SANGFOR | Endpoint Secure

Endpoint Secure

Endpoint Security

The Future of Endpoint Security

Certification of the Best Windows Antivirus Solution
and "TOP PRODUCT" Award by AV-Test

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Recommended Windows Protection by

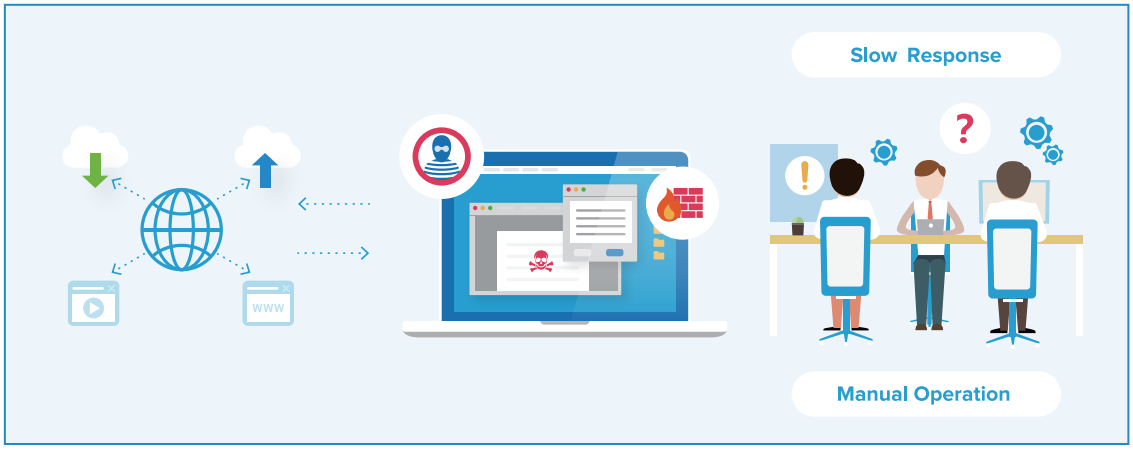
Microsoft

Enterprise-level endpoints face serious security challenges in a new era

기업의 LAN 엔드포인트와 데이터는 사이버 범죄자에게 상당한 가치가 있어 엔드포인트, 서버, 소프트웨어 및 하드웨어가 복잡하고 정교한 바이러스, 랜섬웨어 및 여러 다른 전파 방식의 심각한 공격 위험에 처해 있습니다. 이러한 심각한 엔드포인트 보안 도전과 더욱 엄격해지는 보호, 관리 및 애플리케이션에 대한 규정들은 적극적인 엔드포인트 보호를 필수적으로 만듭니다.

Manual operation and maintenance increase the cost of defense

전통적인 엔드포인트 보안 제품은 일반적인 정책과 특성을 기반으로 운영되며, 대개는 알려진 출처의 위협을 방어하기 위해 설계된 더 전통적인 조직 규칙 및 운영 규정에 기반을 둡니다. 이러한 전통적인 보안 접근 방식을 사용하는 조직은 더 복잡하고 고급 위협으로부터 공격을 받을 때 종종 노동 비용이 기하급수적으로 증가하는 경험을 하며, 전문 기업 운영 및 유지보수(O&M) 인력은 이러한 위협에 효과적으로 대응할 경험이 부족합니다.

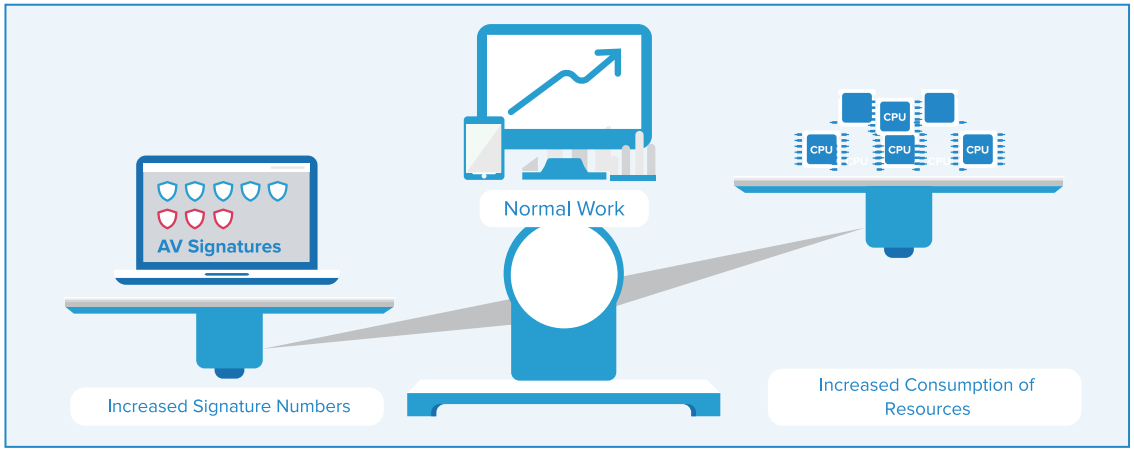


Feature matching response to viruses is inadequate protection to new attack methods

고급 위협으로부터 지속적인 위험이 있는 환경에서, 더 수동적인 바이러스 데이터베이스 식별 및 대응 방법을 사용하는 바이러스 예방 방법은 종종 새로운 바이러스와 랜섬웨어에 의해 침투됩니다. 또한, 지역 특징 데이터베이스의 제한된 용량은 알려지지 않은 바이러스는 물론 일부 알려진 바이러스에 대한 기본적인 보호 요구사항을 충족하지 못하는 경우가 많습니다.

