XG Firewall


SOPHOS
SOPHOS XG 450
SOPHOS
Protection
ENTER
ESC
COM
MGMT
RESET
PWR
COM
5 6 7 8
1/LAN 2/WAN 3/DMZ 4
10
9
BP
3/4
1/2
5 6 7 8
1 2 PoE Load 3 4
1 2 3 4
A B

필수적으로 요구되는 차세대 방화벽의 역할

SOFTWARE EXPLOITS

PROCESS ATTACKS

CRYPTO RANSOMWARE

UNKNOWN THREATS

CREDENTIAL HARVESTING

STEALTH MALWARE

Block Attacks

Visibility and Control (over users/apps)

Contain Threats

Visibility and Control

Over user and application traffic

Block Attacks

Stop hackers, attacks, and malware from entering thenetwork

Contain Threats

Block malware from spreading, exfiltrating data and communicating out

시작하기전에– 현재의 어려움...

Giving you an opportunity to talk about our exclusive advantages

현재 사용중인 방화벽은...

1. Risk에 대한 가시성을 제공하는가?
2. 지능형 위협을 차단하는가?
3. 네트워크내의 현재 사고에 대응하는가?

XG Firewall의 3가지 이점

SOPHOS

XG Firewall's Winning Advantages

최근 네트워크 보안의 가장 큰 문제점을 해결

1. 숨겨진 위험을 노출

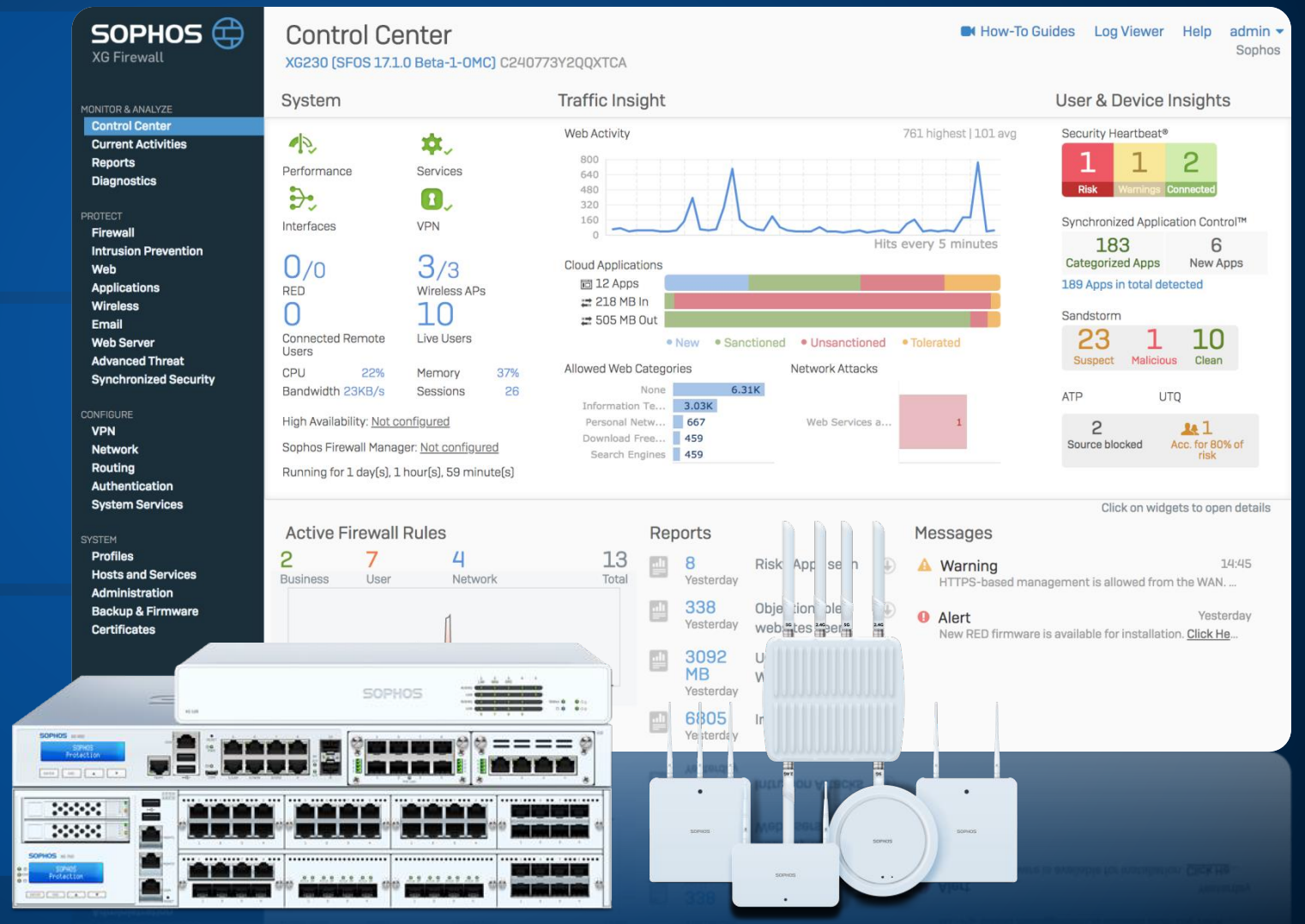
- ✓ 비주얼 대시보드와 풍부한 on-box리포팅
- ✓ 위험도 높은 유저와 의심스러운 payload의 식별
- ✓ 알려지지 않은 클라우드및 네트워크 어플리케이션 식별

2. 알려지지 않은 위협의 방어

- ✓ 전체 보안을 아우르는 Full suite – 쉬운 관리
- ✓ Deep learning
- ✓ 최고성능의 IPS Engine

3. 자동화된 사고 대응

- ✓ 유일한 Security Heartbeat™
- ✓ EP Health와 방화벽의 통합
- ✓ 감염된 시스템의 자동화된 격리

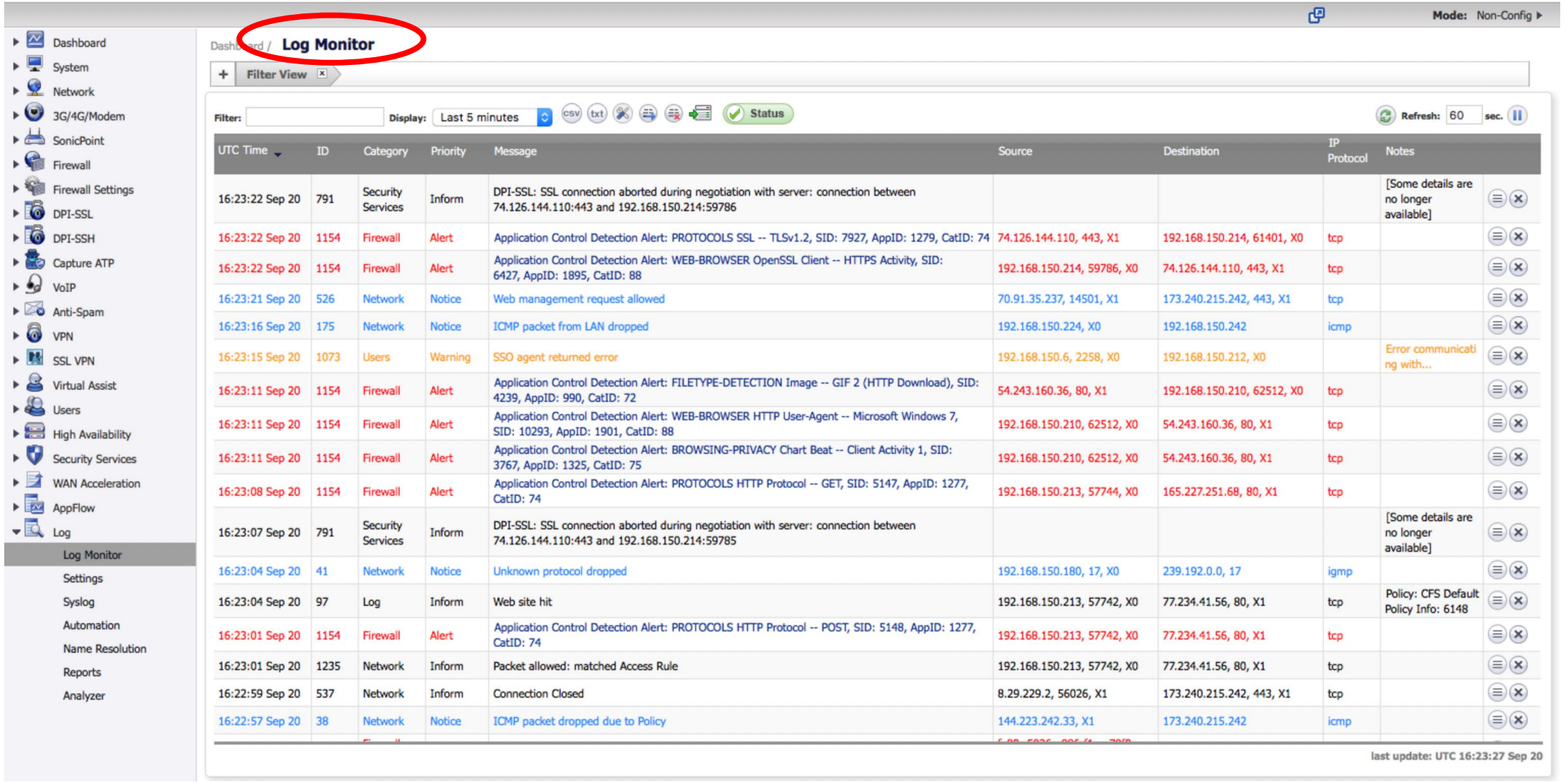


1. Reveal Hidden Risks

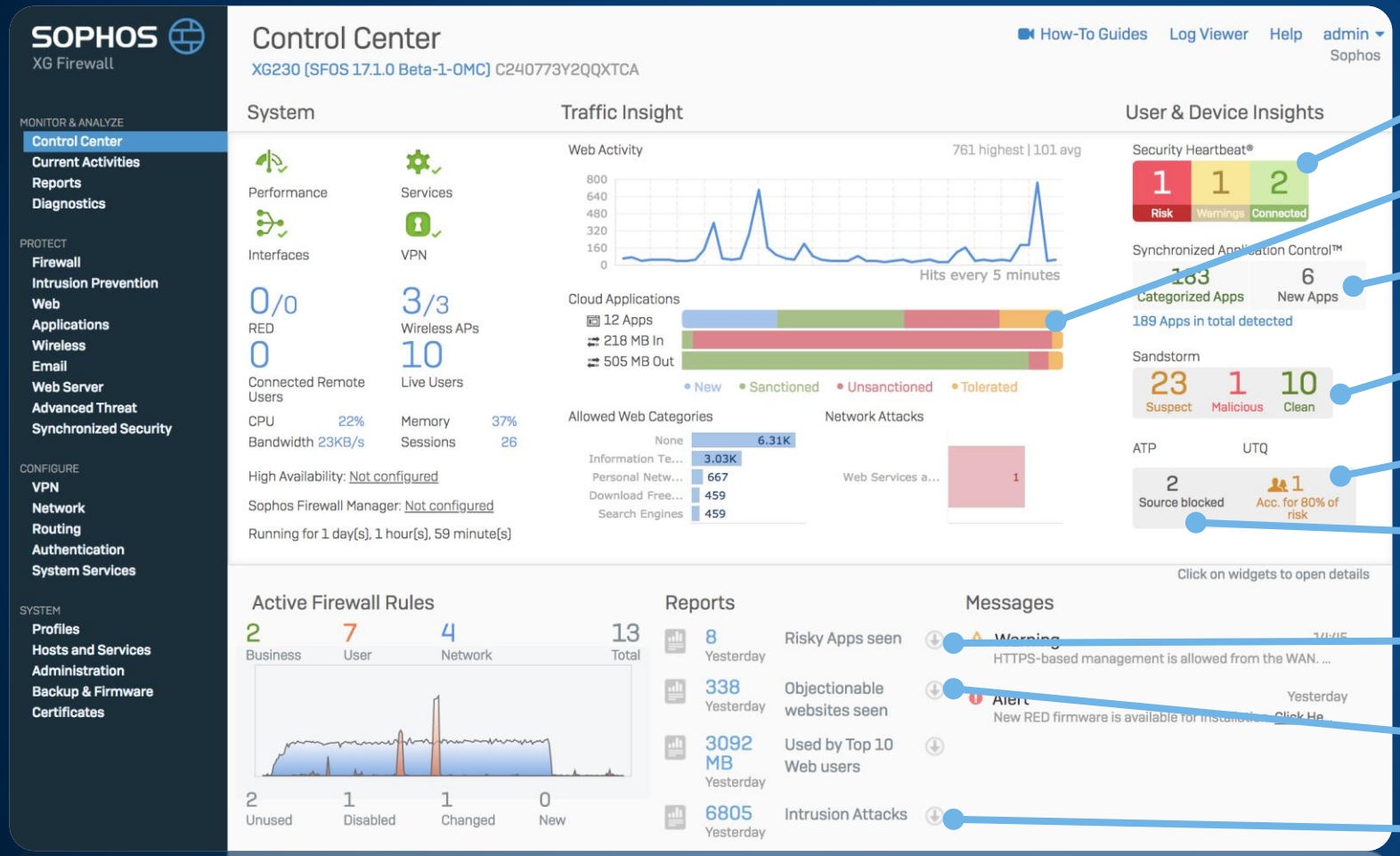
1. 숨겨진 위험의 노출

SOPHOS

현재의 방화벽들 – 활성화된 위협을 식별할 방법은?



XG Advantage: 가시적인 대화형 제어 센터 (Traffic-Light indicator)



위협 및 위험에 처한 시스템

승인되지 않은 Cloud Apps

알려지지 않은 Windows/Mac 앱

의심스러운 Payloads

위험도 높은 사용자

지능형 위협

위험도 높은 어플리케이션

부적합한 Websites

Intrusion Attacks

소포스는 위험 가시성 및 리포팅을 제공하는 유일한 벤더입니다.

CASB - Cloud App 가시성과 감춰진 IT 사용의 확인

클라우드 앱 가시성

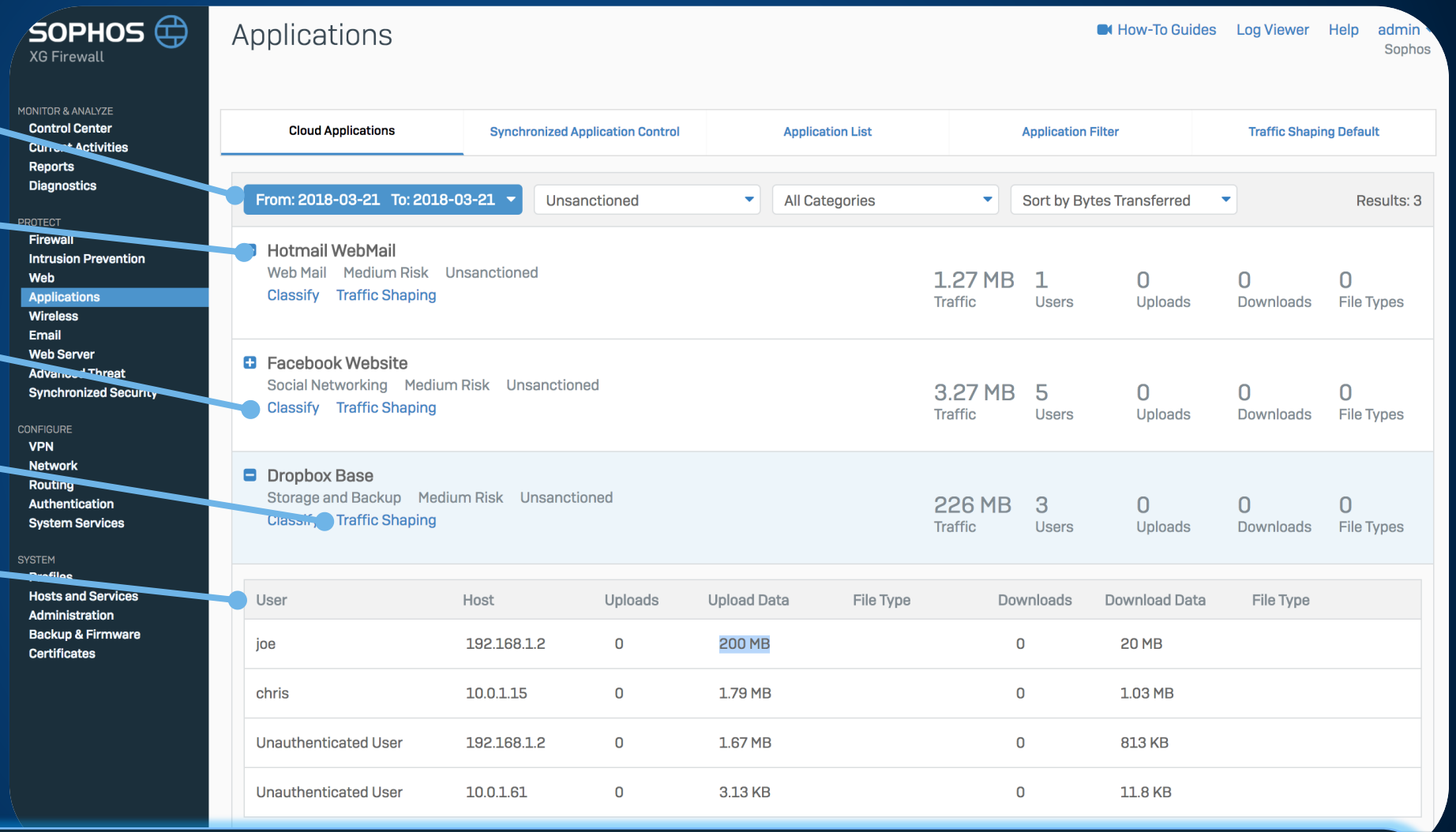
Filter / Sort

Cloud Application

Classify

Traffic Shape

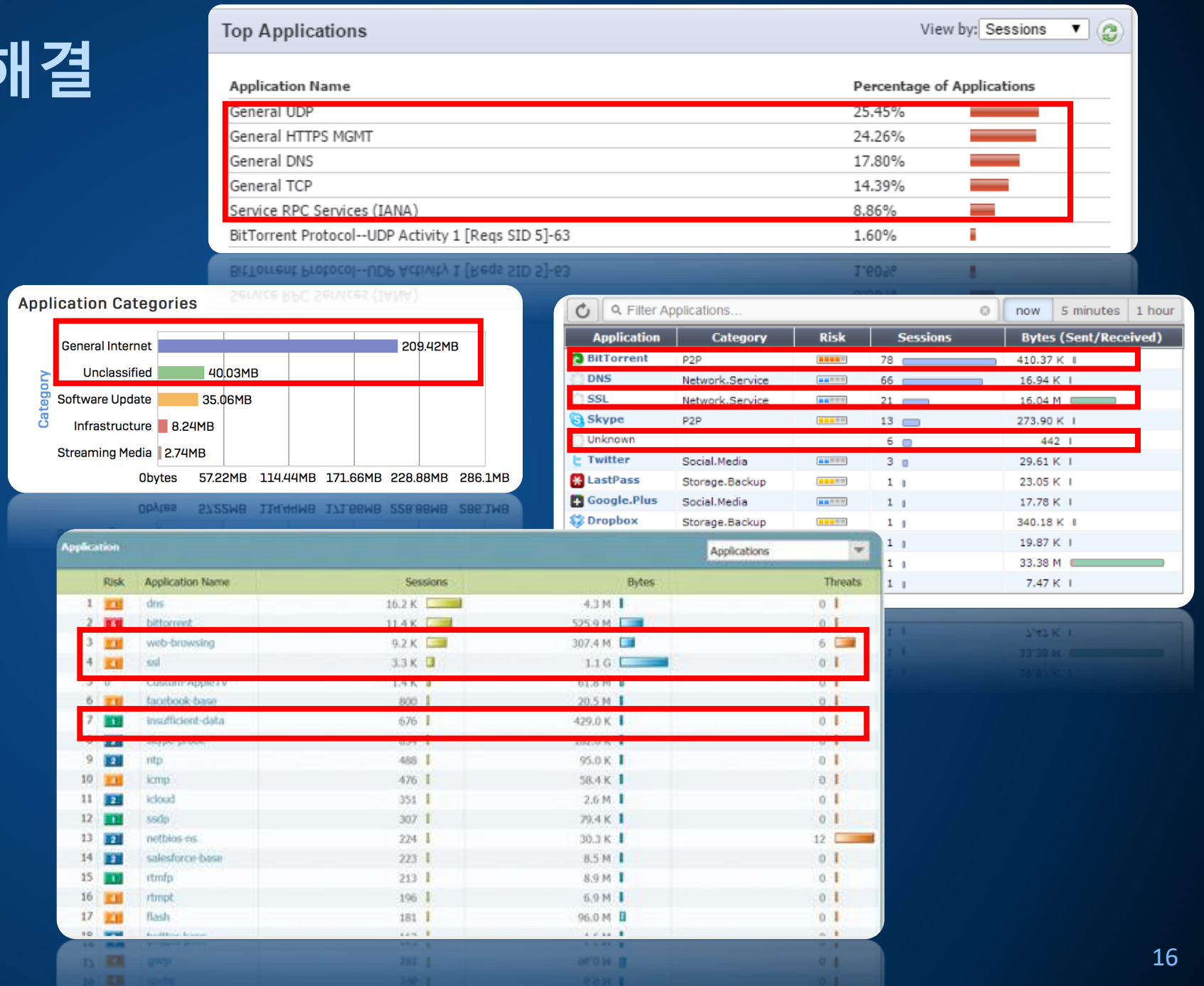
Users and Volume of Data



업계 최고의 앱 가시성이 더욱 향상되었습니다.

