAF enabled. 64K HTTP packets.

7. IPsec VPN Throughput include Sangfor to Sangfor device connection scenario and Sangfor to 3rd party device scenario.

Company Profile

Make Your Digital Transformation Simpler and Secure. This is Sangfor Technologies' commitment to our customers. Since forming in 2000, Sangfor has been a global leader of IT infrastructure, security solutions and cloud computing. Four business groups deliver industry leading products for Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Firewall, Secure Web Gateway, Endpoint Protection, Ransomware Protection, Incident Response, SASE, and SD-WAN. Constant innovation and dedication to creating value for our customers are the heart of our corporate strategy.

Sangfor's 9500+ employees take customer's business needs and user experience seriously by servicing and supporting them at over 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy, Türkiye and Mexico.

Continuous Innovation & Excellent Service

Sangfor invests at least 20% of annual revenue in R&D to improve products and develop new solutions at our five R&D centers located. With over 2,690+ patents, Sangfor has more patent applications submitted in 2023. This dedication to innovation enables us to release product updates every quarter and launch new products annually.

We pride ourselves on our excellent service. Customers enjoy fast 24x7 online support 365 days a year and personalized on-site service support from over 10,000 certified engineers at our three Customer Service Centers in Malaysia & China.

Sangfor has more than 100,000 satisfied customers worldwide, including Fortune Global 500 companies. Governments, universities & schools, financial institutions, manufacturing, and other industries trust us to protect them from the next generation of cyberthreats and help them on their journey to digital transformation with a future-proof IT infrastructure.

SANGFOR NETWORK SECURE

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi
Techpark (Lobby B), Singapore 408564
Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)
Unit 1612-16, 16/F, The Metropolis Tower,
10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR INDONESIA
Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav.
B 10-11 Kuningan, Setia Budi, Kecamatan Setiabudi, Kota Jakarta
Selatan, Daerah Khusus Ibukota Jakarta 12910, Indonesia
Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA
No. 45-10 The Boulevard Offices, Mid Valley City,
Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3645

SANGFOR THAILAND
141 Major Tower Thonglor (Thonglor10) Floor 11 Sukhumvit Road,
Kholngtan Nuea Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES
Unit 14B 14th Floor, Rufino Pacific Tower, 6784 Ayala Avenue,
Makati City, Metro Manila, Philippines
Tel: (+63) 916-267-7322

SANGFOR VIETNAM
210 Bùi Văn Ba, Tân Thuận Đông, Quận 7,
Thành phố Hồ Chí Minh 700000, Vietnam
Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA
Floor 15, Room 1503, Yuwon bldg. 116, Seosomunro,
Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

SANGFOR UAE
D-81 (D-Wing), Dubai Silicon Oasis HQ Building,
Dubai, UAE
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
Office No.210, 2nd Floor, "The Forum",
Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton, Karachi, Pakistan
South Region: +92 321 2373991
North Region: +92 345 2869434
Central Region: +92 321 4654743

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-6487-73

SANGFOR TÜRKIYE
A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk,
Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul
Tel: (+90) 216-5156969

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

Network Secure - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

Omni-Command - Extended Detection and Response
Revolutionize Your Cyber Defense with Intelligent XDR

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/AI Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
Seamless Experience, Secure and Efficient

Access Secure - Secure Access Service Edge
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

SANGFOR

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com

Copyright © 2024 Sangfor Technologies. All Rights Reserved.

Sangfor Network Secure_BR_P_Sangfor Network Secure-Brochure_20240515