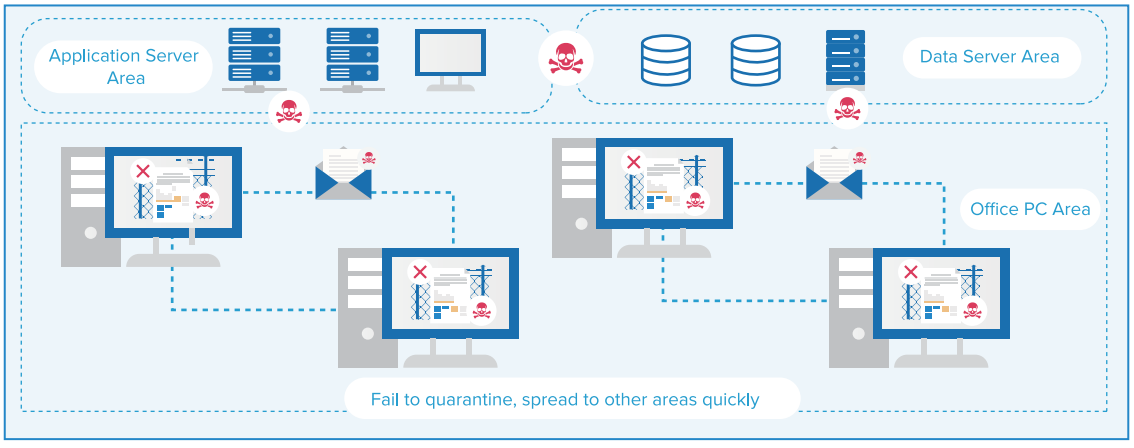
High-capacity antivirus feature databases lead to increased host computing resource costs

바이러스 특성 데이터베이스의 양이 점차 증가함에 따라 엔드포인트 저장 공간 및 컴퓨팅 자원의 비용이 증가합니다. 위협 방어가 상당한 양의 근무 시간과 직원 노력을 독점할 때, 사용자들은 클라우드로의 전환과 같은 최적화 시나리오에 집중할 수 없습니다.



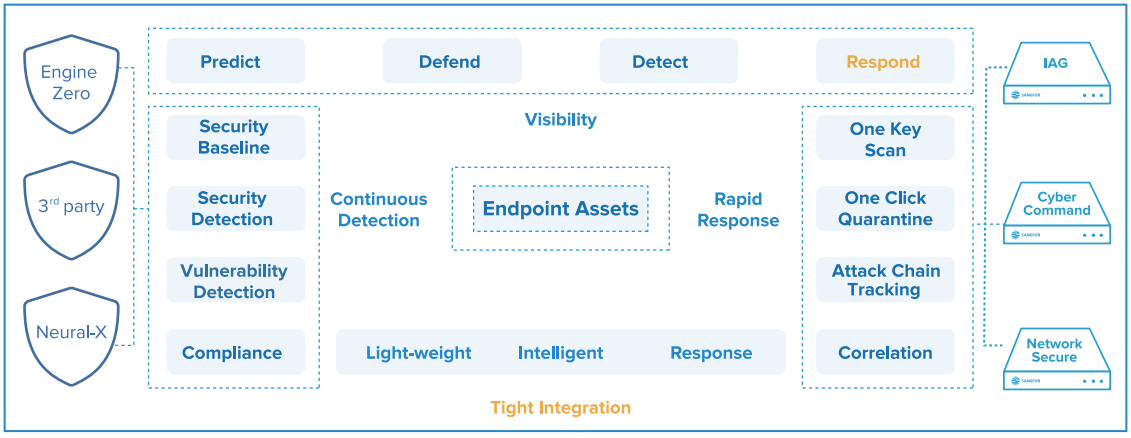
Outdated virus protection is incompatible with new propagation modes and virus environments

파일 격리 방식을 기반으로 한 바이러스 킬링은 구식이며, 실패할 경우 단일 지점 위협이 빠르게 퍼질 수 있습니다. 새로운 바이러스와 전파 방식은 종종 새로운 위협과 환경에 적응하도록 설계되지 않은 전통적인 바이러스 백신 제품을 우회할 수 있습니다.