Application 문제 해결

- 방화벽 어플리케이션은 시그니처 기반입니다.
- 어플리케이션의 최대 90%가 인식되지 않습니다.
- 일부 앱들은 절대 시그니쳐를 갖을수 없습니다.
- 일부 앱들은 탐지회피 기능을 가지고 있습니다.
- 일부 앱들은 일반적인 Web커넥션을 갖고 있습니다 (HTTP/HTTPS)



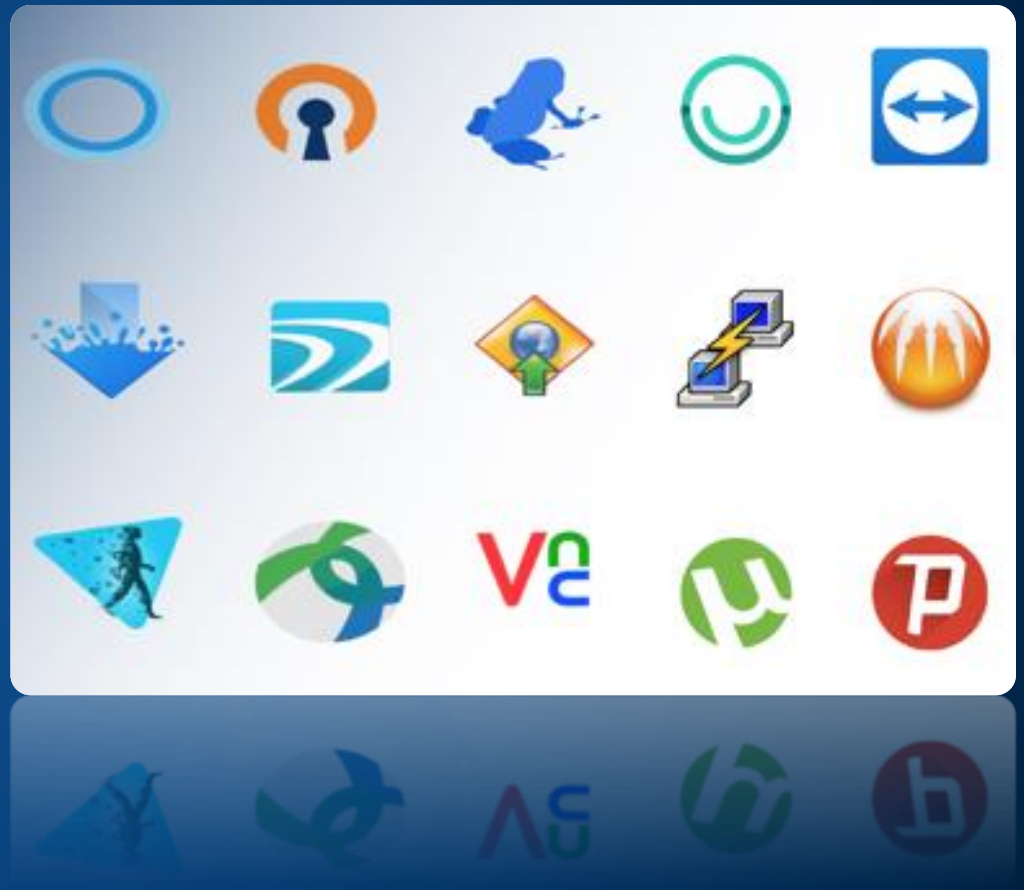
악성 Apps - 회피 및 분류되지 않는 상위 Applications

IM and Conference Apps
(Skype, TeamViewer)

BitTorrent and other P2P Clients
(uTorrent, Vuze, Freenet)

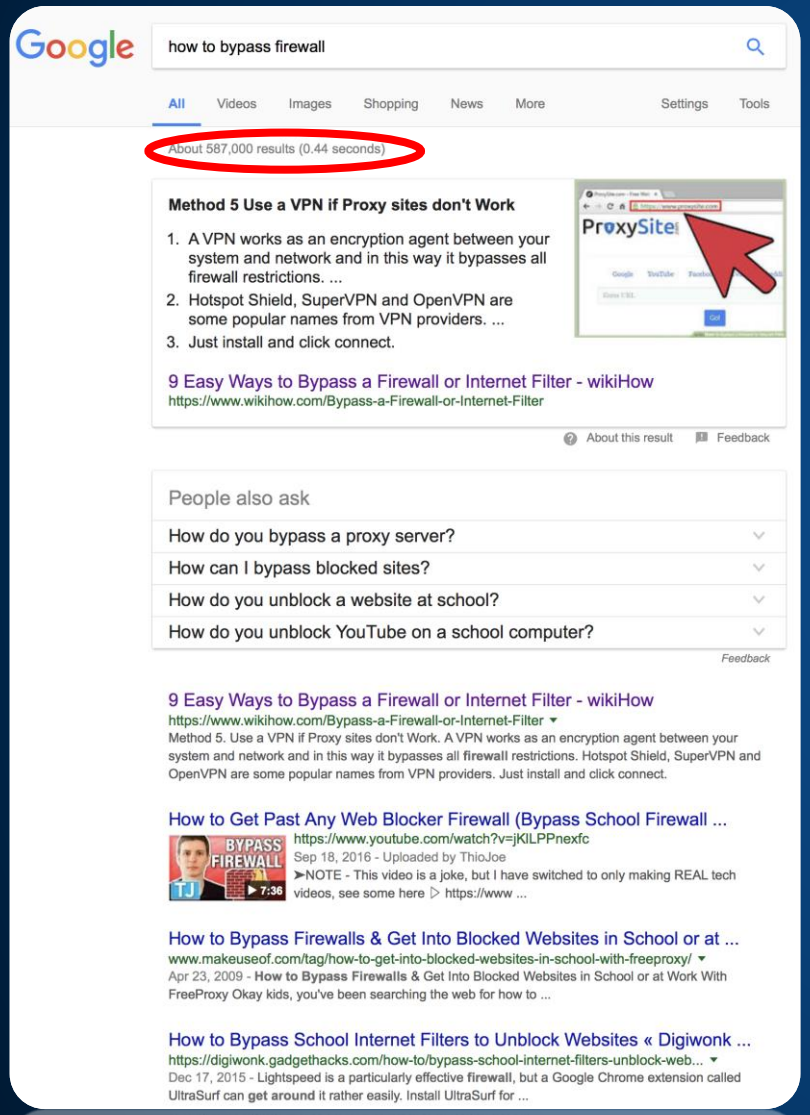
Proxy and Tunnel Clients
(Ultrasurf, Hotspot Shield, Psiphon)

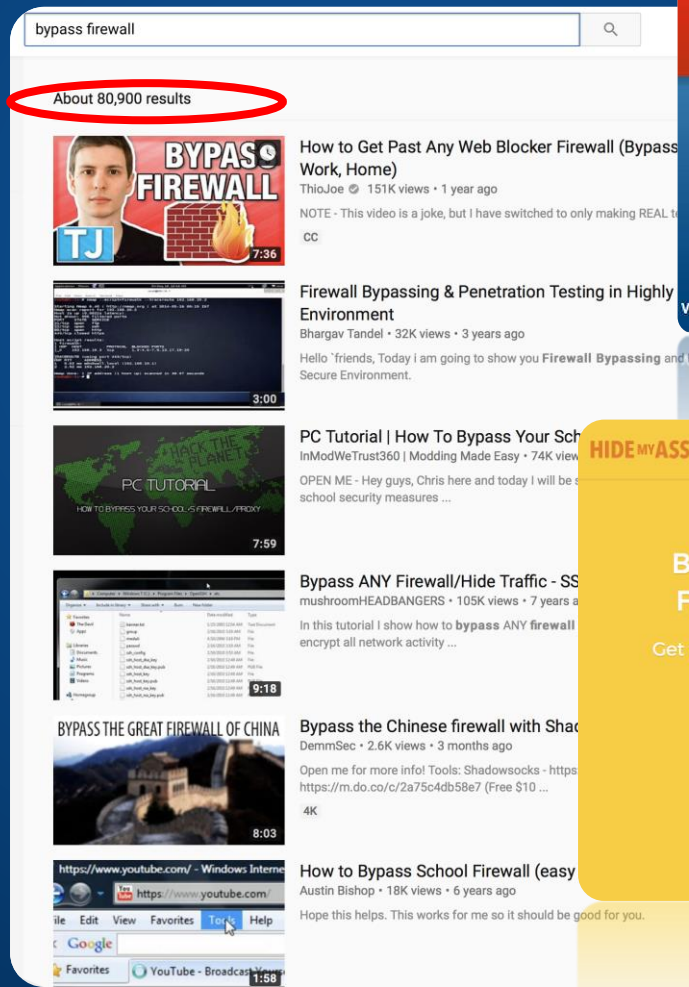
Games
(Valve and Steam)

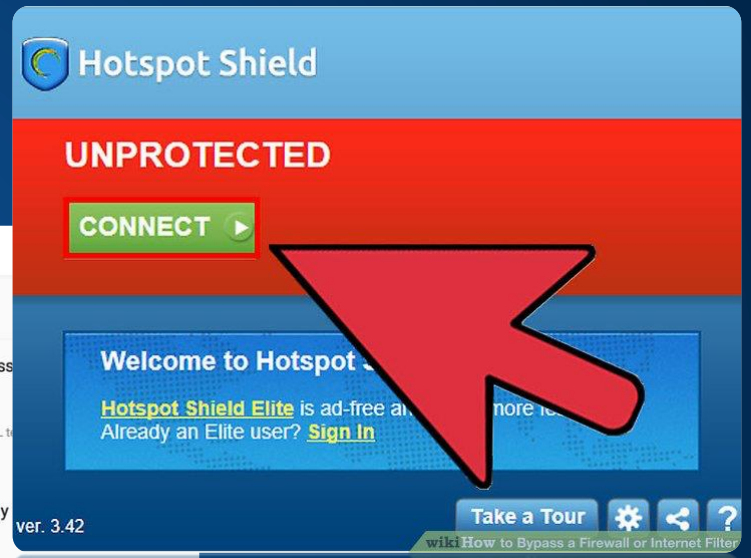


악성 사용자 – 방화벽의 제어를 회피중인

사용자, 어플리케이션, 심지어 멀웨어가 탐지를 회피하는 방법

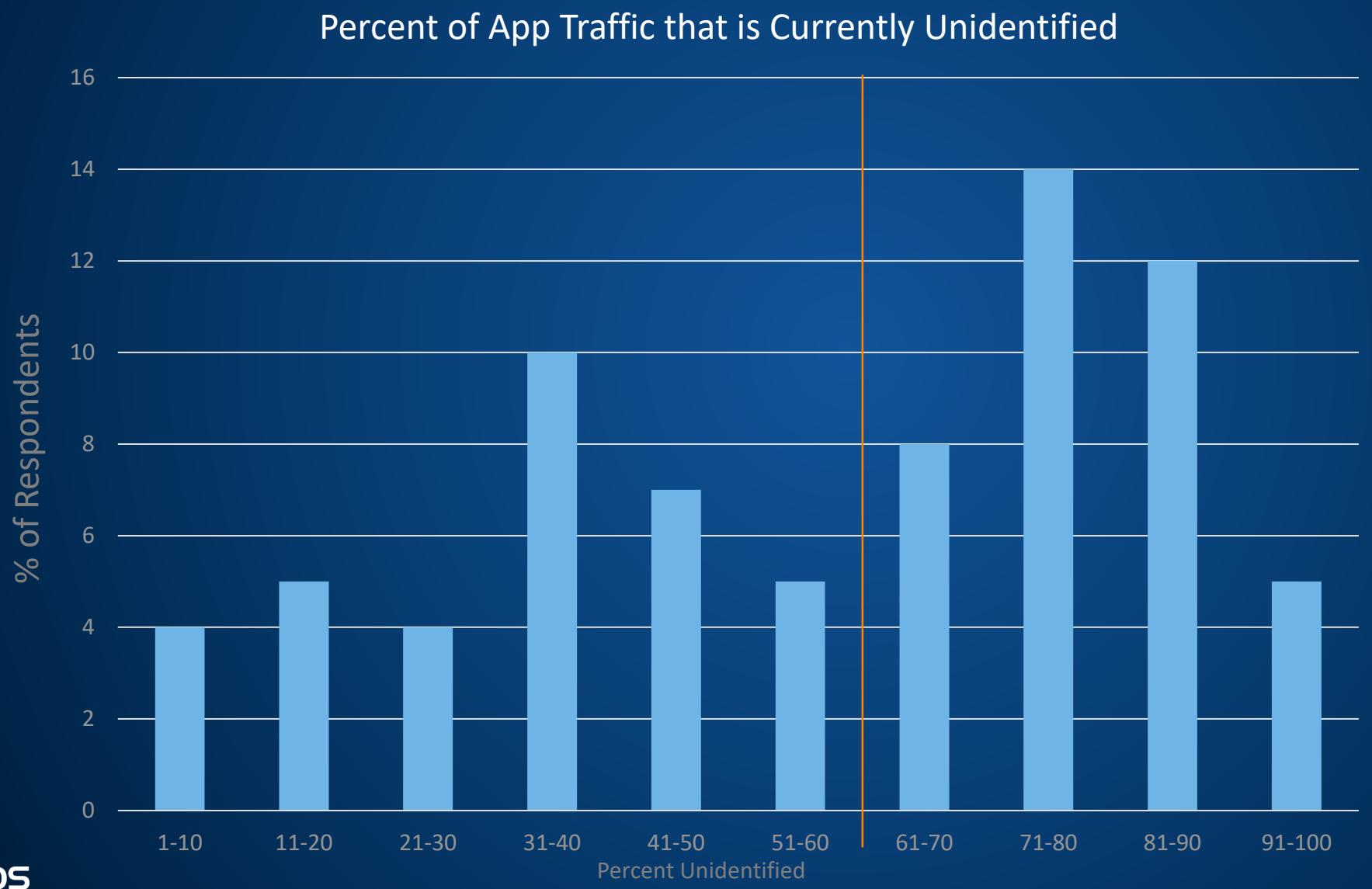






SOPHOS

이것이 얼마나 큰 문제인가요?