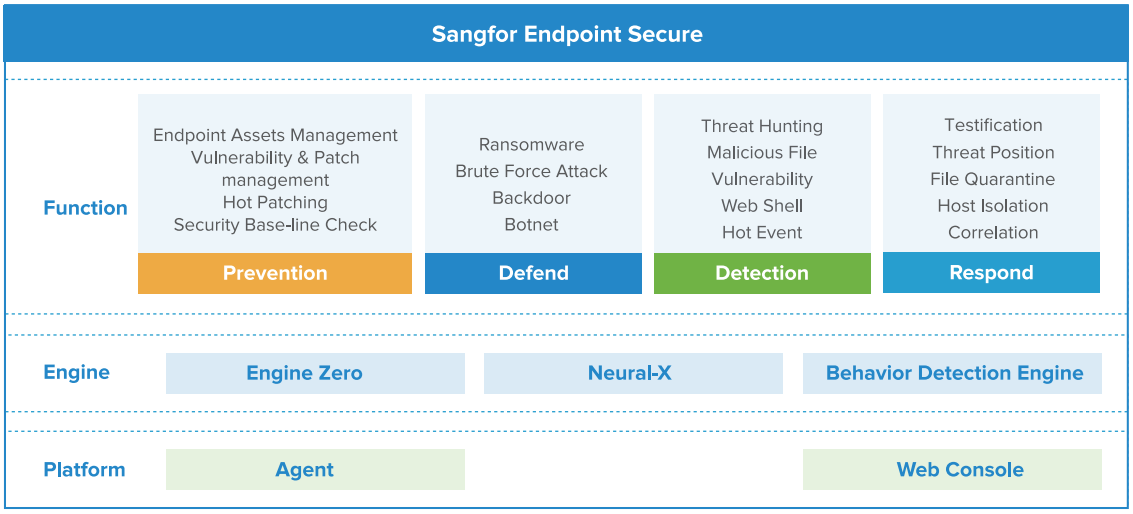


Sangfor Endpoint Secure

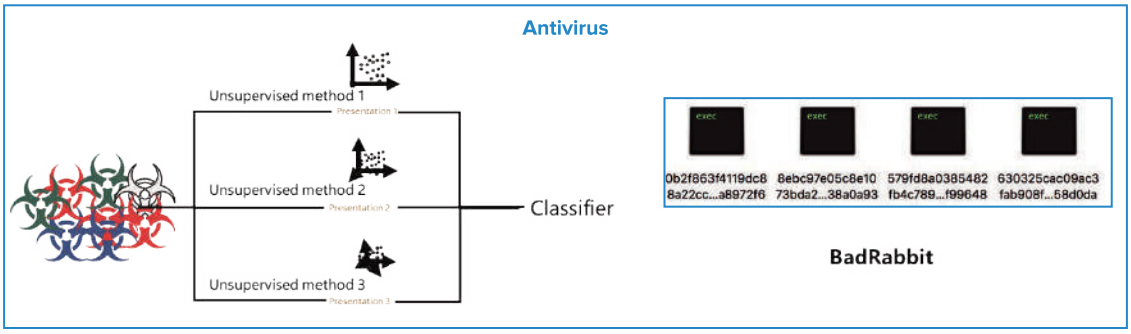
Sangfor의 엔드포인트 보호 및 대응 플랫폼(Endpoint Secure)은 엔드포인트에 더 자세한 격리 정책을 제공하여, 보다 정확한 검색 및, 지속 가능한 탐지 능력 및 예방, 방어, 탐지 및 대응을 포함한 더 빠른 처리 능력을 가능하게 합니다. Endpoint Secure는 클라우드 연계 및 조정, 위협 정보 공유 및 다중 레벨 대응 메커니즘을 통해 구축됩니다. 고급 위협 대응은 즉각적이며, Endpoint Secure는 새로운 경량, 지능형 및 즉각적인 엔드포인트 보안 시스템을 통해 사용자가 어떠한 엔드포인트 보안 문제도 다룰 수 있도록 지원합니다.



Architecture of Endpoint Secure



Application Scenarios



위험 시나리오:

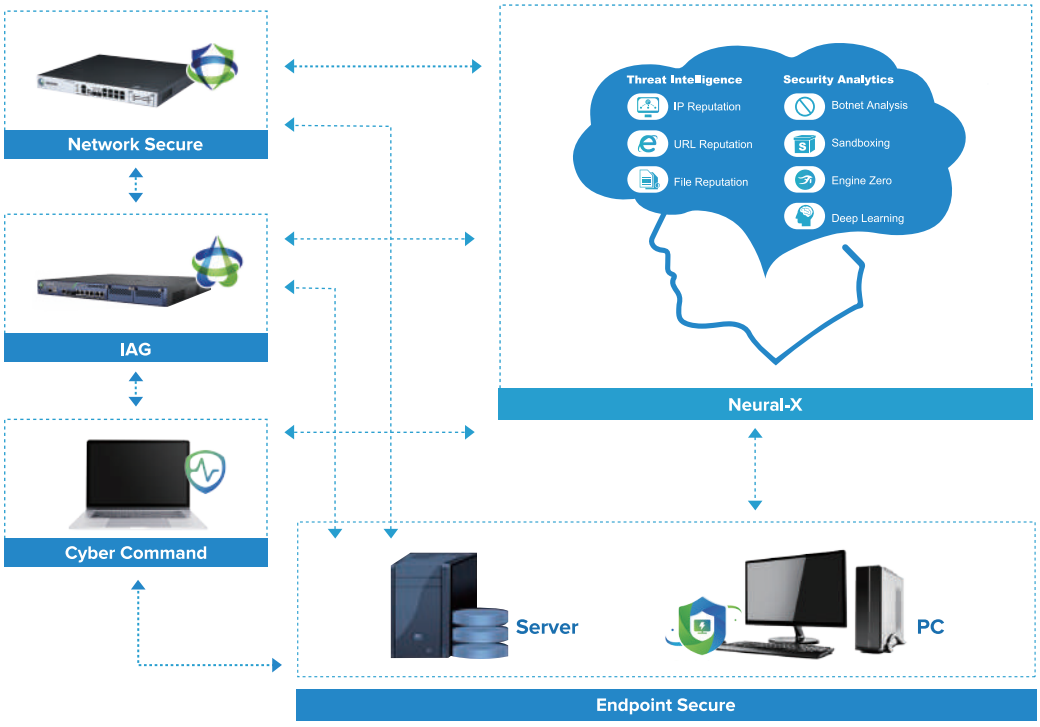
내부 엔드포인트가 여러 사무실 네트워크에 널리 배포되어 있습니다. 알려지지 않은 맬웨어 또는 랜섬웨어의 공격은 비즈니스 핵심 애플리케이션에 심각한 영향을 미치고, 조직의 핵심 데이터 보안을 위협합니다. 위험이 증가하는 이유는 다음과 같습니다:

1. 고급 및 알려지지 않은 위협을 감지하고 대응할 수 있는 자원 부족으로 인해 적극적인 방어가 방해받습니다.
2. 빠르게 움직이는 알려지지 않은 위협을 처리할 때 수동 시스템 관리가 부족하여 시스템이 수많은 공격 면에 노출됩니다.

Endpoint Secure 애플리케이션 효과:

1. 인공지능 코어와 시그니처 데이터베이스, 시그니처 및 행동 분석 기능의 보완은 즉각적이고 포괄적인 감지 및 예방이 가능한 100% 위협 방어 시스템을 제공합니다.
2. 다차원적인 혁신적인 마이크로 세분화 기술과 클라우드-파이프-디바이스 기능의 지능적 조정은 즉각적인 식별과 대응 및 포괄적인 위협 완화를 제공합니다.

Device Linkage



Risk Scenario:

대부분의 내부 인프라는 방화벽, 침입 방지 및 기타 다양한 경계 게이트웨이 장치를 활용하지만, 많은 게이트웨이 장치는 자체 독립 기능을 수행하여 일관되고 효과적인 보안 방어를 방해합니다.

1. 게이트웨이 장치가 독립적으로 악의적 공격을 방지하는 것은 경계가 침해되면 악의적 공격자가 빠르게 확산되어 통제할 수 없게 됨을 의미합니다.

2. 외부 위협이 알려져 있더라도 엔드포인트와 효과적인 공유 연계를 형성할 수 없으며 엔드포인트 제어를 달성할 수 없습니다.

애플리케이션 효과:

1. Endpoint Secure는 Sangfor Neural-X, Network Secure, IAG 및 Cyber Command와 조정 및 연결되어 클라우드, 경계 및 엔드포인트를 포괄하는 방어 구조를 형성하며 내부 및 외부 위협 정보를 실시간으로 공유합니다.

2. Endpoint Secure 지능 연계 메커니즘은 외부 위협 정보를 적시에 공유하여 자동 응답을 허용합니다.

Advantages and Characteristics

Ransomware Protection and Recovery

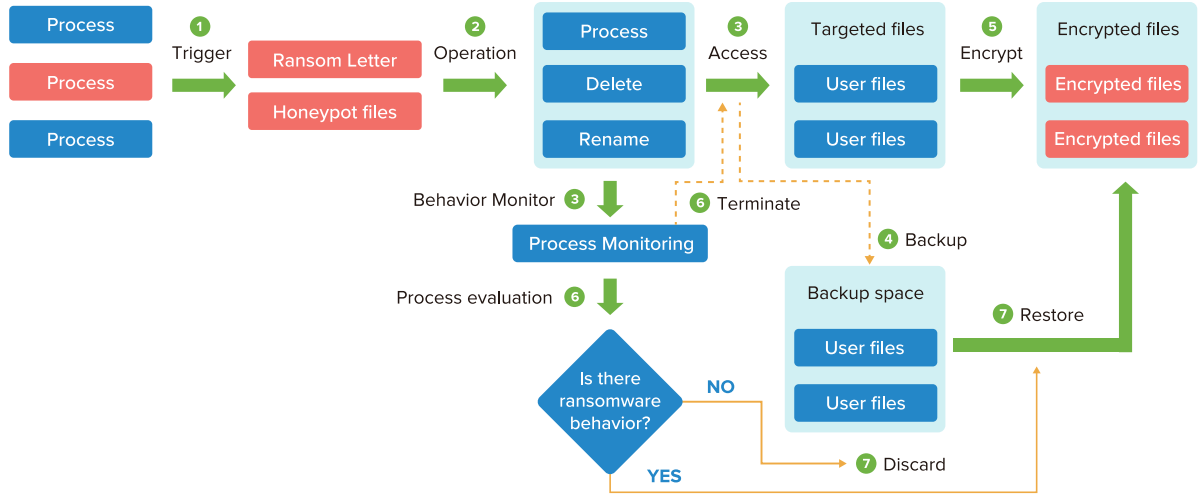
랜섬웨어 보호 및 복구

정적 및 동적 AI 기반 감지 엔진을 통해 모든 종류의 랜섬웨어로부터 보호합니다.