평균 트래픽의

60%

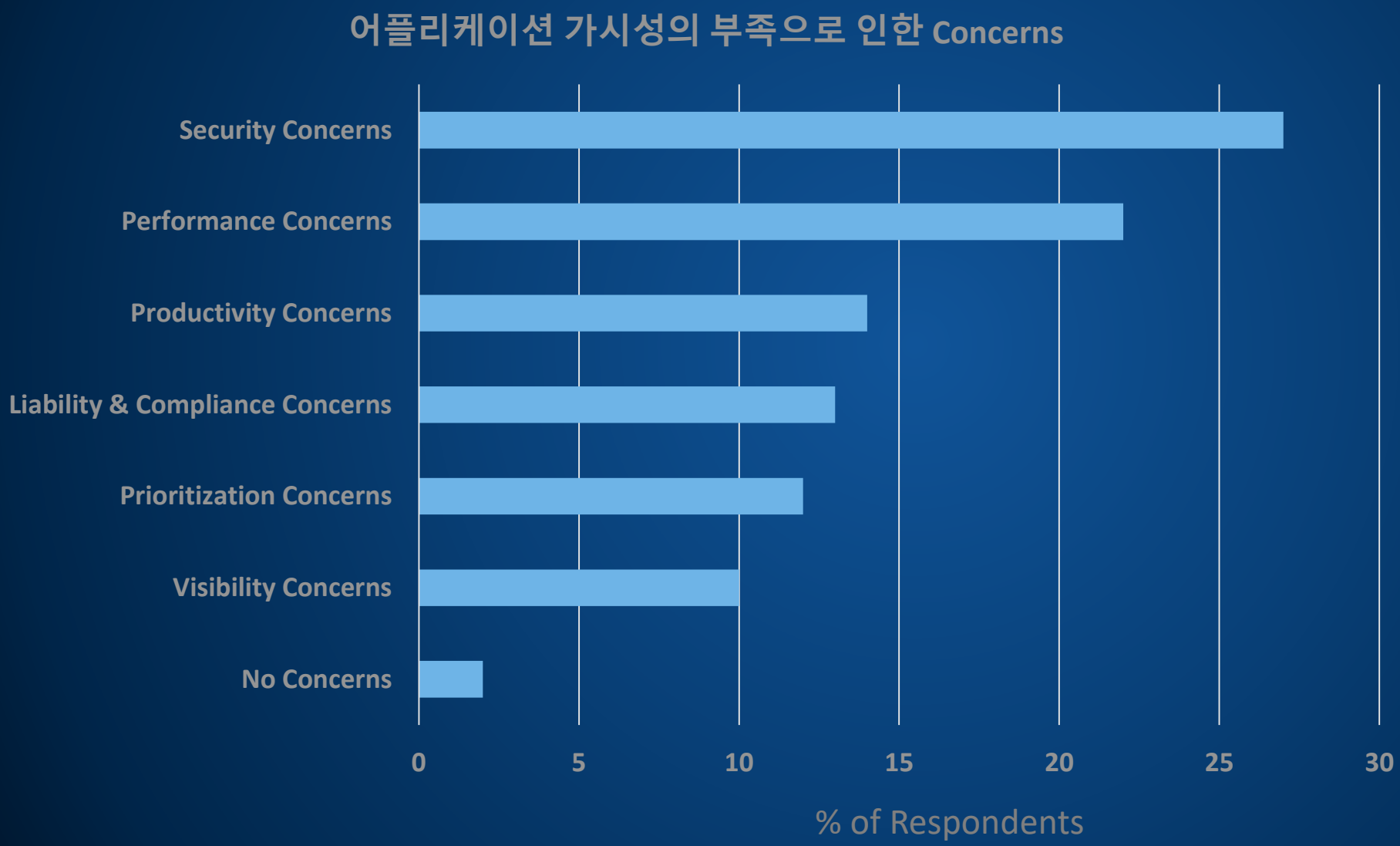
가 인식되지 않음

80%

의 트래픽을
방화벽의 ¼이
분류하지 못함

SOPHOS

Top Concerns



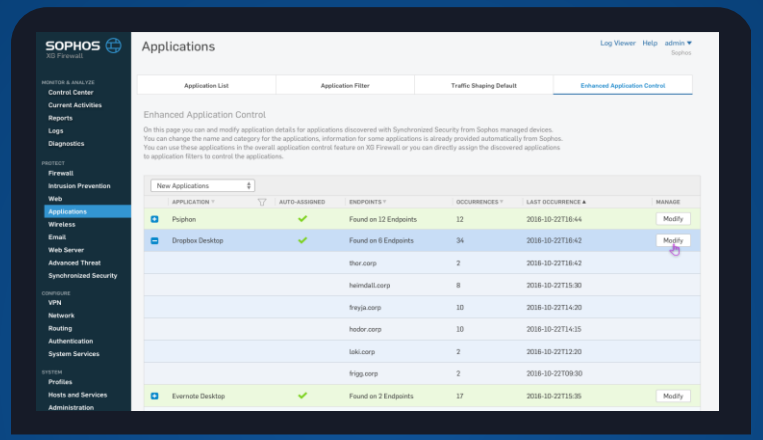
99%
의 관리자가 동의

54%
의 관리자는 염려중

SOPHOS

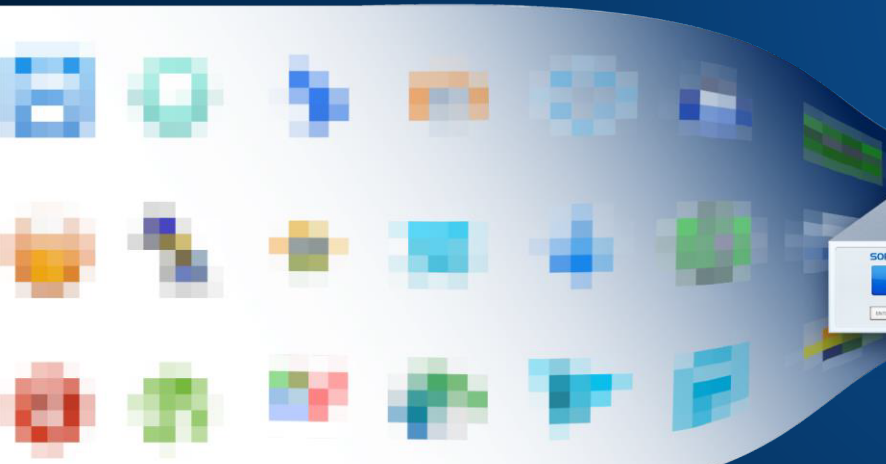
Retake control of your network

Synchronized Application Control



What Firewalls See Today

What Synchronized App Control Sees



오늘날의 어플리케이션 제어문제를 해결할 솔루션

100%
어플리케이션 식별 및 제어

1 **알려지지 않은 어플리케이션**
XG Firewall sees app traffic that does not match a signature

2 **엔드포인트는 APP정보를 공유**
os Endpoint passes app name, path and even category to XG Firewall for classification

3 **어플리케이션은 재분류 및 제어 가능**
Automatically categorize and control where possible or admin can manually set category or policy to apply.

소포스는 이 레벨의 가시성을 제공하는 유일한 벤더

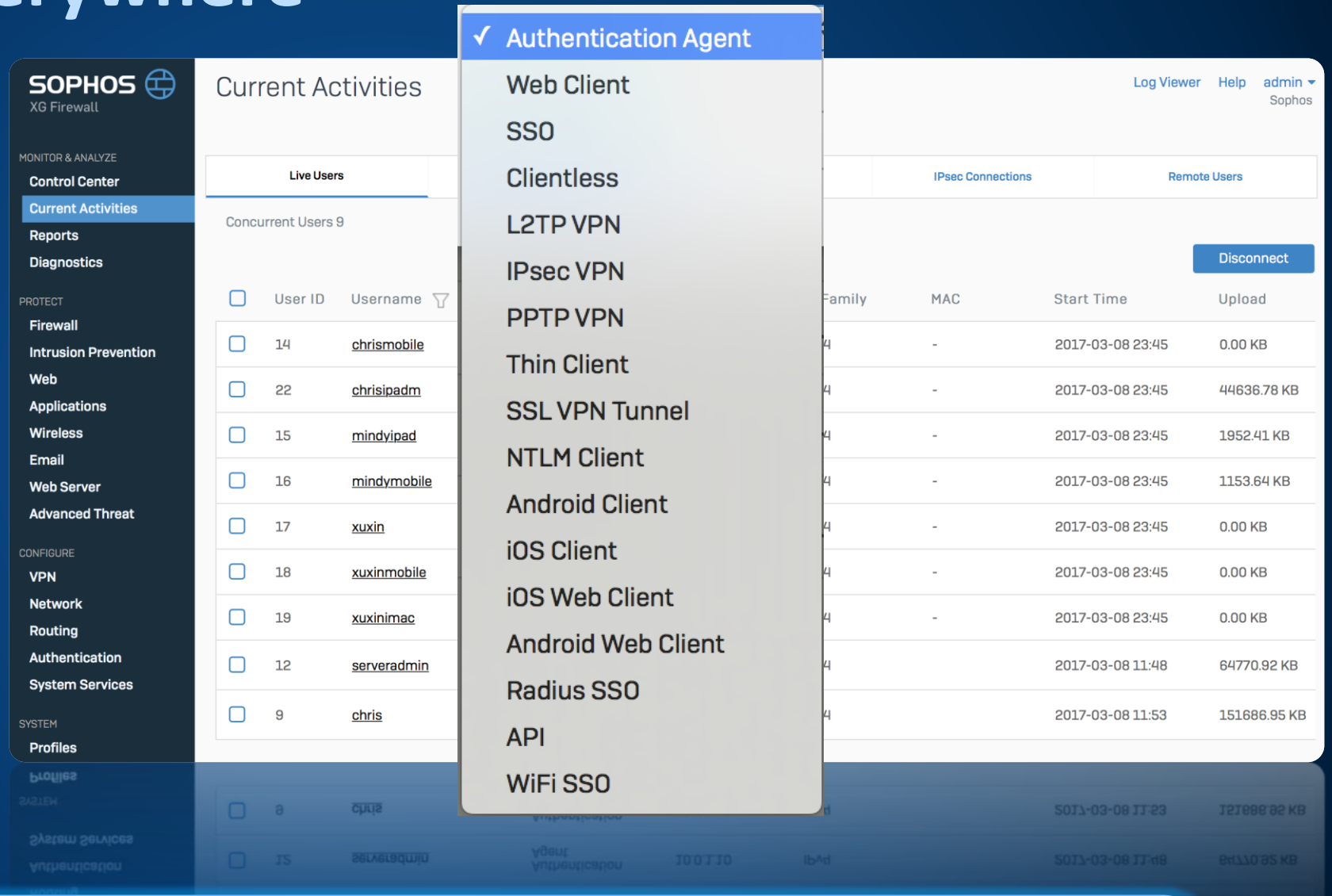
SOPHOS

사용자 식별- Everywhere

XG Firewall 사용자 식별

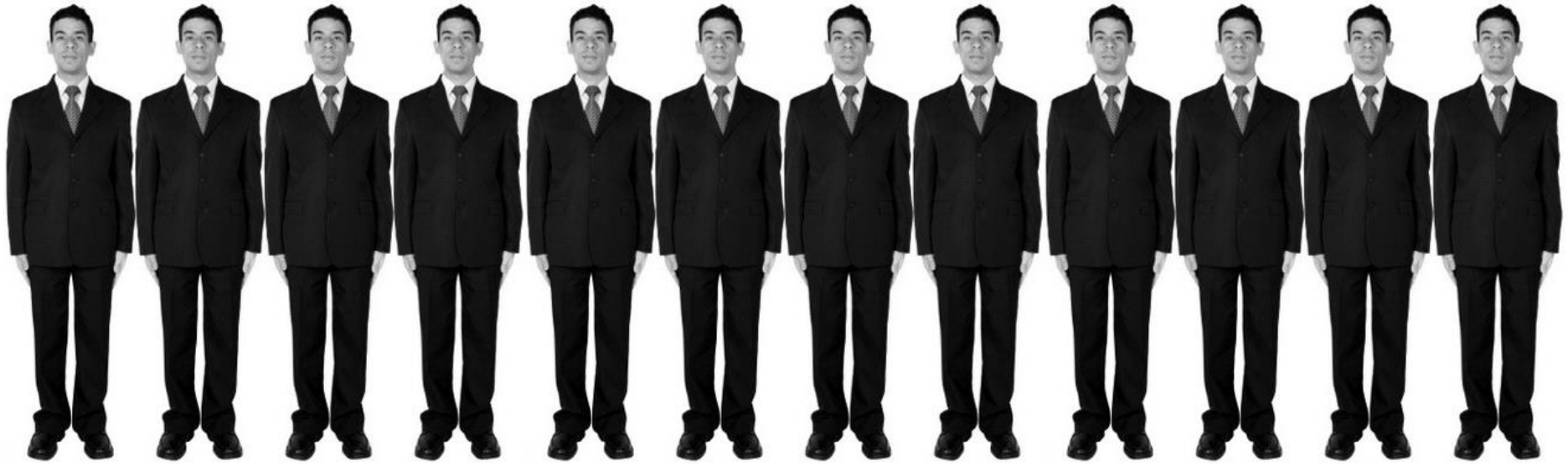
- 사용자 식별과 인증에 최고의 유연성
- 하나의 룰에서 하나의 화면을 통해 모든 사용자정책을 관리

모든 유형의 네트워크에 적합한 사용자 식별



Sophos is the only vendor to offer this level of user auth flexibility

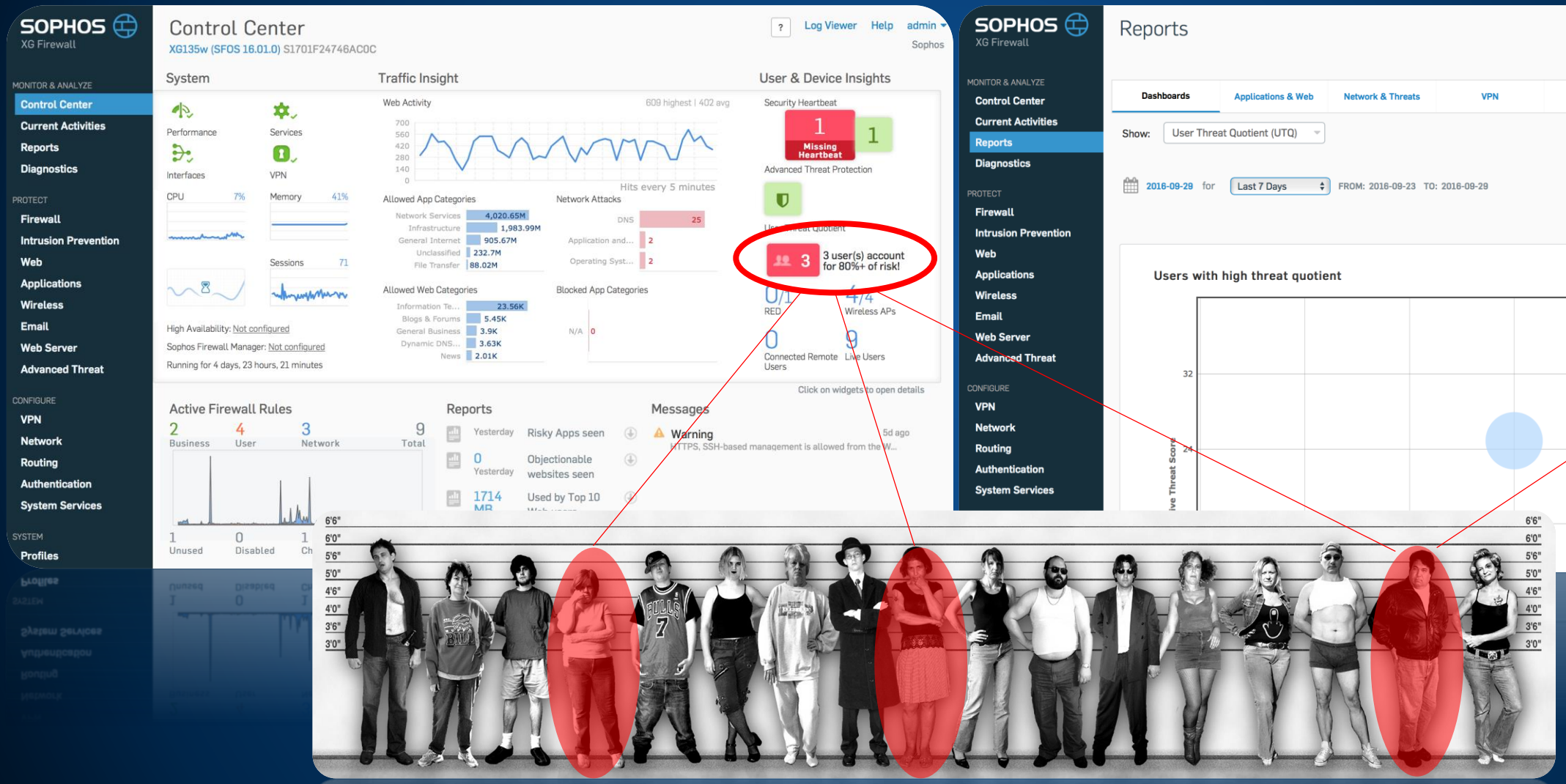
현재 방화벽들은 사용자를 다음처럼 식별



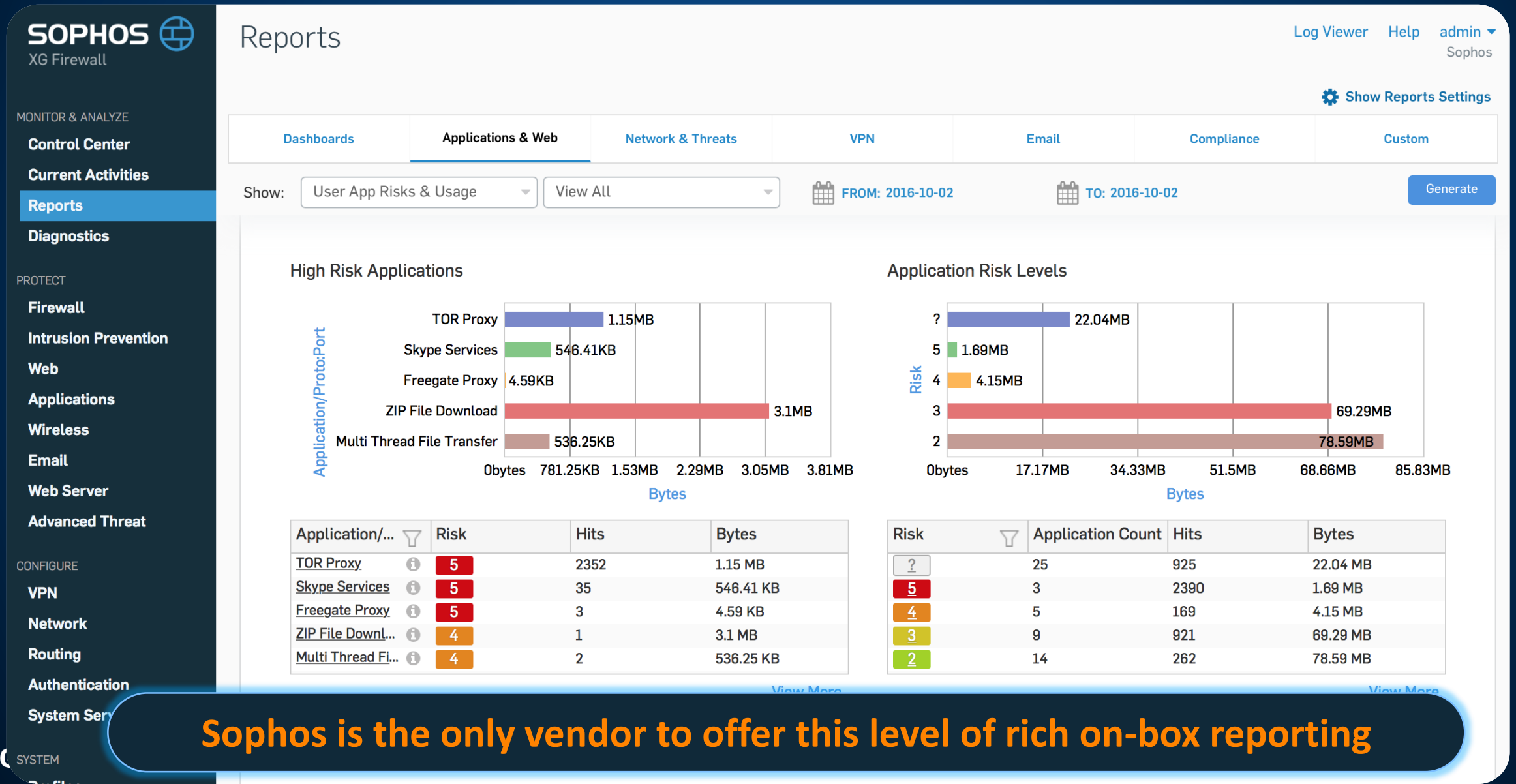
실제로는, 사용자는 이것보다도 다양합니다.

문제가 발생되기전 위험을 식별

You can take action before HR needs to



수백개의 내장 리포팅



Sophos is the only vendor to offer this level of rich on-box reporting

2. Block Unknown Threats

2. 알려지지 않은 위협 방어

SOPHOS


Most Firewalls make you feel about as safe as…

최신 위협 트렌트

Office File Exploits

최신 Office Doc Exploit은
일반적인 Word 경고
메시지없이 작동합니다.