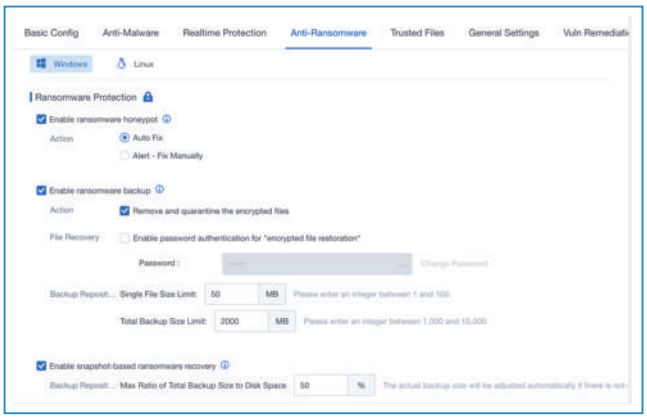
의심스러운 랜섬웨어 관련 프로세스를 감지하고 3초 이내에 차단하여 사용자의 자산에 미치는 영향을 최소화합니다.

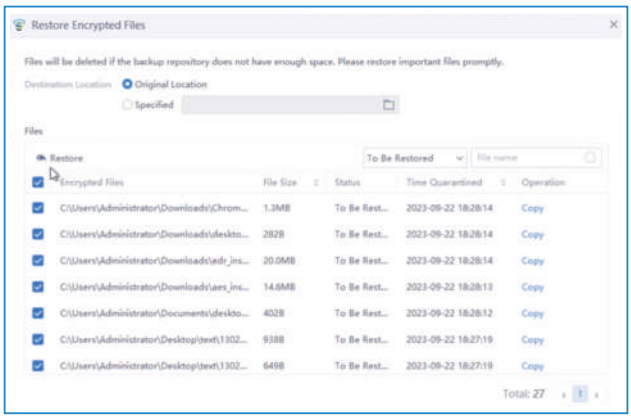
Sangfor Endpoint Secure에 배포된 1200만 대 이상의 장치에서 수집된 랜섬웨어 침해 지표를 통해 99.83%의 감지 정확도를 달성합니다.

허니팟과 RDP 이중 인증과 같은 기존 랜섬웨어 보호 기능 외에도, Sangfor Endpoint Secure는 파일 복구 및 Windows 볼륨 그림자 복사 서비스(VSS) 스냅샷 백업을 통한 복구 기능을 제공하여 랜섬웨어 암호화의 경우 데이터를 완전히 보호하고 복원할 수 있습니다.



1. Suspicious process makes a trigger on the system
2. Process tries to change or encrypt files
3. Behavior is monitored by Sangfor Endpoint Secure
4. Files are backed up in real time
5. Malicious process encrypts user files
6. Sangfor Endpoint Secure determines process is malicious and blocks and terminates the process
7. Backed up files are ready to be restored immediately



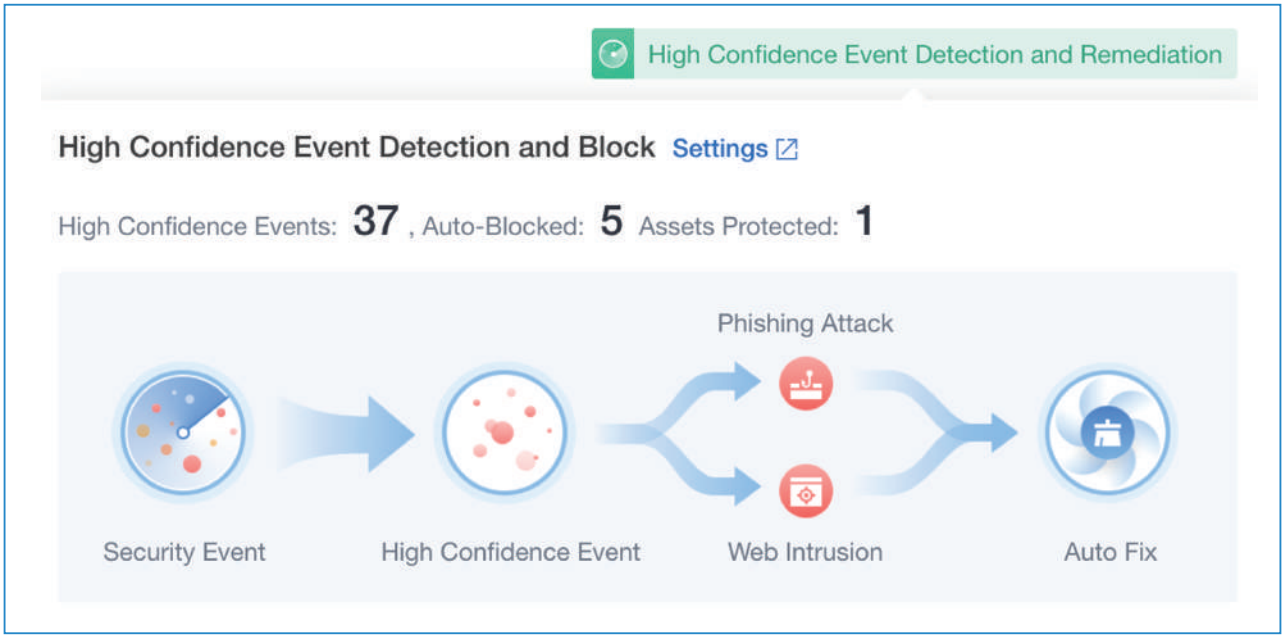


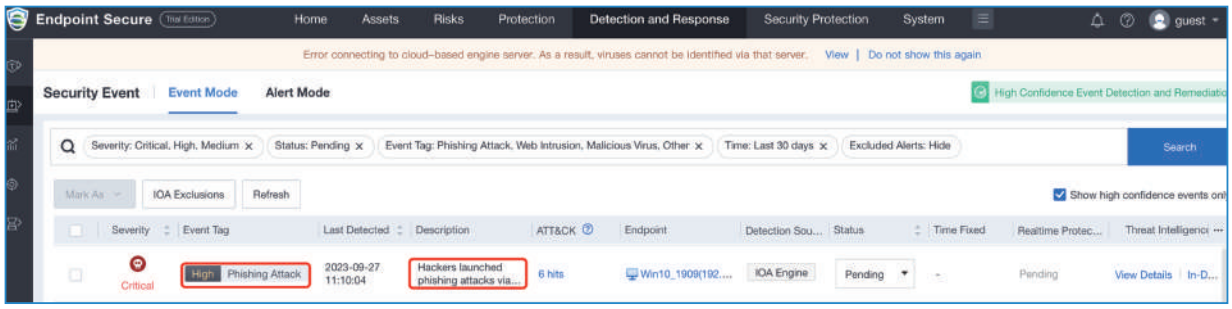
자동 응답을 통한 피싱 및 웹 침입 방지

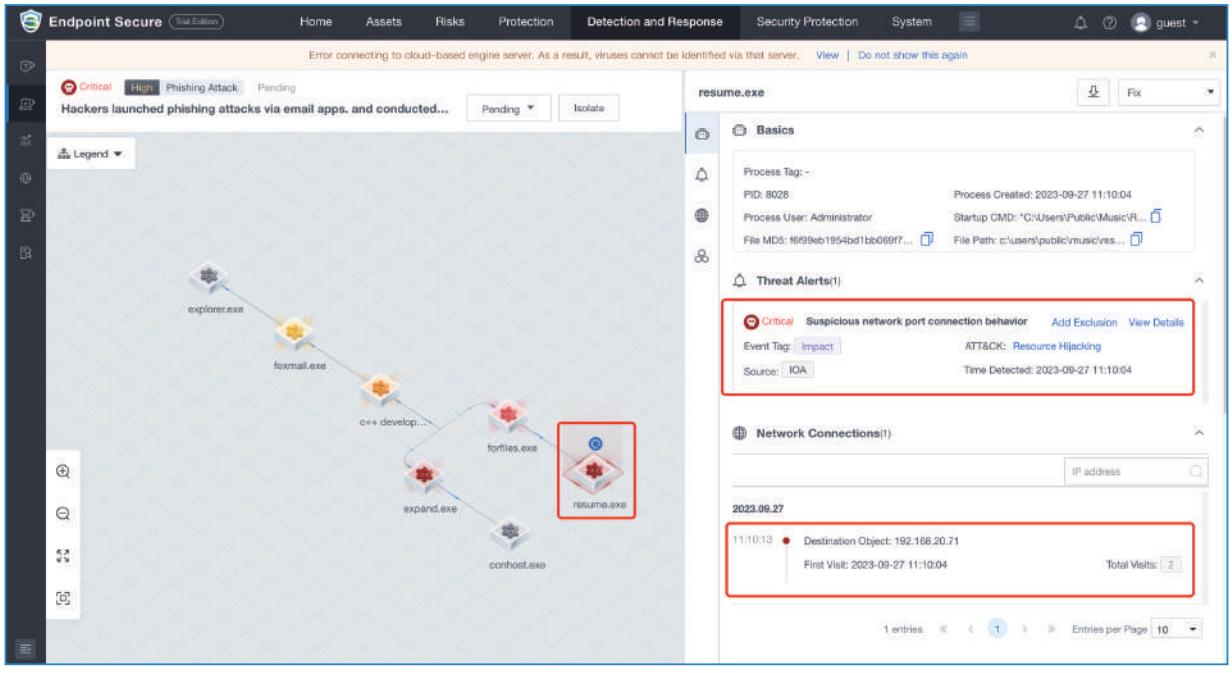
전 세계적으로 증가하는 사건 수에 대응하기 위해 피싱 및 웹 침입 공격에 대한 강화된 보호를 제공합니다.