Crypto Currency Mining

Bots 과 심지어 웹사이트들도
가상화폐 마이닝작업으로
와해되는 중입니다.

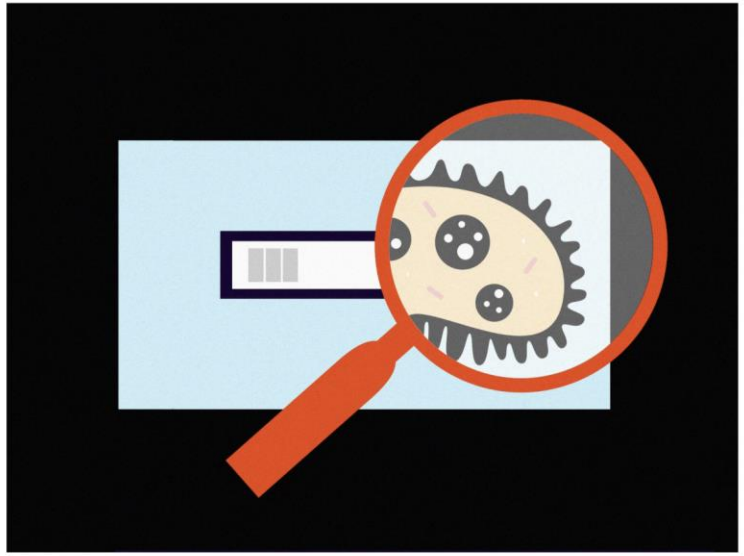
Remote Access Trojans

스팸과 오피스 문서로 전달되며,
네트워크를 걸쳐 전파됩니다.
아웃룩 데이터나 개인정보를
가로채 계좌에 접근하기위한
페이로드를 전달합니다.

Ransomware in Software Updates

ANDY GREENBERG SECURITY 07.07.17 10:00 AM

THE PETYA PLAGUE EXPOSES THE THREAT OF EVIL SOFTWARE UPDATES



GETTY IMAGES/WIRED

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

New Mac Malware Found Hiding In A Fake Adobe Flash Update

Lee Mathews, CONTRIBUTOR
Observing, pondering, and writing about tech. Generally in that order.
FULL BIO

Opinions expressed by Forbes Contributors are their own.

Suppose you're surfing and suddenly you see a notification that software on your computer needs to be patched. Sounds urgent, right? You don't want to be wandering the Web with outdated software, and you mi
through the update process w

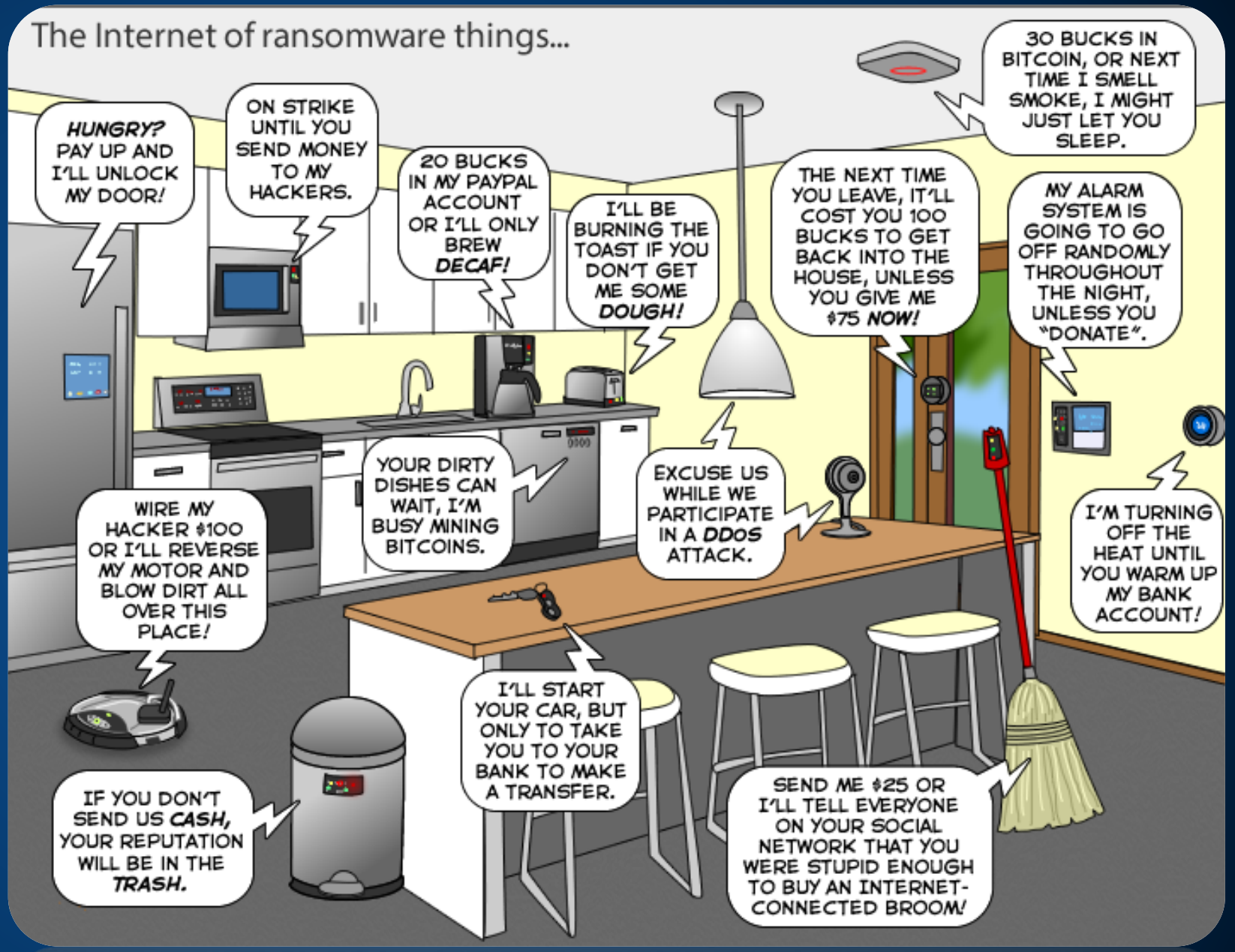
HandBrake Download Mirror Compromised With Mac Malware

By Ryan Whitwam on May 10, 2017 at 10:30 am | 2 Comments

56 shares

SOPHOS

What's Next?
IoT Ransomware?



Data Science + 소포스 랩=
자신있는 적극적인, 공격적인 탐지

DATA SCIENCE + LABS:
시스템 정확도와 예측력을 개선을 위해 피드백을 지속적으로 통합

DATA SCIENCE: 사이버보안의 난제를 해결하기 위해 가장 효율적인 알고리즘을 생성

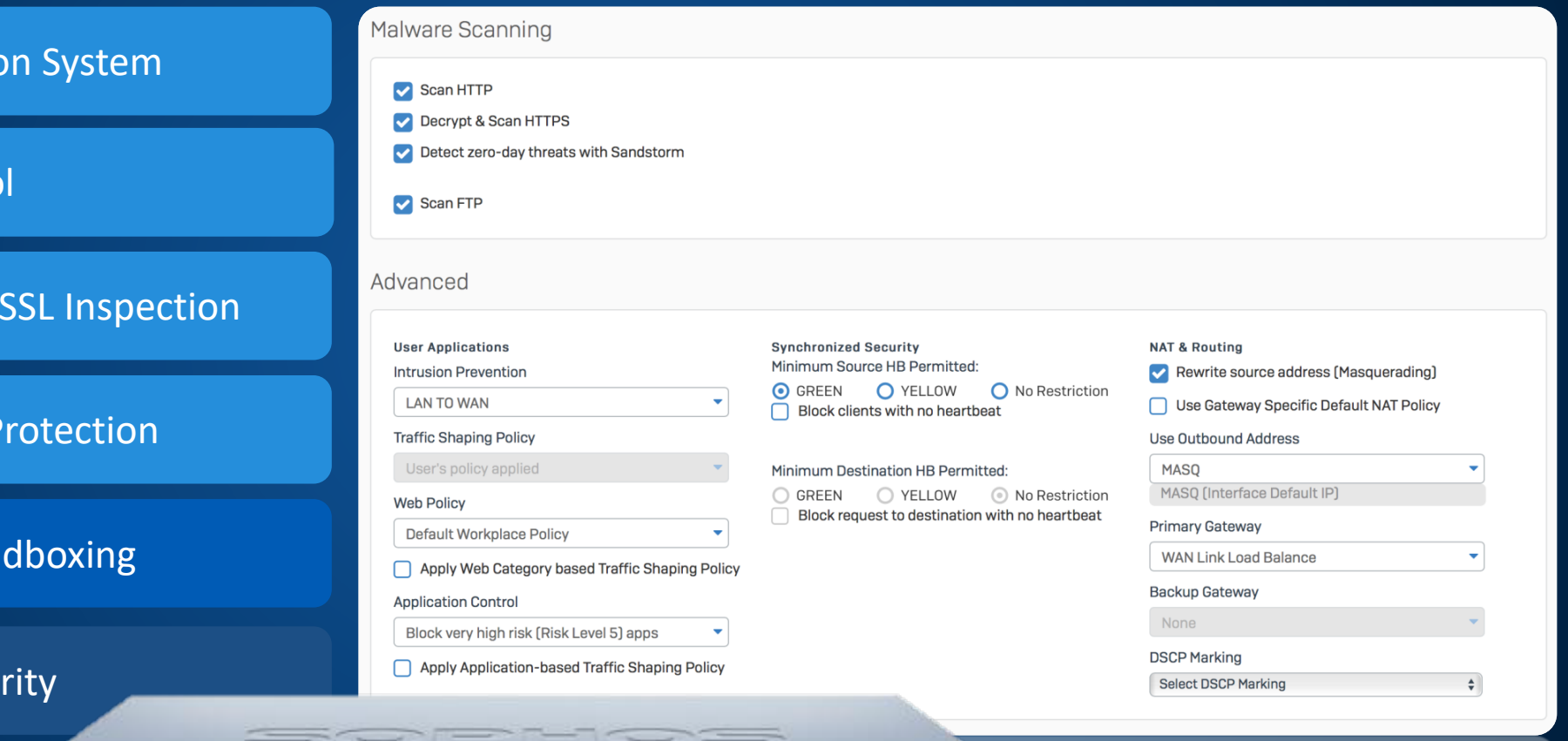
LABS: 최선의 예측을 위한 수억개의 샘플을 제공

LABS: Labeling 정밀도를 보장하기 위한 Lab시스템과 프로세스의 활용

알려지지 않은 위협 차단

A full suite of technologies easily managed from a single screen

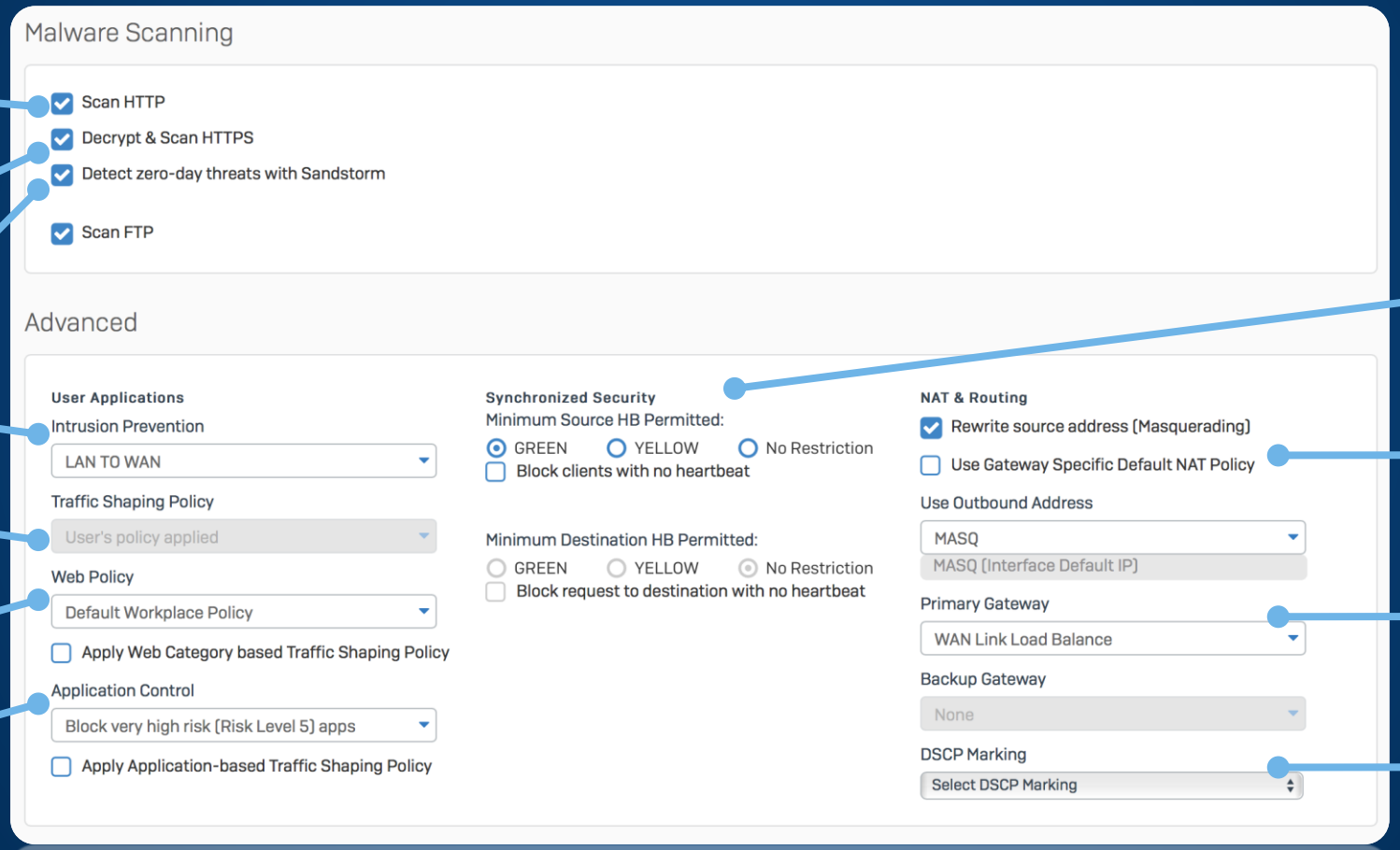
- Intrusion Prevention System
- Application Control
- Web Protection & SSL Inspection
- Advanced Threat Protection
- Deep Learning Sandboxing
- Synchronized Security