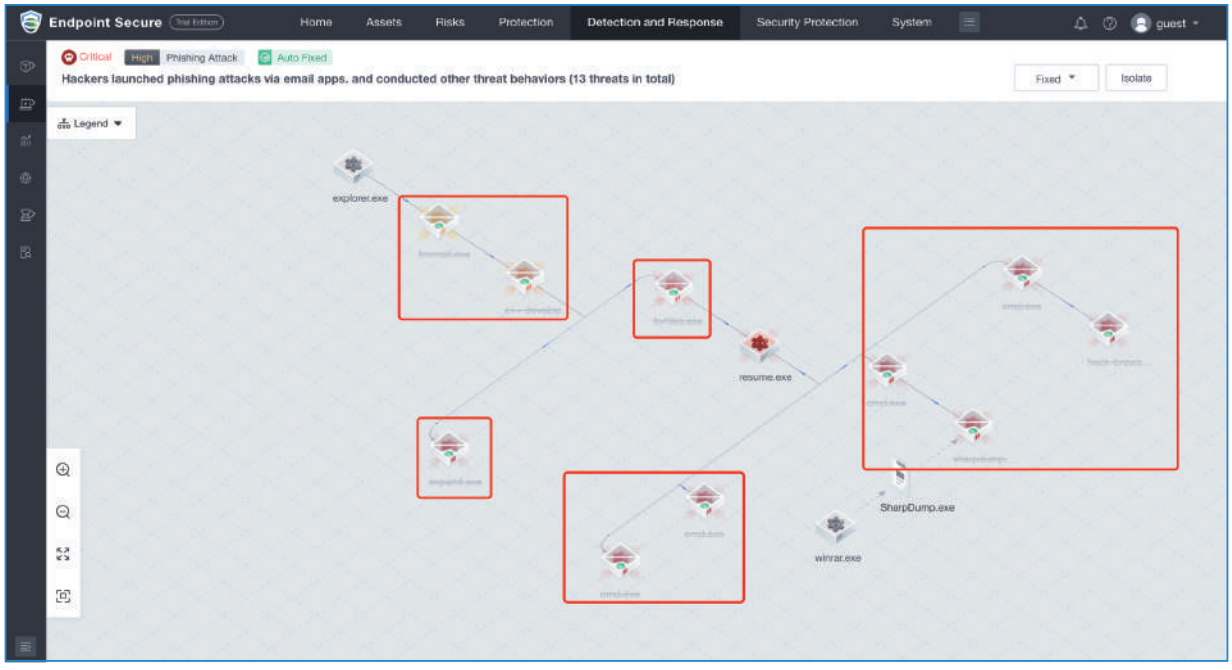
피싱 및 웹 침입 공격을 정확하게 감지하며, 공격의 원점과 관련 행동을 정확히 파악할 수 있는 포괄적인 시각적 킬 체인을 포함한 자세한 인사이트를 제공합니다.

사용자는 Sangfor Endpoint Secure를 구성하여 이러한 공격에 자동으로 대응하도록 설정할 수 있으며, 악의적인 프로세스 종료 및 악의적인 파일 삭제를 통해 측면 이동을 방지할 수 있습니다.




Endpoint Secure
Home
Assets
Risks
Protection
Detection and Response
Security Protection
System
guest
Security Event
Event Mode
Alert Mode
Search
Severity
Event Tag
Last Detected
Description
ATT&CK
Endpoint
Detection Sou...
Status
Time Fixed
Realtime Protec...
Threat Intelligenci
Critical
High
Phishing Attack
2023-09-27 11:10:04
Hackers launched phishing attacks via...
6 hits
IOA Engine
Pending
View Details


Endpoint Secure
Home
Assets
Risks
Protection
Detection and Response
Security Protection
System
guest
Critical
High
Phishing Attack
Pending
Hackers launched phishing attacks via email apps. and conducted...
Isolate
Legend
explorer.exe
foxmail.exe
c++ develop...
forfiles.exe
expand.exe
resume.exe
conhost.exe
resume.exe
Fix
Basics
Process Tag: -
PID: 8028
Process Created: 2023-09-27 11:10:04
Process User: Administrator
Threat Alerts(1)
Critical
Suspicious network port connection behavior
Add Exclusion
View Details
Event Tag: Impact
ATT&CK: Resource Hijacking
Source: IOA
Time Detected: 2023-09-27 11:10:04
Network Connections(1)
IP address
2023.09.27
11:10:13
Destination Object: 192.168.20.71
First Visit: 2023-09-27 11:10:04
Total Visits: 2
1 entries
Entries per Page 10


Endpoint Secure
Home
Assets
Risks
Protection
Detection and Response
Security Protection
System
guest
Critical
High
Phishing Attack
Auto Fixed
Hackers launched phishing attacks via email apps. and conducted other threat behaviors (13 threats in total)
Fixed
Isolate
Legend
explorer.exe
resume.exe
SharpDump.exe
winrar.exe

New Artificial Intelligent Antivirus Engine

기존의 안티바이러스 엔진과 달리, Engine Zero는 인공지능(AI) 비특징 기술을 도입하여 안티바이러스 데이터베이스에 등록되지 않은 미확인 바이러스와 변종을 효과적으로 식별할 수 있습니다.

AV-TEST에서 실시한 공식 성능 테스트에서 Sangfor Endpoint Secure는 보호, 성능, 사용성 면에서 만점을 받아 AV-TEST "TOP PRODUCT" 상을 수상하였습니다.like 1

Sangfor Engine Zero
Sangfor Anti-Malware Engine
Artificial Intelligence Based Non-Signature Engine
Detect Unknown Malware Accurately

Complete Antivirus Protection for Business PCs:

	Industry average	July 2023	August 2023
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 306 samples used	99.7%	100%	99.4%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 18,589 samples used	100%	100%	100%
Protection Score		6.0/6.0	

Figure 1. Sangfor Endpoint Secure Protect test results for Protection

Antivirus Solution for Business Efficiency:

	Industry average	July 2023	August 2023
Slowing-down when launching popular websites 65 websites visited	27%	24%	24%
Slower download of frequently-used applications 25 downloaded files	1%	1%	0%
Slower launch of standard software applications 70 test cases applied	9%	5%	5%
Slower installation of frequently-used applications 25 installed applications	19%	13%	12%
Slower copying of files, locally and in a network 9,772 files copied	3%	3%	2%
Performance Score		6.0/6.0	

Figure 2. Sangfor Endpoint Secure Protect test results for Performance

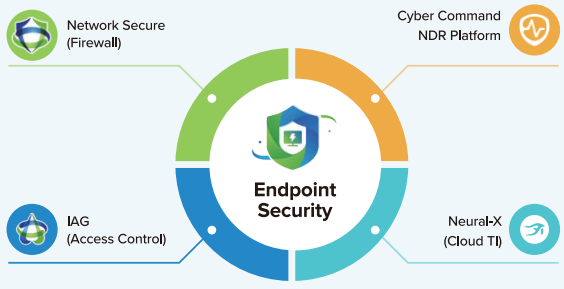
High Compatibility

Continuously protect the End of Support (EOS) OS system and provide hot patching function to protect None-Restart server.