SOPHOS

간결하고 강력한 XG Firewall의 하나의 룰 설정

A full suite of technologies easily managed from a single screen



Dual AV

SSL Inspection

Sandboxing

IPS

QoS

Web Filtering

App Control

Heartbeat

NAT

Routing

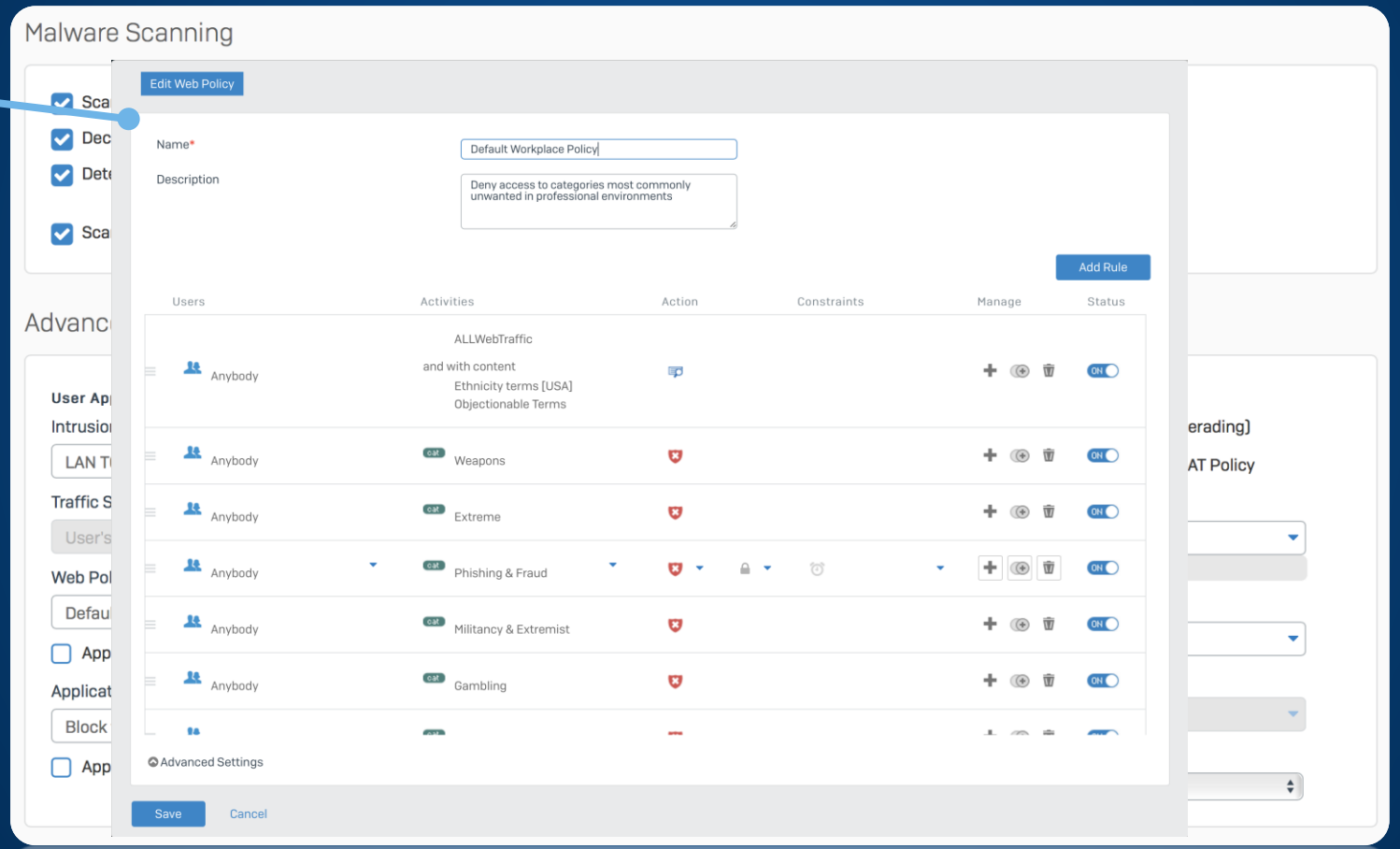
Prioritization

SOPHOS

간결하고 강력한 XG Firewall의 하나의 룰 설정

IPS, Web, App Control and Traffic-Shaping and Edit-in-place을 위한 스냅인 정책

Edit-in-place



Sophos is the only vendor providing this level of integration

SOPHOS

Sandstorm Deep Threat Prevention

zero day 위협으로 부터 가장 안전하게

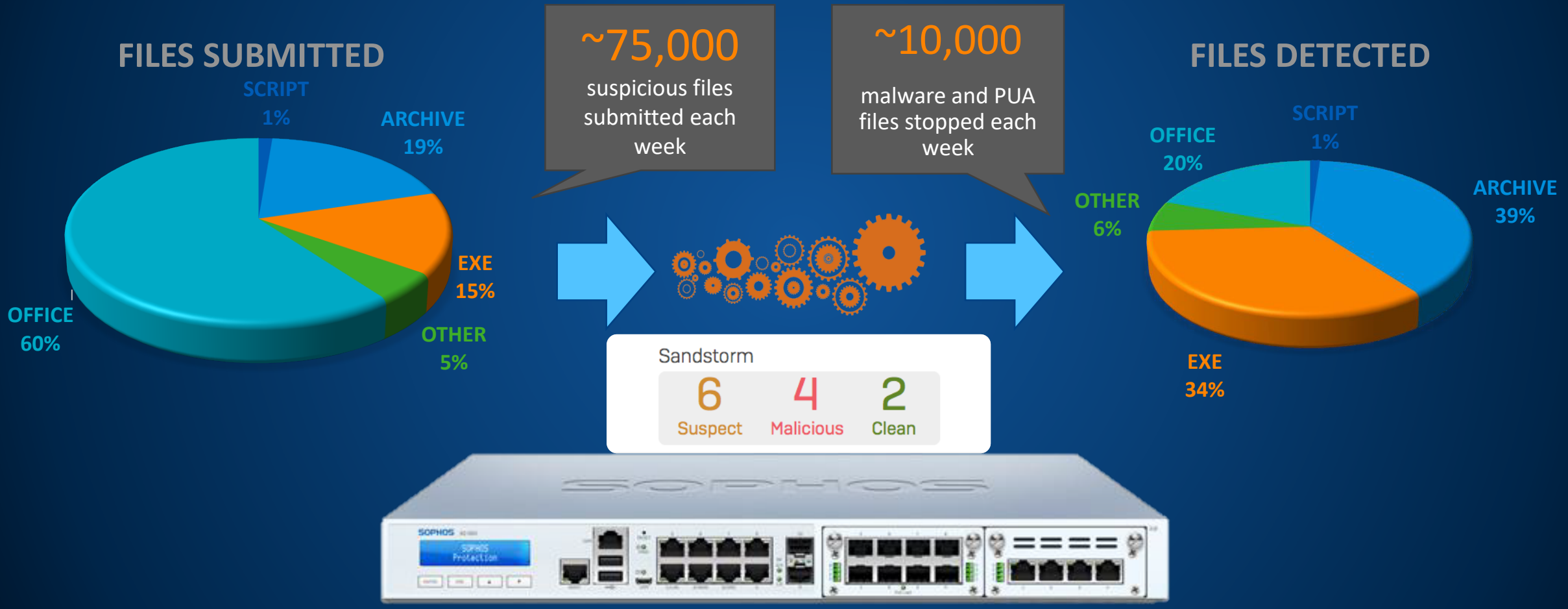
Deep Memory Analysis		Deep Behavioural Analysis		Deep Network Analysis		Deep Learning Analysis	
초기 및 실행 이후 메모리 감지 및 분석	적극적이고 빈번한 런타임 분석	Sandbox 회피 기술, API & File 시스템 동작	Intercept X 취약점 공격 탐지와 크립토가드 엔진	모든 포트와 프로토콜을 분석	IPS detections 추가예정	보내진 모든 실행파일들 분석	지속적 적응 학습 모델

Sophos Labs의 실시간 위협 인텔리전스

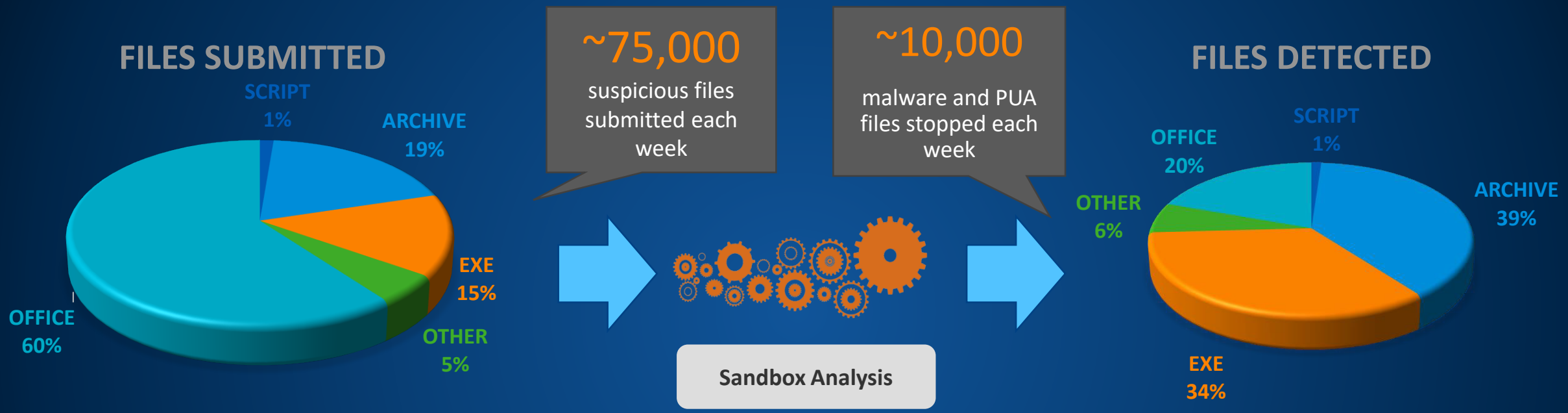
Sandstorm의 보호력은 엔드포인트와 방화벽을 뛰어넘습니다

SOPHOS

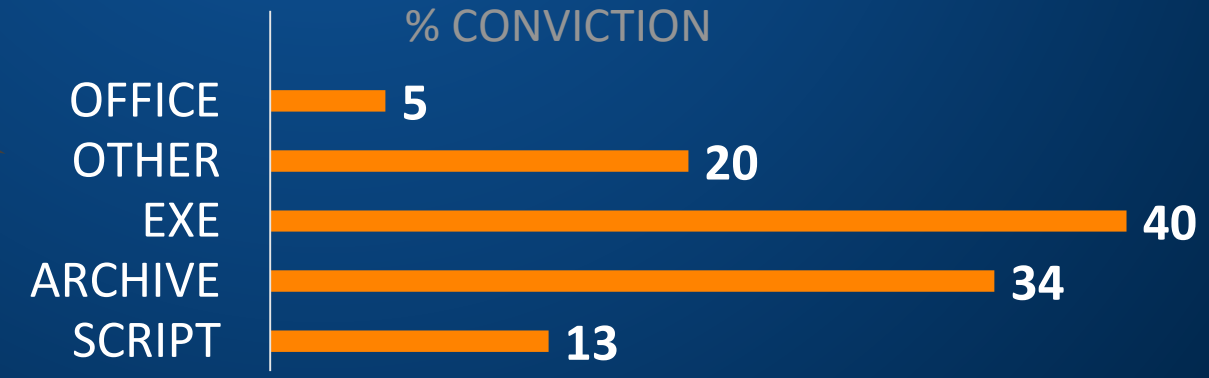
이전 보다 더 높아진 보호 – Powered by Deep Learning



파일 유형 분류



파일 타입별 멀웨어 호근 PUA로 식별되고 차단된 제출된 파일 비율



행위적인 탐지 + 딥러닝 (Deep learning)

Stops **10%** more of EXE malware

알려진 악의 적인 행위로 부터 위협을 탐지

File Submission
- Detect suspicious files
- Pick execution environment

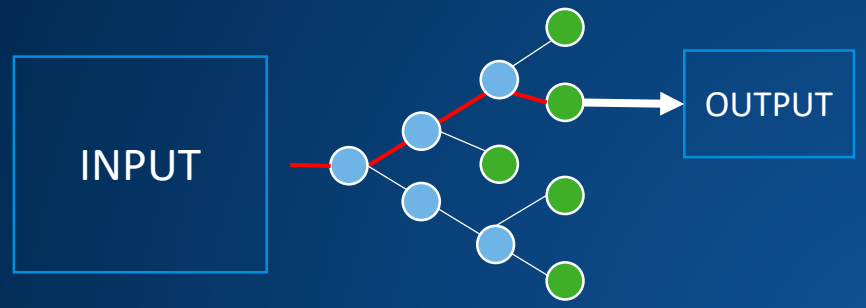
Attack Replay
- Event logging
- Payload추출
- Anti-evasion

Behavior Analysis
- Rules
- Patterns
- Event 상관관계

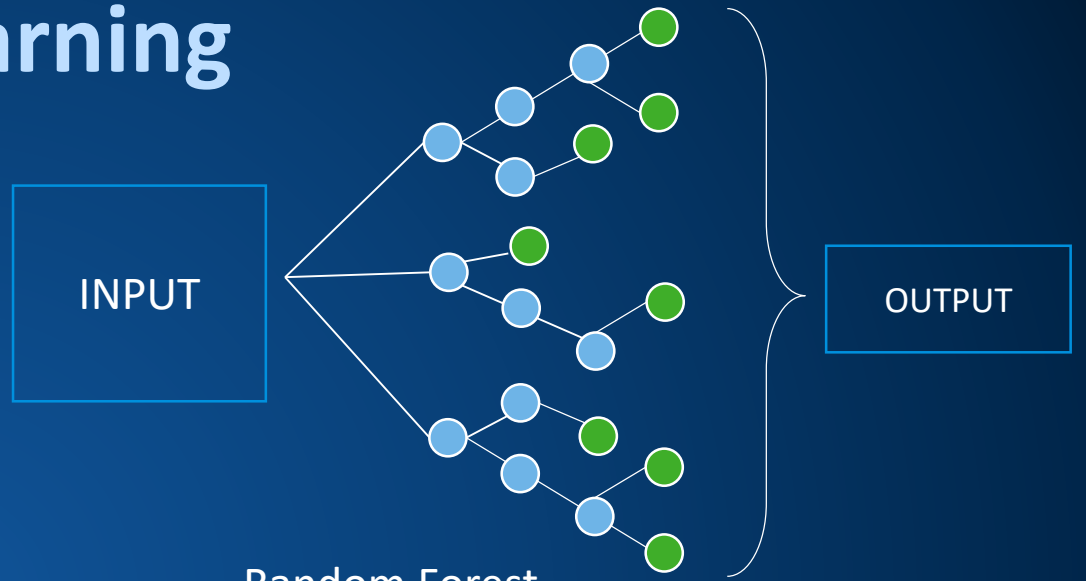
Deep Learning
- Detect unknown executable threats

Machine learning Vs. deep learning

MACHINE LEARNING

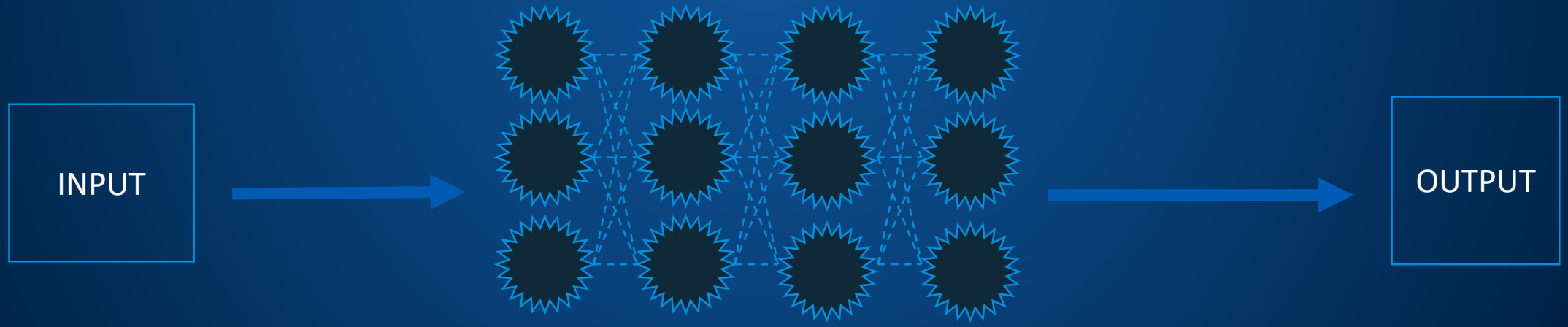


Decision Tree



Random Forest

DEEP LEARNING



Interconnected Layers of Neurons, Each Identifying More Complex Features

SOPHOS

Sophos deep learning advantages

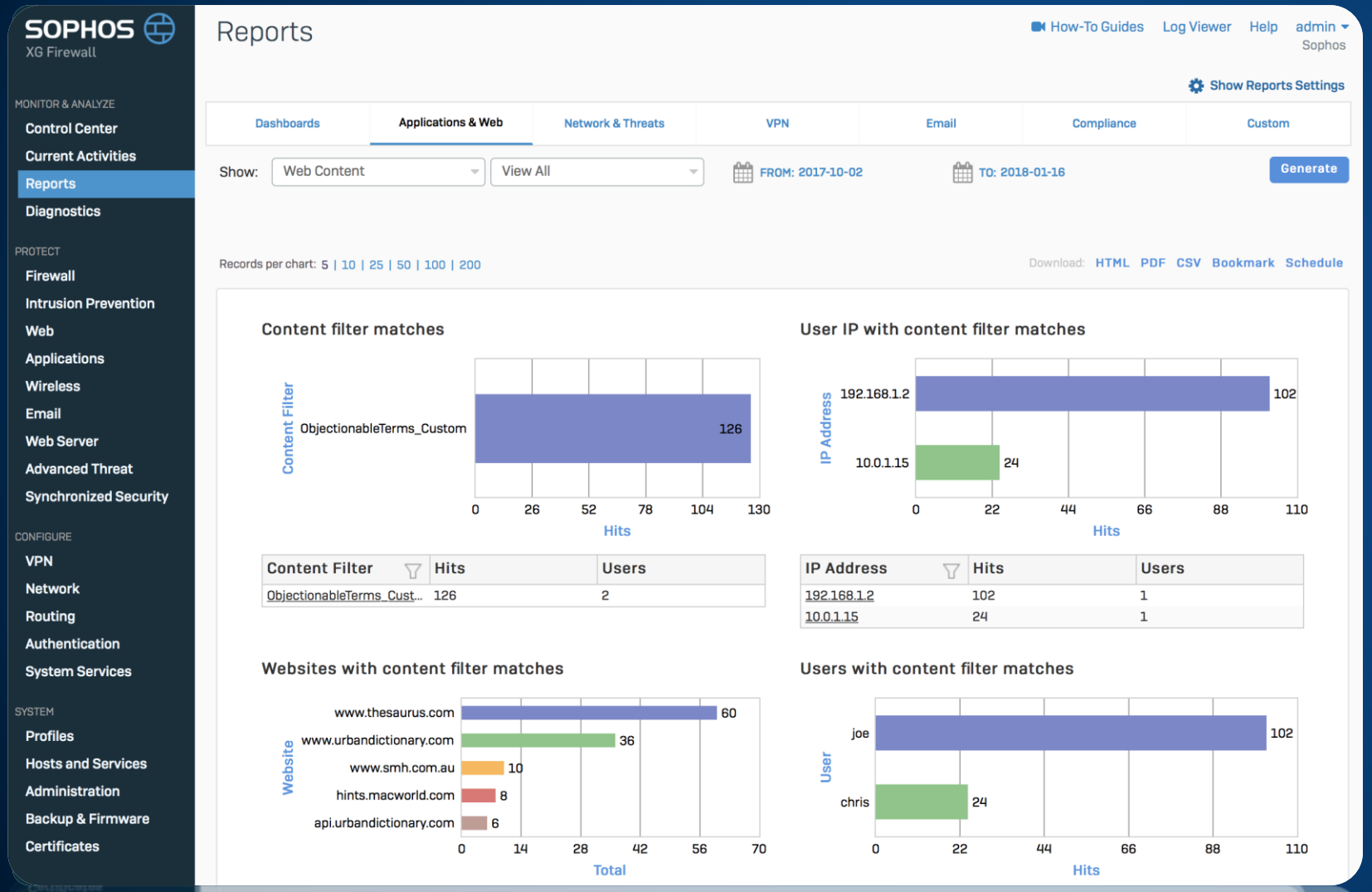
- 증명된
  - 업계 #1위의 멀웨어 탐지율
  - Validated on VirusTotal since August 2016, 3rd party validated
- 성능
  - 시그니쳐없이 알려지지 않은 위협의 차단
  - 20millisecond(0.02초) 이내에 위협의 탑지 및 차단
- 경험
  - In development since 2010
  - DARPA가 주도한 기술로서, 소포스 랩의 Data scientists에 의해 생성
- 소포스랩: 수억개의 샘플을 트레이닝

> “One of the ***best performance scores*** we have ever seen in our tests”
>
> *Maik Morgenstern, CTO, AV-TEST*

VIRUS TOTAL NSS LABS AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS

Web Content Filtering (v17)

Enabling child safety in education

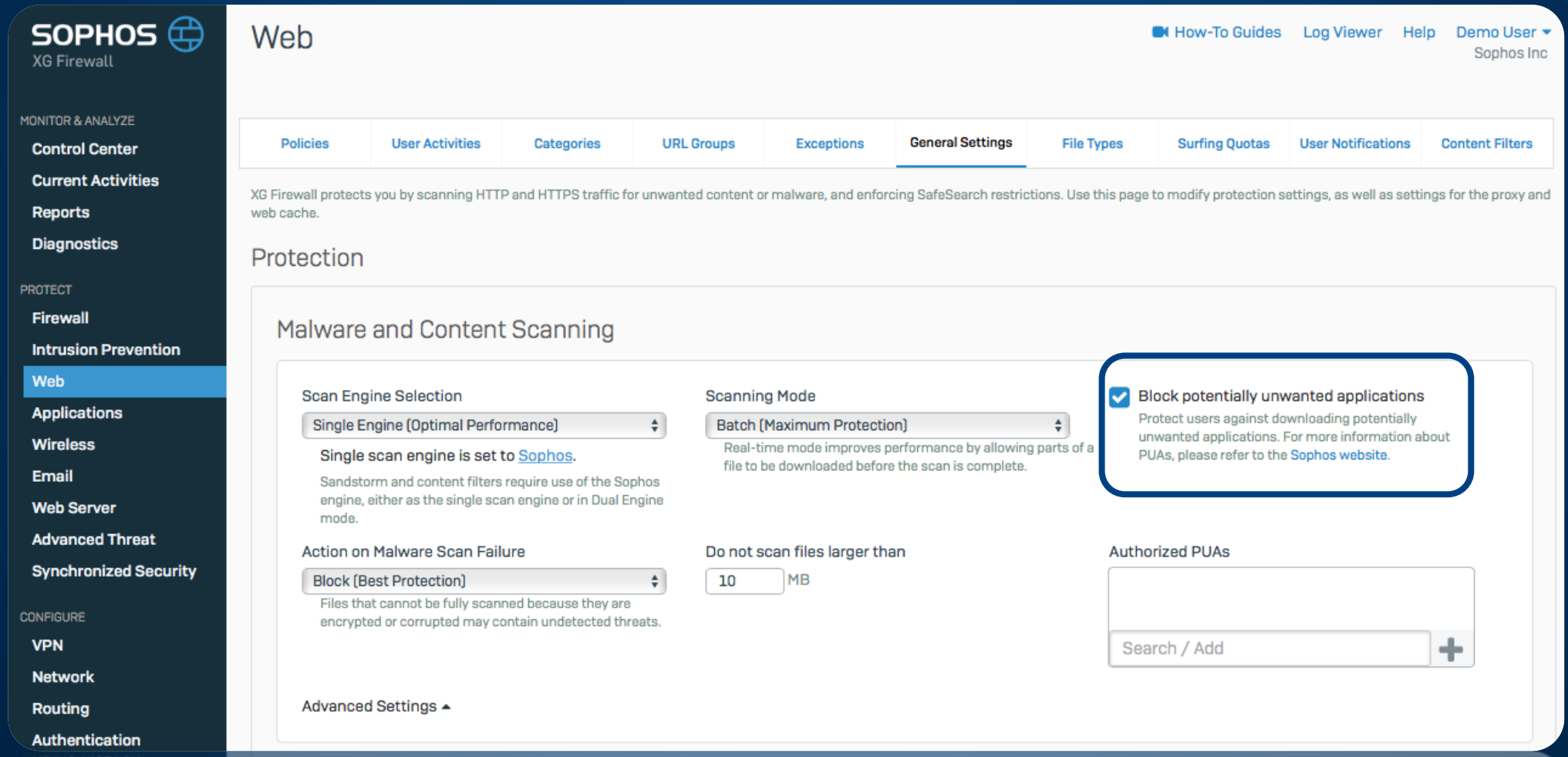


동적 컨텐츠 모니터링과 필터링

- 괴롭힘, 극단주의 테러리즘, 학대, 자해등을 문제가 되기 전에 빠르게 인식합니다.
- 카테고리에 무관, 컨텐츠를 기반으로 웹사이트를 동적으로 차단합니다.

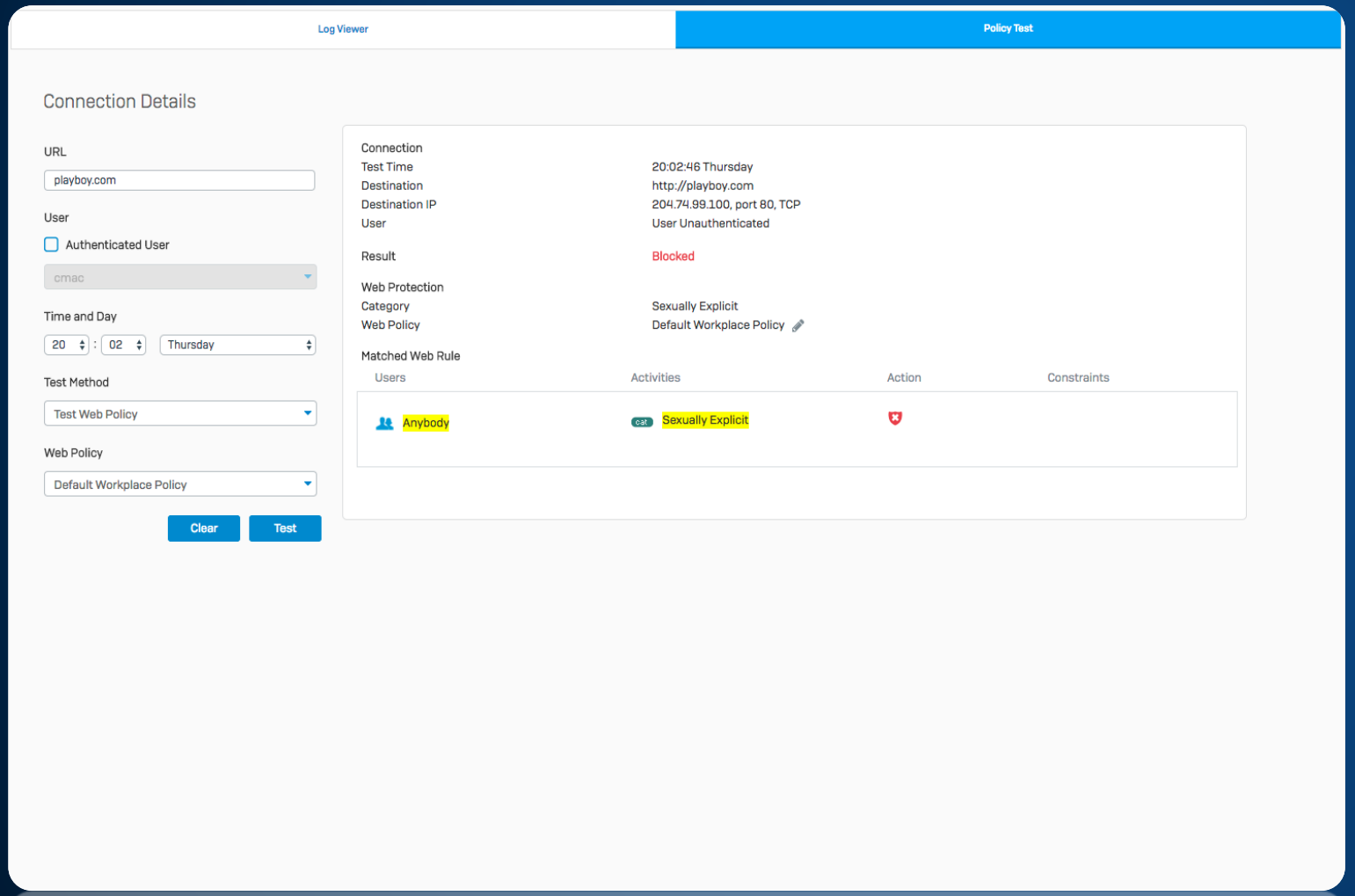
JavaScript CryptoJacking 보호

단지 한번의 클릭으로



Policy Test Simulator

Making troubleshooting quicker and easier



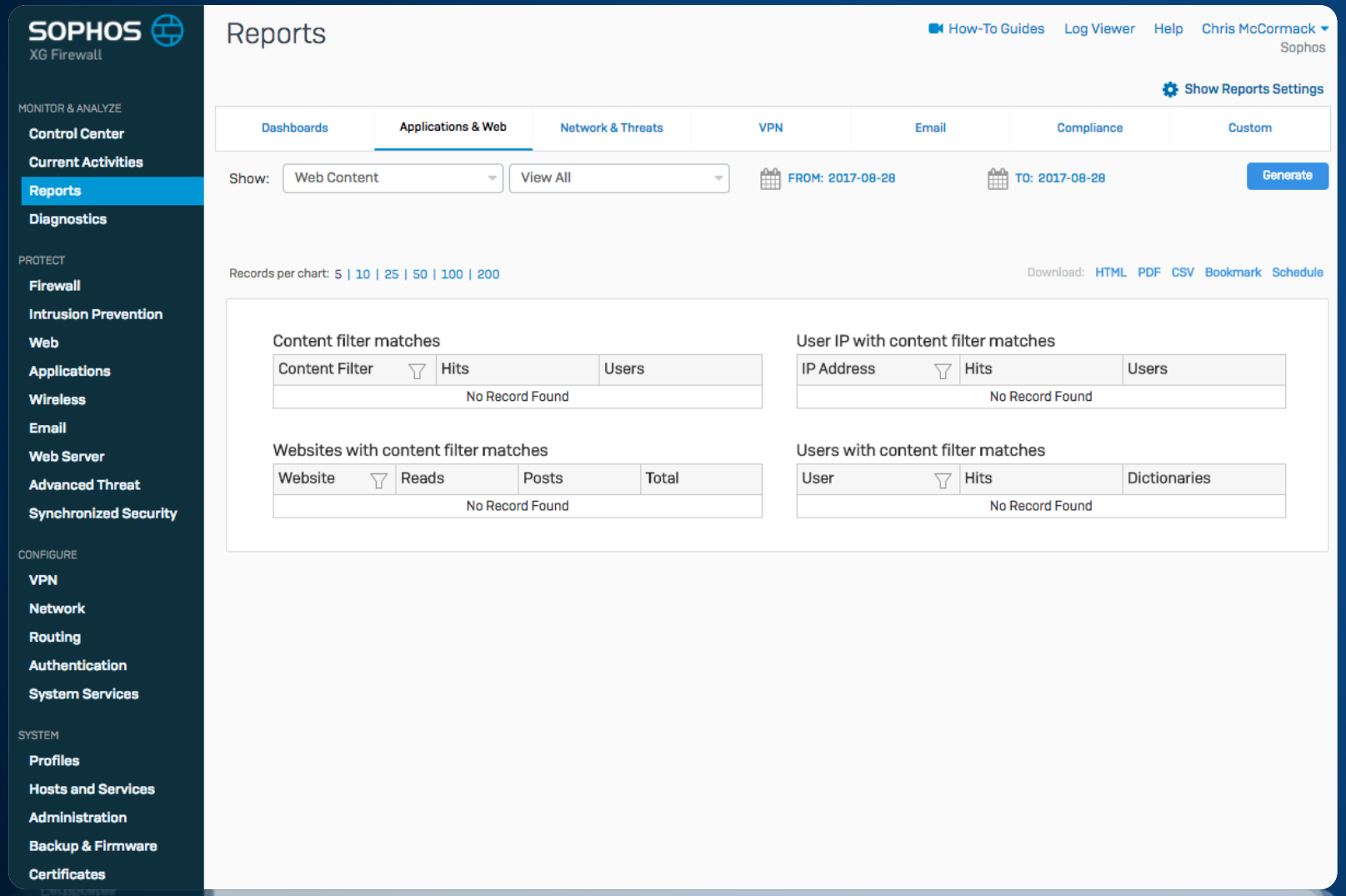
Policy Test Simulator

- Simulate web policy or firewall rules quickly and easily
- Test a variety of protocols or any website
- Test web policy, firewall rules, or both
- User, Date, Time Criteria
- Full report on what's allowed/blocked and what rule or policy is matched

SOPHOS

Web Keyword Monitoring

Enabling child safety in education (and identifying bad behaviour in general)



Dynamic Content Blocking

- Keyword lists can be added and then applied to web polices
- Websites are scanned for matching keyword content
- Log or Block action when a match occurs
- Report shows users and websites matching keyword content

Benefits

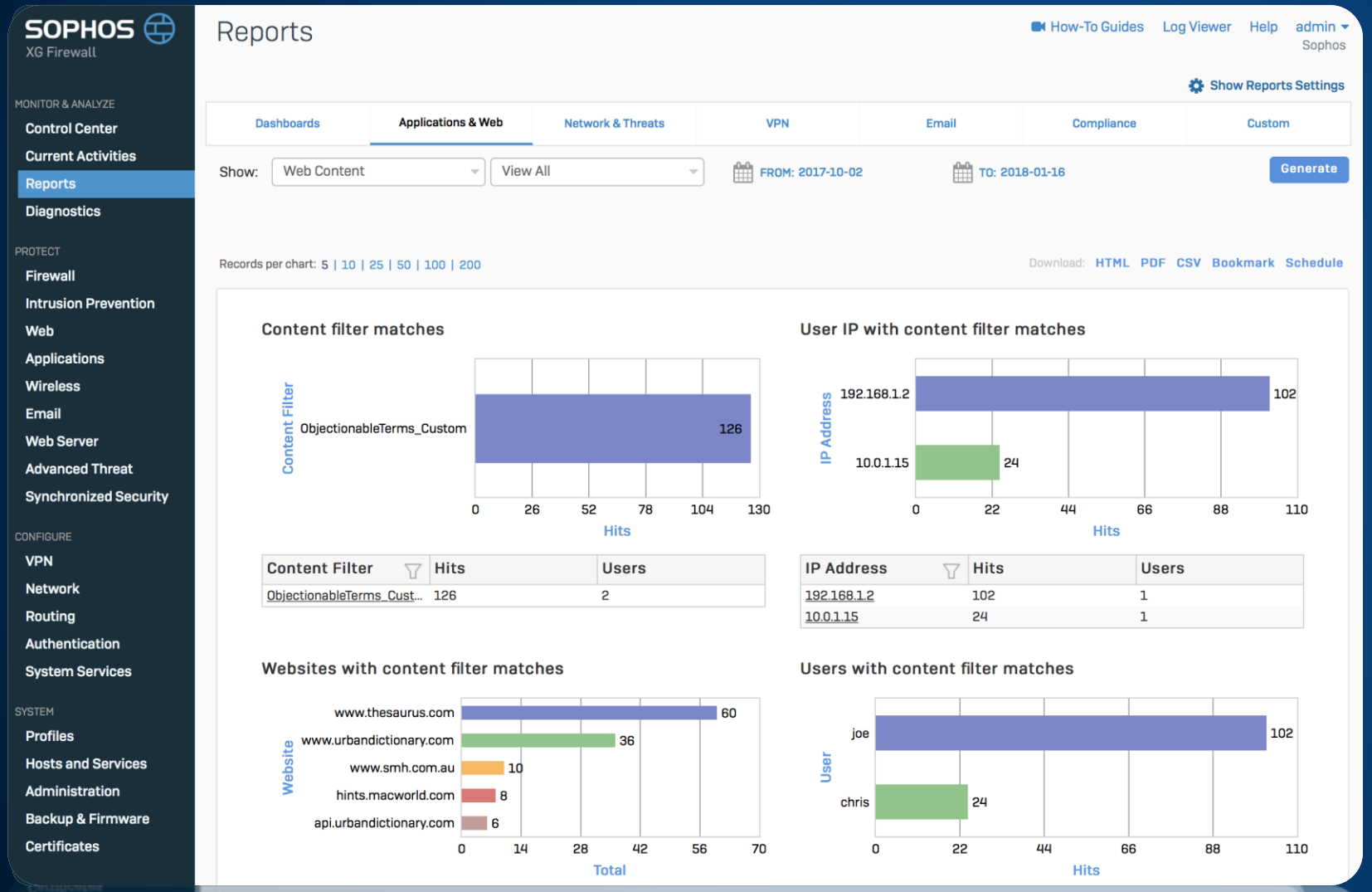
- Quickly identify signs of bullying, radicalization, abuse or self-harm before they become a problem
- A key requirement for the UK Education market
- Dynamically block websites based on content regardless of their category – block sites that otherwise might be allowed

Note

- Initial keywords included may be limited – may need to rely on 3rd party sources

Web Keyword 모니터링

직장내, 학교내 안전한 웹사용 및 사전 확인



Dynamic Content Blocking

- 원하는 키워드 리스트를 생성 후 웹 정책에 적용할 수 있습니다.
- 웹사이트는 해당 키워드가 사용되는지 스캔됩니다.
- 동일한 내용이 확인되면, 로그를 남기거나 차단합니다.
- Report는 키워드가 매칭된 사용자와 웹사이트를 보여줍니다.

Benefits –사용 이점

- 괴롭힘, 자해, 학대, 과격화등 다양한 사내문제가 발생되기 전에 먼저 내용을 파악할수 있습니다.
- 교육 마켓에서 필수 요구사항이며, 직장내에서도 불필요한 정보에 대한 필터링이 가능합니다.
- 카테고리와 관계없이 컨텐츠 기반으로 웹사이트를 차단할 수 있습니다.