Windows	macOS	Ubuntu	Redhat	CentOS	Debian	SuSE	Oracle Linux	Other
• Windows XP SP3 * • Windows 7 * • Windows 8 * • Windows 8.1 * • Windows 10 • Windows 11 • Windows Server 2003 SP2 * • Windows Server 2008 * • Windows Server 2008R2 * • Windows Server 2012 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.13 • macOS 10.14 • macOS 10.15 • macOS 11.x • macOS 12.x • macOS 13.x	• Ubuntu 10 • Ubuntu 11 • Ubuntu 12 • Ubuntu 13 • Ubuntu 14 • Ubuntu 16 • Ubuntu 18 • Ubuntu 20 • Ubuntu 22	• RHEL 5 • RHEL 6 • RHEL 7 • RHEL 8	• CentOS 5 • CentOS 6 • CentOS 7 • CentOS 8	• Debian 6 • Debian 7 • Debian 8 • Debian 9	• SUSE 12 • SUSE 11.X • SUSE 15.X	• Oracle Linux 5 • Oracle Linux 6 • Oracle Linux 7 • Oracle Linux 8 • Oracle Linux 9	• Red Flag Asianux Server 4 • NeoKylin 5 • NeoKylin 6 • NeoKylin 7 • KylinOS 4 • Ubuntu Kylin 18

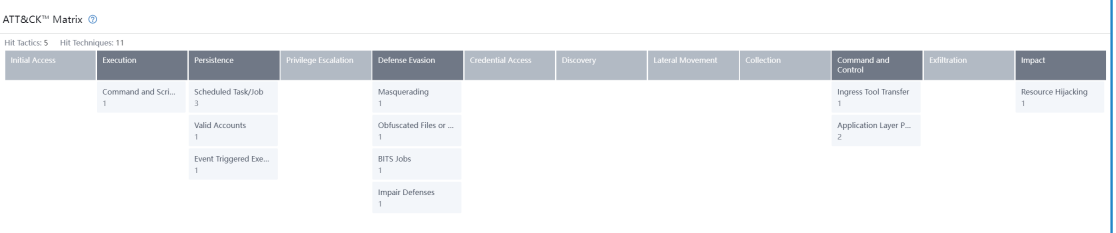
** The following Windows versions are no longer supported or receiving security updates from Microsoft.*

Multi-dimensional Linkage



Endpoint Security coordinated with Network Secure, IAG and Cyber Command to provide faster response and more integrated chain of evidence.

Advanced threat analysis & respond with MITRE ATT&CK®



Faster and more accurately find the threats in the endpoint.

Edition and Features

	Feature/Module	Essential Edition	Ultimate Edition
Prevention	Vulnerability Scan	✓	✓
	Remediation	✓	✓
	Security Compliance Check	✓	✓
	Asset Inventory	✓	✓
	Asset Discovery	✓	✓
	Micro-Segmentation		✓
	Hot Patching		✓
	TOTP Authentication	✓	✓
	Endpoint Behavior Data & Log Collection		✓
Protection	Realtime File Monitoring	✓	✓
	Ransomware Honeypot	✓	✓
	Ransomware Protection	✓	✓
	Ransomware Backup Recovery	✓	✓
	Ransomware Defense	✓	✓
	Fileless Attack Protection		✓
	End-of-Support Windows System Protection	✓	✓
	RDP Secondary Authentication (Anti-Ransomware)		✓
	Trusted Processes (Anti-Ransomware)		✓
	Key Directory Protection (Anti-Ransomware)		✓
Detection	Malicious File Detection	✓	✓
	APT Detection	✓	✓
	Brute-Force Attack Protection	✓	✓
	Improved Phishing and Web Intrusion Detection	✓	✓
	Coordinated Malware Response with XDDR		✓
	WebShell Detection		✓
	Advanced Threat Detection		✓
	Suspicious Login Detection	✓	✓
	Memory Backdoor Detection		✓
	Reverse Shell Detection		✓
	Local Privilege Escalation Detection		✓
	Remote Command Execution Detection		✓
Response	File Quarantine	✓	✓
	Endpoint Isolation	✓	✓
	File Remediation	✓	✓
	Virus Mitigation	✓	✓
	Automated Response to Phishing and Web Intrusion events	✓	✓
	Extended Detection, Defense and Response (XDDR)		✓
	Threat Hunting		✓
	Domain Isolation	✓	✓
	Process Blocking	✓	✓
Maintenance	Script File Upload	✓	✓
	USB Control	✓	✓
	Unauthorized Outbound Access Detection	✓	✓
	Remote Support	✓	✓
IT Governance	Application Blacklist		✓
	Software Metering		✓
	Software Uninstallation		✓

Ultimate Edition is recommended for device linkage scenario and advanced protection.

SANGFOR ENDPOINT 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

Sangfor_BR_P_Endpoint-Secure-Brochure_20240515