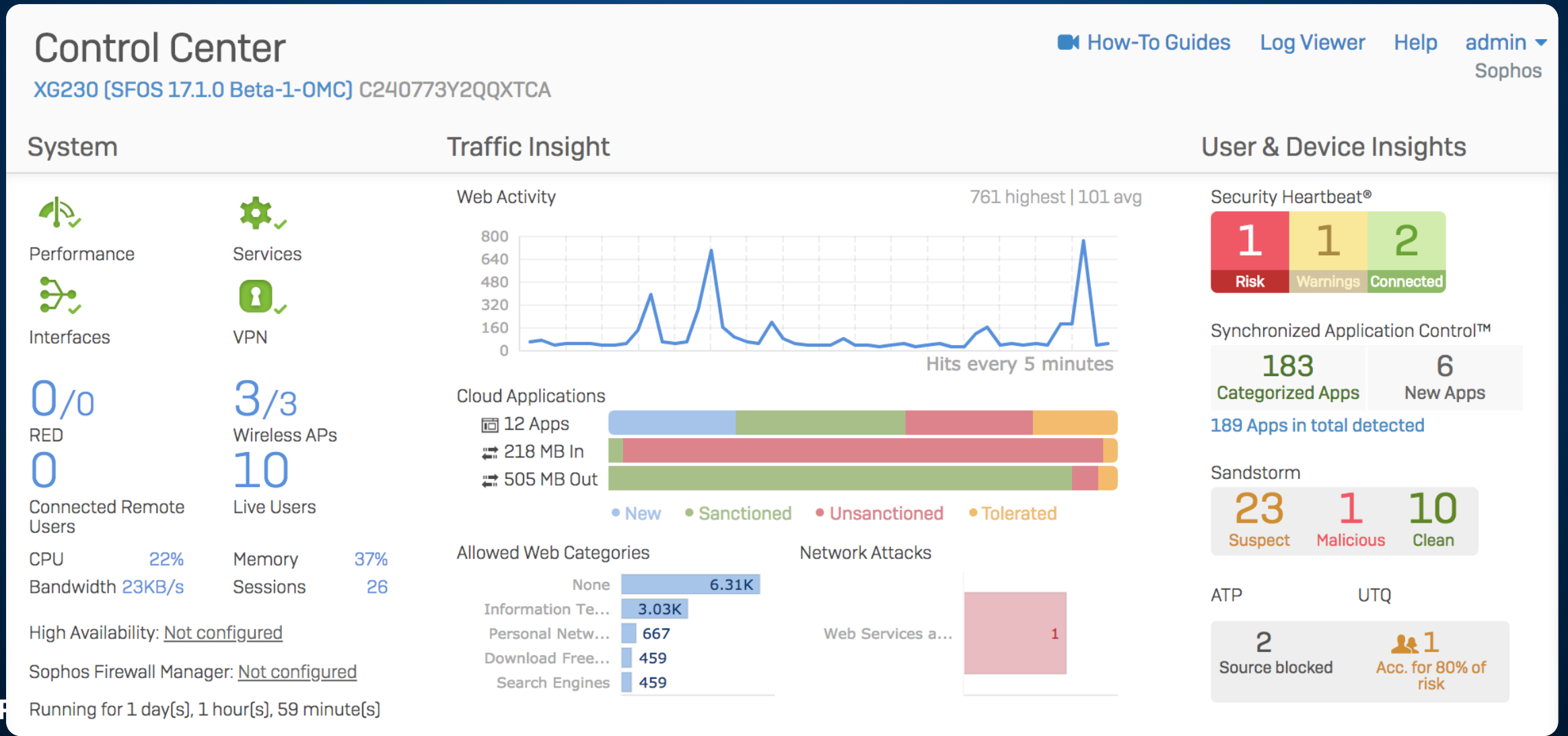
3. Automatically Respond to Incidents

3. 자동화된 사고 대응

SOPHOS

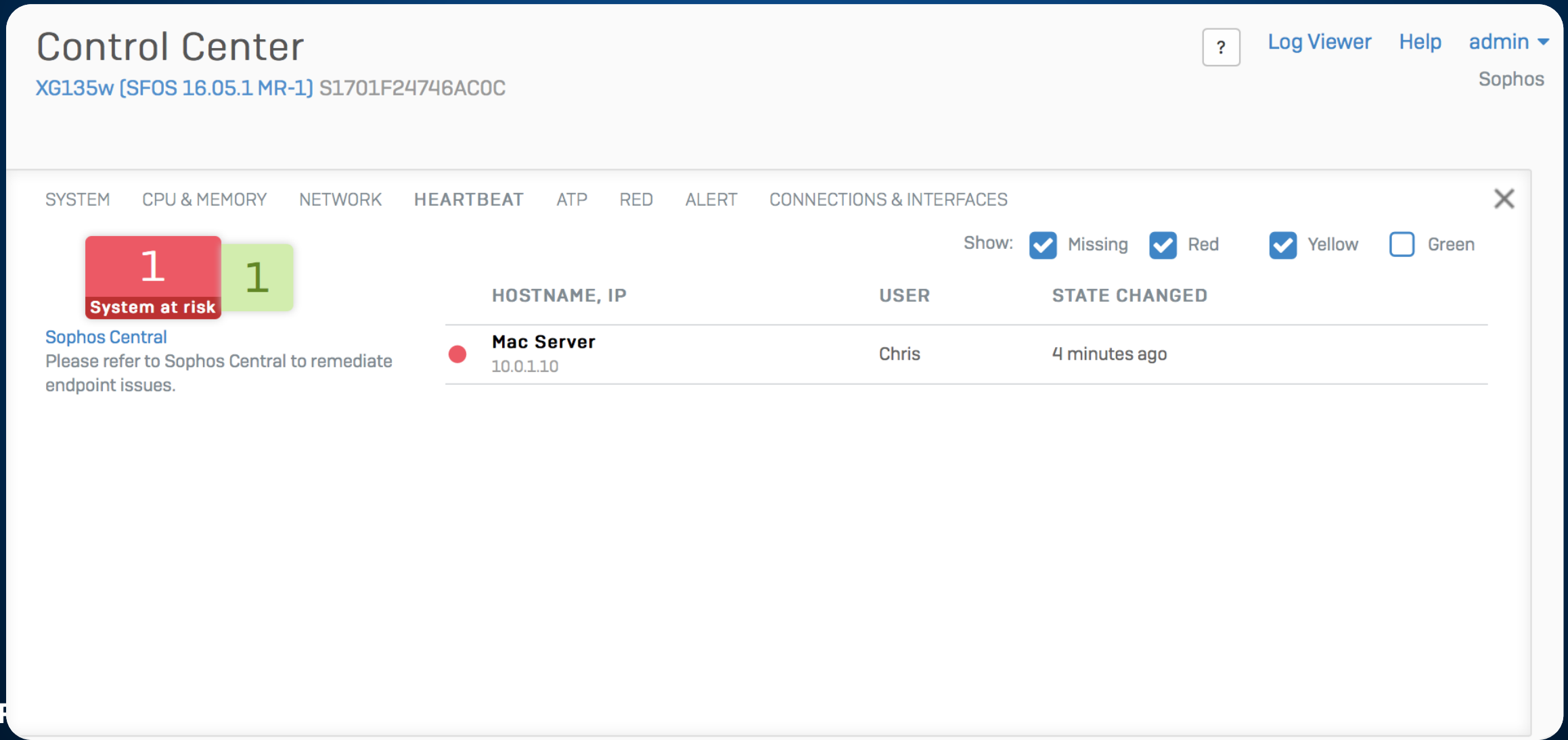
Synchronized Security – 즉각적인 위협의 식별

장치 및 사용자를 향하는 위협을 즉시 확인



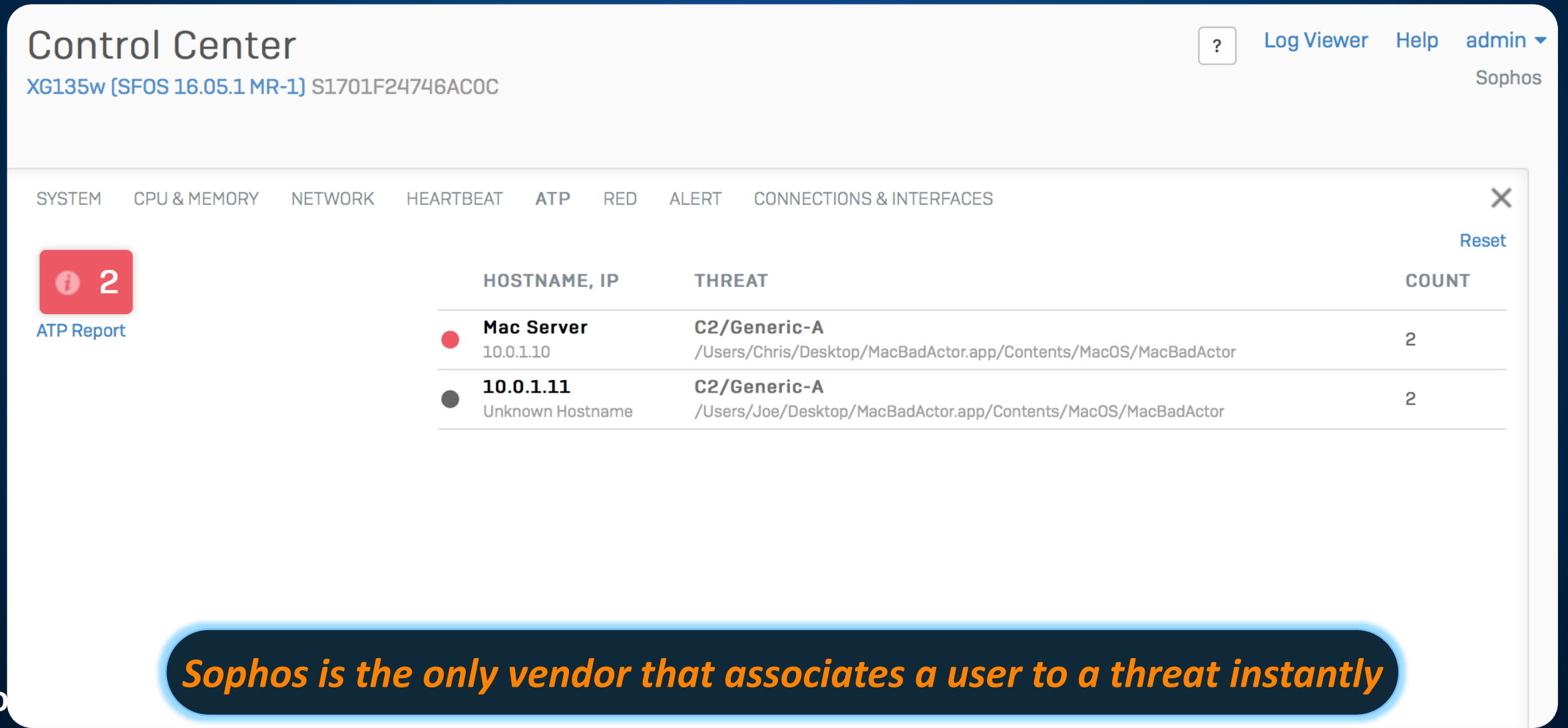
Synchronized Security – 즉각적인 위협의 식별

Associating threats to a device and a user immediately



Synchronized Security - 즉각적인 위협의 식별

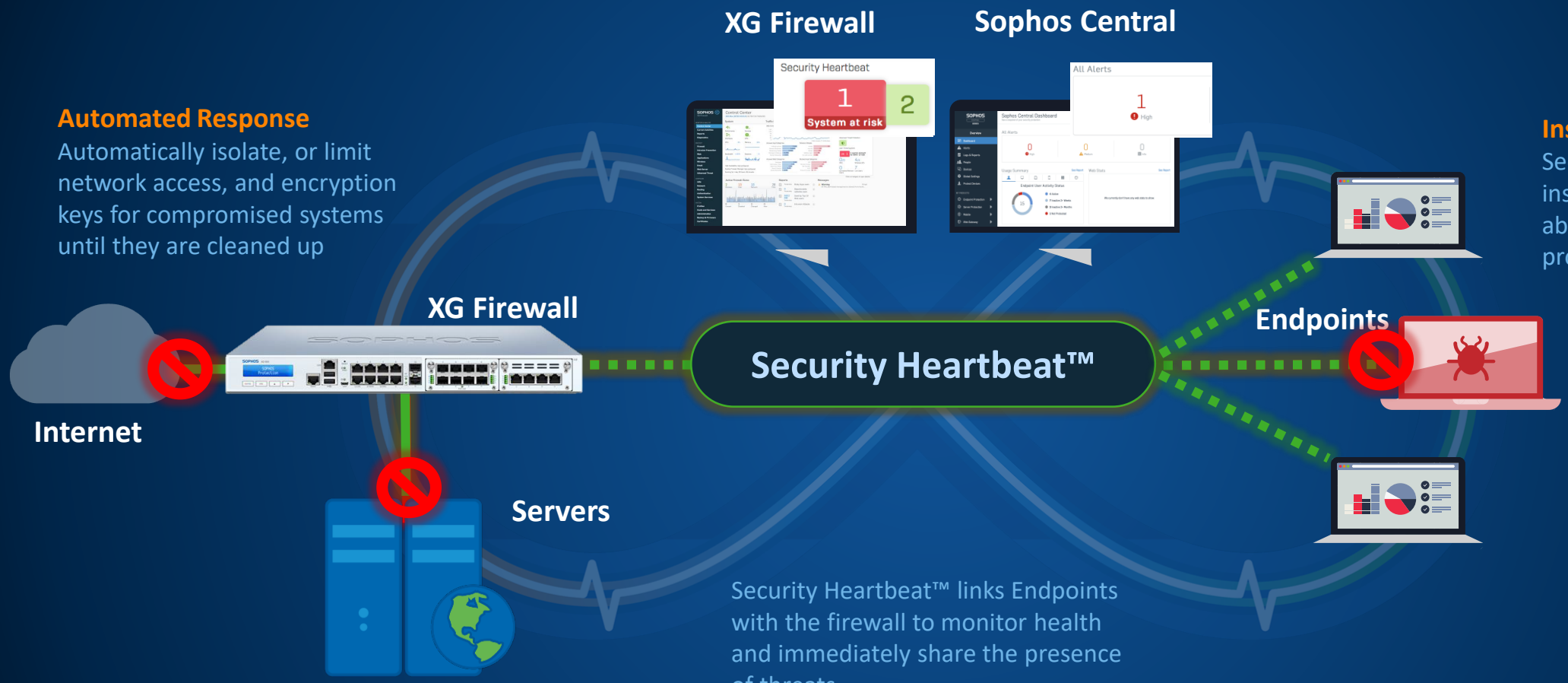
Associating threats to a device and a user immediately



Sophos is the only vendor that associates a user to a threat instantly

Synchronized Security – 자동화 된 대응

Automated Response
Automatically isolate, or limit network access, and encryption keys for compromised systems until they are cleaned up



Instant Identification
Security Heartbeat can instantly share telemetry about the user, systems and process responsible

Security Heartbeat™ links Endpoints with the firewall to monitor health and immediately share the presence of threats.

소포스는 이러한 대응을 제공하는 유일한 벤더

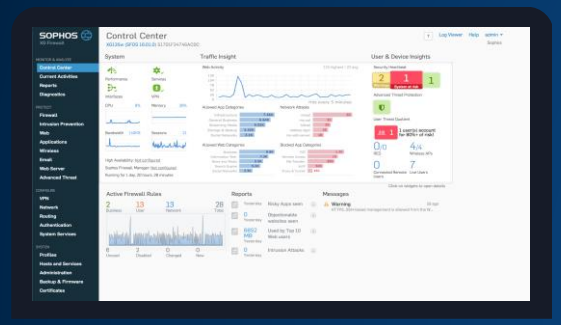
SOPHOS

XG Firewall Features

SOPHOS

Sophos XG Firewall Features

Comprehensive next-gen firewall protection



SYNCHRONIZED SECURITY	Security Heartbeat	Missing Heartbeat	Destination Heartbeat	Dynamic App Control
CONTROL	User identity & awareness	Web Control	App Control	Content Control
SECURITY	Advanced Threat Protection	Next-Gen IPS	Web Protection	Web Application Firewall
	Stateful Firewall	Deep-packet inspection	Dual anti-virus	Encrypted Traffic Inspection
	Email anti-spam & phishing protection	Email Encryption	Data Loss Prevention	Sandboxing
NETWORKING	Routing, Bridging & NAT	Zone Segmentation	Traffic Shaping	Wireless Controller
	FastPath Packet Optimization	Full standards-based VPN	RED VPN	IPv6 Support

The XG Firewall Advantage

		Sophos XG Firewall	CheckPoint NGFW	WatchGuard Firebox	Fortinet FortiGate	SonicWALL NSA	Cisco Meraki
Next-Gen Firewall and ATP	FastPath Packet Optimization	✔	✔		✔		
	Dual AV Engines	✔					
	IPS (NSS Recommended)	✔	✔	✔	✔		✔
	Application Control	✔	✔	✔	✔	✔	✔ (partial)
	Web Protection and Control	✔+	✔	✔	✔	✔	✔
	User and App Risk Assessment & Visibility	✔			✔ (partial)		
	HTTPS Filtering	✔	✔	✔	✔	✔	✔
	Advanced Threat Protection	✔	✔	✔	✔	✔	✔
	Sandboxing	✔	✔	✔	✔	✔	✔
Synchronized Security	Identify Compromised Host, User, & Process	✔					
	Compromised System Isolation	✔					
	Unknown Application Identification	✔					
UTM & Deployment	Full-Featured Web Application Firewall	✔			+1Box	+1Box	
	Email AV, AS, Encryption & DLP	✔	+1Box	+1Box	+1Box	+1Box	+1Box
	Full Historical Reporting	✔	+1Box	+1Box	+1Box	+1Box	
	Plug-and-Play Remote Office Security (RED)	✔					
	Flexible Deployment (HW, SW, VM, IaaS)	✔	✔	No SW/IaaS	No SW	No SW/IaaS	HW only

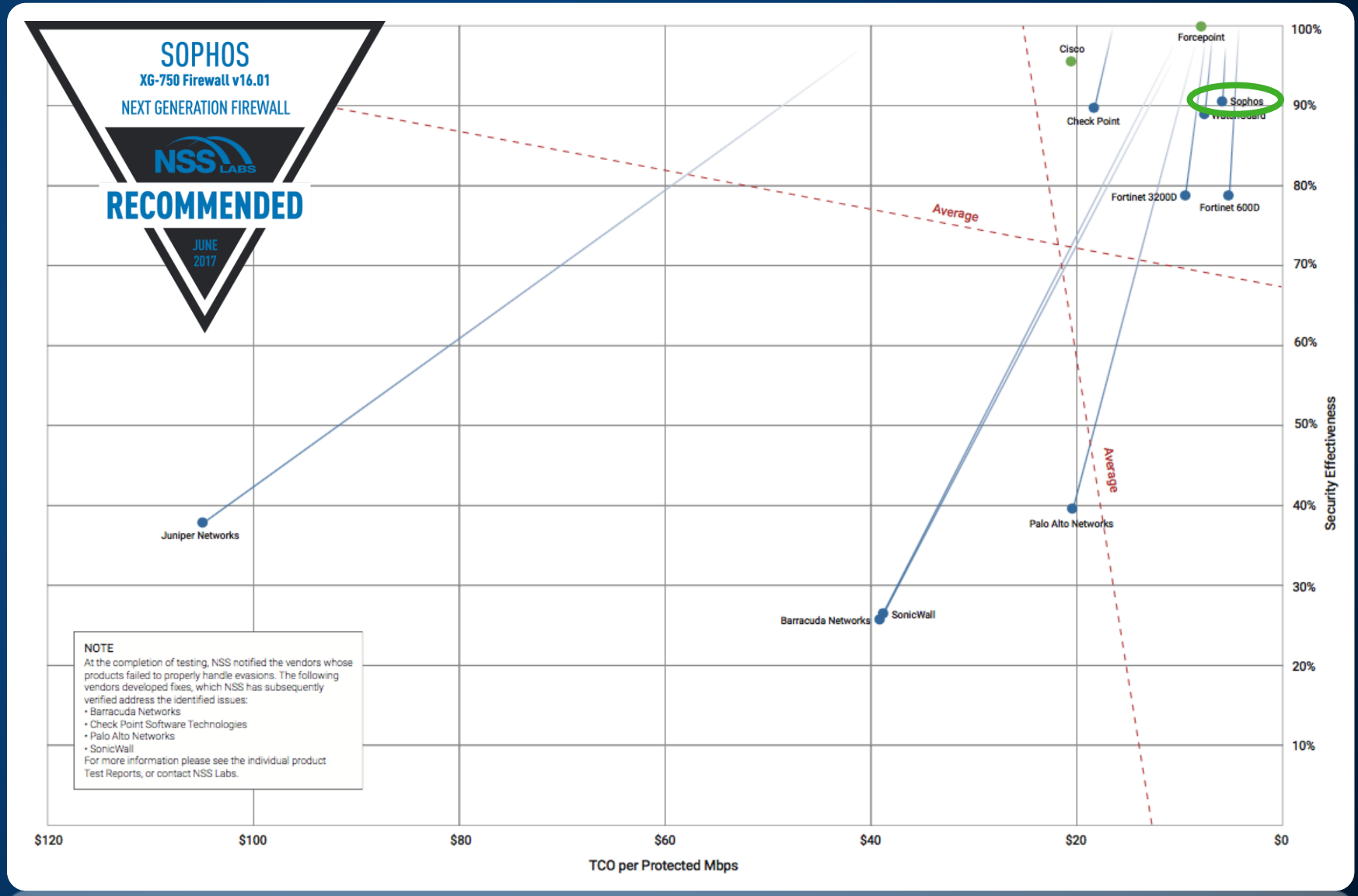
SOPHOS

Top Rated by Industry Analysts

SOPHOS

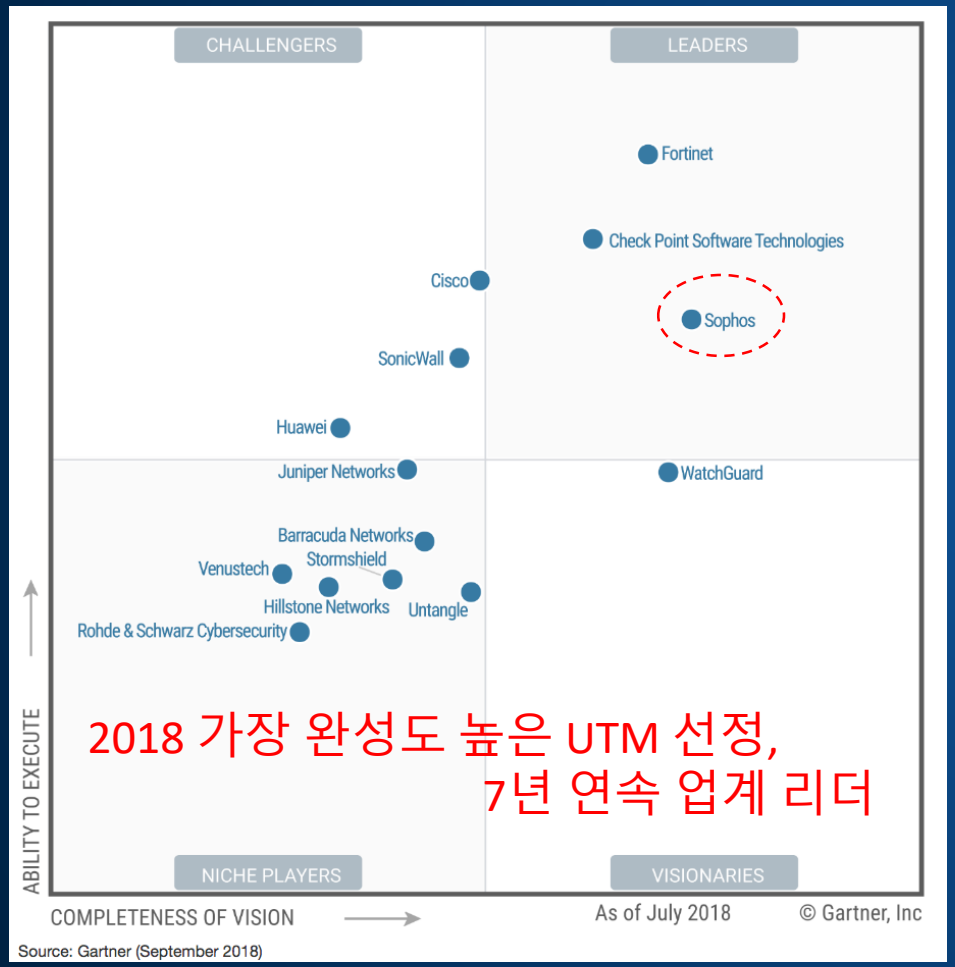
NSS Labs 2017 NGFW Report

- Best mix of protection, performance, and value
- 3rd in Security Effectiveness Beating: Check Point, WatchGuard, Fortinet, PAN, SonicWall, and Juniper
- Effectively tied for best Price-Performance with Fortinet
- Lines indicate final performance from baseline protection after evasion detection is considered
- Sophos only missed 2 out of 137 evasion techniques and we are working on patches for those
- Performed much better than most competitors in evasion detection



Sophos is a MQ Leader in both Network and Endpoint

MAGIC QUADRANT for UNIFIED THREAT MANAGEMENT



2018 년도 Magic Quadrant for Unified Threat Management,

Magic Quadrant for Unified Threat Management,
Rajpreet Kaur, Claudio Neiva, 20 September, 2018

MAGIC QUADRANT for ENDPOINT PROTECTION PLATFORMS

2018 년도 Magic Quadrant for Endpoint Protection Platforms,

Magic Quadrant for Endpoint Protection Platforms,
Ian McShane, Avivah Litan, Eric Ouellet, Prajeet Bhajanka; 24 January, 2018

SC Media Review

- STRENGTHS: *Very creative convergence of a lot of solid functionality. Documentation is presented in a novel way on the web portal.*
- WEAKNESSES: *None that we saw.*
- VERDICT: *This demands your attention no matter what size your organization.*

RATING BREAKDOWN

SC Lab Reviews

Reviews from our expert team

Features: ★★★★★ Documentation: ★★★★★ Value for Money: ★★★★★

Performance: ★★★★★ Support: ★★★★★ Ease of Use: ★★★★★

5/5

GROUP TEST UTM/SIEM/NGFW

SC ★★★★★

Sophos

XG Firewall

DETAILS

Vendor Sophos

Product XG Firewall

Website sophos.com/xgfirewall

Price Starting at $249/year on a three-year term for TotalProtect Plus & Enhanced Support on an XG 85.

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Very creative convergence of a lot of solid functionality. Documentation is presented in a novel way on the web portal.

Weaknesses None that we saw.

Verdict This demands your attention no matter what size your organization. There are models to cover most requirements.

This product is a UTM that bills itself as a next-generation firewall. This was one that rather took us aback because we don't tend to think of UTMs as firewalls. However, the argument is that a UTM really has a lot of traditional firewall functionality. So, if we add the next-generation functionality, the characterization makes sense. The functionality in this UTM includes, among other things, firewall, IPS, application security, wireless gateway and advanced threat protection.

We dropped into the landing page, what Sophos calls the Control Center, and got the usual top-level dashboard. From here there are extensive drill-downs. One particular feature that we liked was the User & Device Insight. This is a top-level view of a device being monitored. It gives a lot of detail about the device, including the Security Heartbeat. As one would expect, the Sophos anti-malware legacy shows up extensively with just about any type of malware identified and addressed.

This is a unique function that lets the endpoint communicate directly with the tool – resulting in a lot of endpoint information being sent for analysis. This includes analysis of suspicious files in the Sophos cloud-based sandbox, called Sandstorm. Sandstorm can simulate activity for a delay of up to six months for delayed detonation malware. This is more than just a passive look at the endpoint.

The User Threat Quotient – UTQ – identifies high-risk users based on their activities, such as suspicious file downloads. Setting rules is straightforward and the firewall rules look exactly as you would expect, which simplifies management for experienced engineers who are seeing what they expect to see. Editing rules is easy, consisting mostly of making selections from a menu page. However, if your selection is not there, you certainly can add your own.

Reporting is a strong suite for XG Firewall. There are over 1,000 reports available out of the box. Overall, we found this to be a useful tool. If you are a Sophos shop, reporting can aggregate across Cyberoam, XG and UTM 9 devices into a single report, a winning feature. Like the UTQ, the App Risk Analysis identifies high-risk applications.

Pricing on this product is very reasonable and there are multiple levels of support. There is a basic level of support at no cost during the first 90 days to cover the deployment period. After that there are two additional levels of fee-based support. The website has a good assistance portal that includes such things as a knowledge base and an FAQ. There also are forums along with some self-help guides.

So, next-generation firewalls as UTMs? We believe there is a very good case to be made for that. Time will tell, of course, but this is a market space that is certainly characterized by convergence.

– Peter Stephenson, technology editor

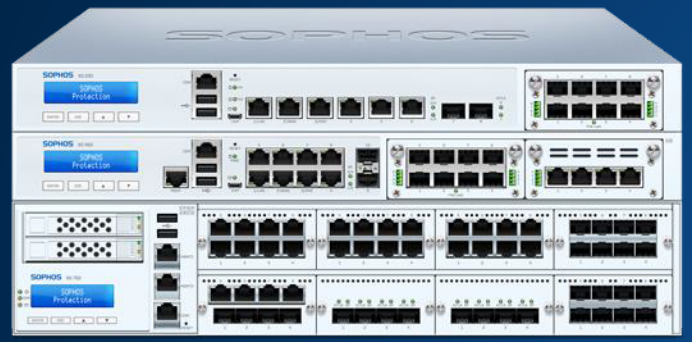
SOPHOS
Security made simple

Sophos
The Pentagon, Abingdon Science Park
Abingdon OX14 3YP
United Kingdom
Toll Free: 1-866-866-2802 - Email: nasales@sophos.com

Reprinted from SC Magazine, May 2017 • www.scmagazine.com

타협이 없는 배포의 유연성

오늘날의 비지니스에 최적화된 배포 옵션



XG Series Hardware

Full range of hardware appliances with wireless AP and RED add-ons
Multi-core processors, solid-state storage, generous RAM
Industry-leading performance at all price points – Miercom tested

Windows Server Hyper-V
KVM
XenServer
Integrate, manage, and automate a virtual datacenter.
vmware

Virtual/Software

Vmware, Hyper-V, Citrix XEN, KVM
Flexibility regarding resource assignment and high availability
Compatible with all x86 hardware

Microsoft Azure

IaaS

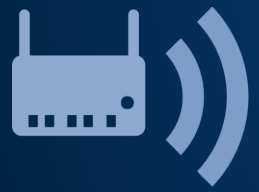
Available in Microsoft Azure Marketplace
Up and running in minutes with preconfigured VM
Pay-as-you-go or BYOL

XG 제품들

하드웨어, 보호, 중앙화된 관리

Hardware

Appliances
(optional High-Availability)



Wireless APs

RED Devices

Protection Modules

Network Protection

Web & App Protection

Sandstorm Protection

Email Protection

Web Server Protection

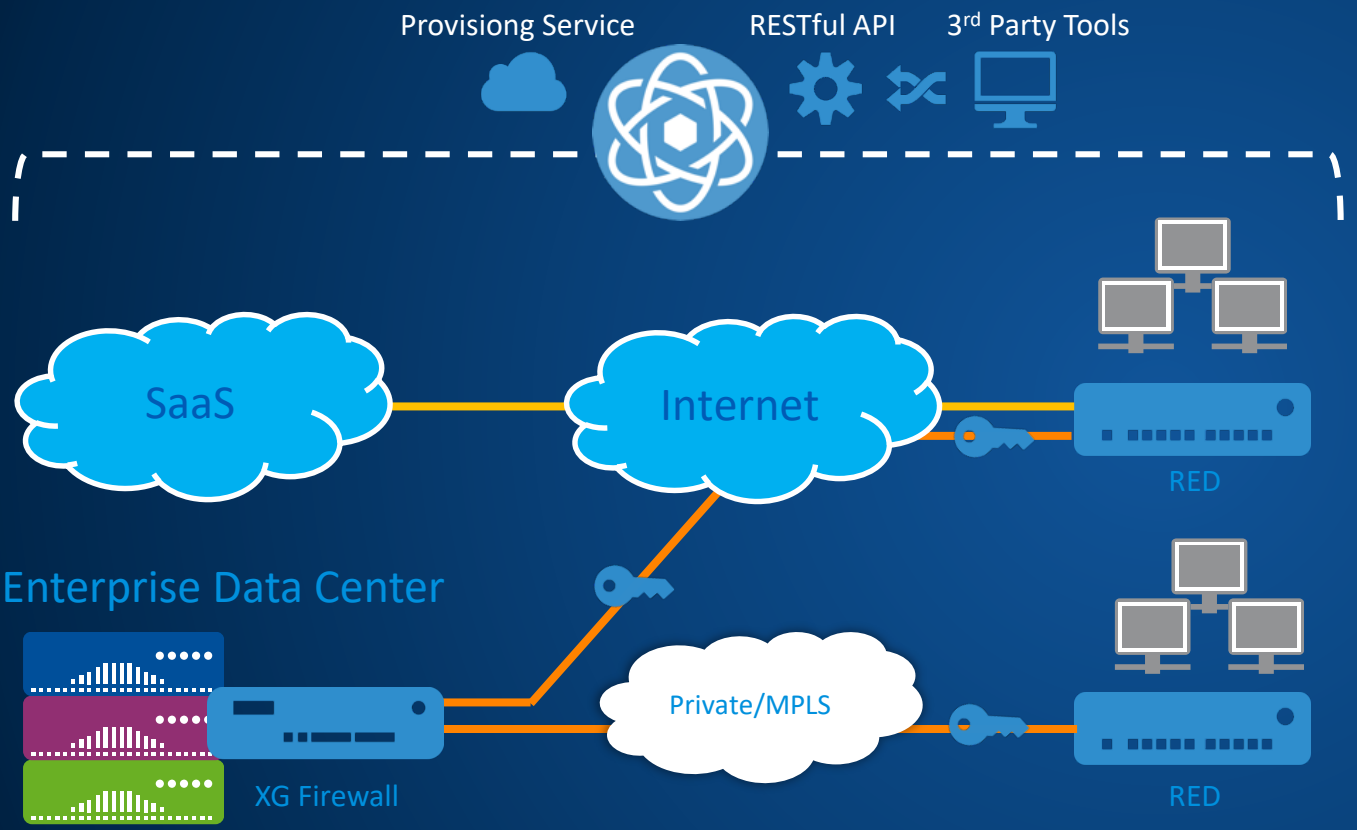
Central Management

Sophos Firewall Manager

Sophos iView

다수지점으로 분산된 환경 - Sophos RED

SD-WAN 구축시 고려 사항



- 간편한 원격지 배포
- 유연한 배포 옵션
- Full Tunnel 혹은 Split Tunnel 구성
- Hybrid WAN & dynamic path
- 완전히 암호화된 트래픽
- 중앙 제공 및 관리
- 라이센스 필요 없음.

Dynamic Path Selection

RED dynamic multipath optimization includes WAN link monitoring and balancing, auto fail-over, WAN link characteristic detection, routing, and QoS

Three models:

- RED 15 / 15w and RED 50

SOPHOS

Synchronized Security & Threat Protection

SOPHOS

Threat Landscape > Technology Focus & Investment

Ransomware

EternalBlue (Wanna)와 같은
패치되지 않은 취약점은
여전히 가장 큰 문제

Synchronized Security & IPS

Office Files

문서의 취약점 공격을
포함한 이메일 첨부파일과
웹 다운르드

Sandboxing

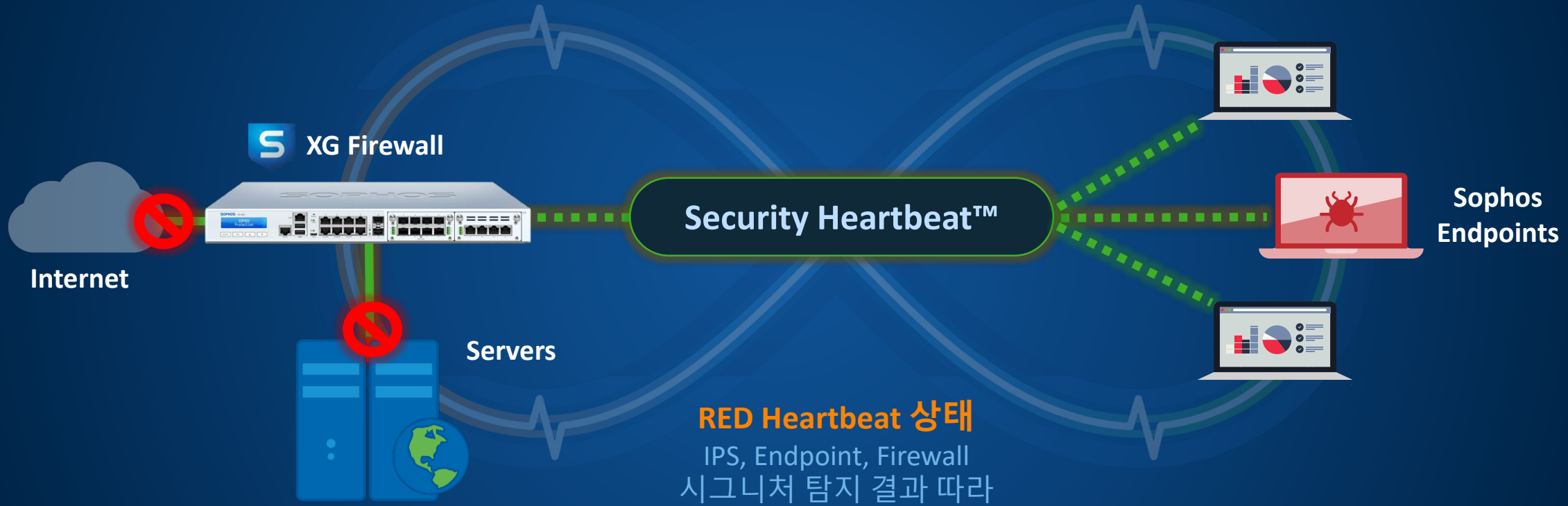
Cryptojacking

가상화폐 마이닝을 수행하는
감염된 웹사이트들

Web Protection & PUAs

엔드포인트 격리 & Security Heartbeat

방화벽에서 자동시스템 격리



RED Heartbeat 상태

IPS, Endpoint, Firewall
시그니처 탐지 결과 따라
격리를 시작합니다.

래터럴 무브먼트 보호

엔드포인트에서 자동으로 시스템 격리– 동일한 네트워크에서도 적용

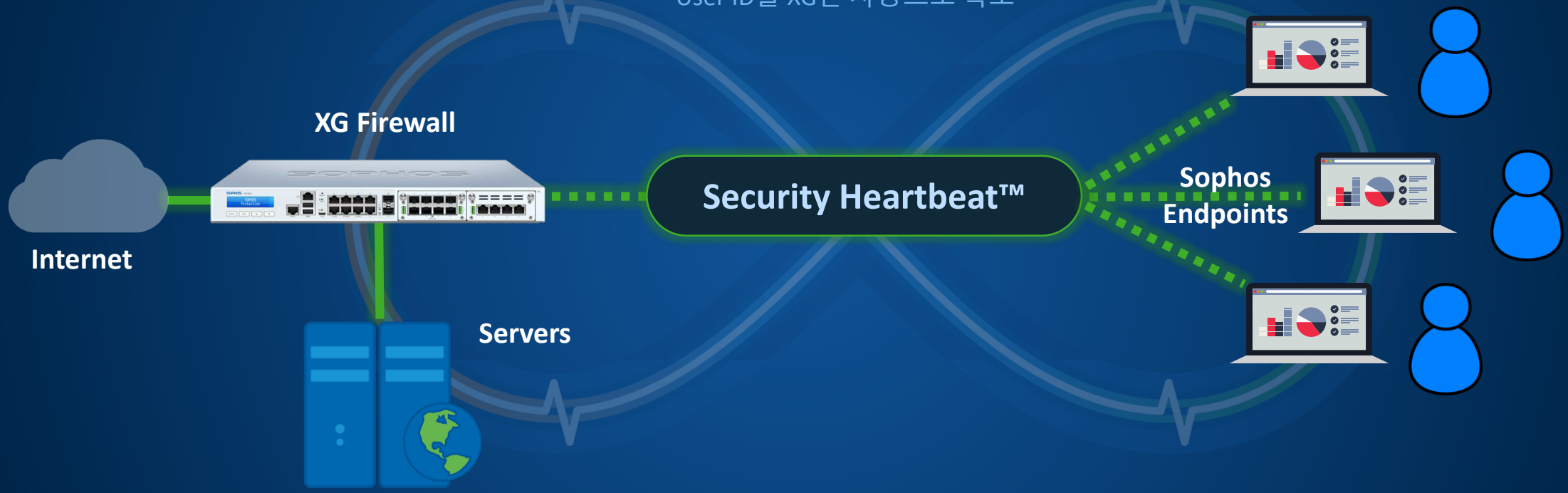
래터럴 무브먼트 보호
XG는 감염된 장치로부터의 모든
트래픽을 차단할것을 다른
엔드포인트들에게 즉시 알림

RED Heartbeat 상태
IPS, Endpoint, Firewall 시그니처
탐지 결과 따라 격리를
시작합니다.

싱크로나이즈드 User ID

인증 에이전트 필요성 제거

Synchronized User ID
AD 도메인에 있는 엔드포인트의
User ID를 XG는 자동으로 확보



AD 통합 없이도 전체 네트워크 유저 인식

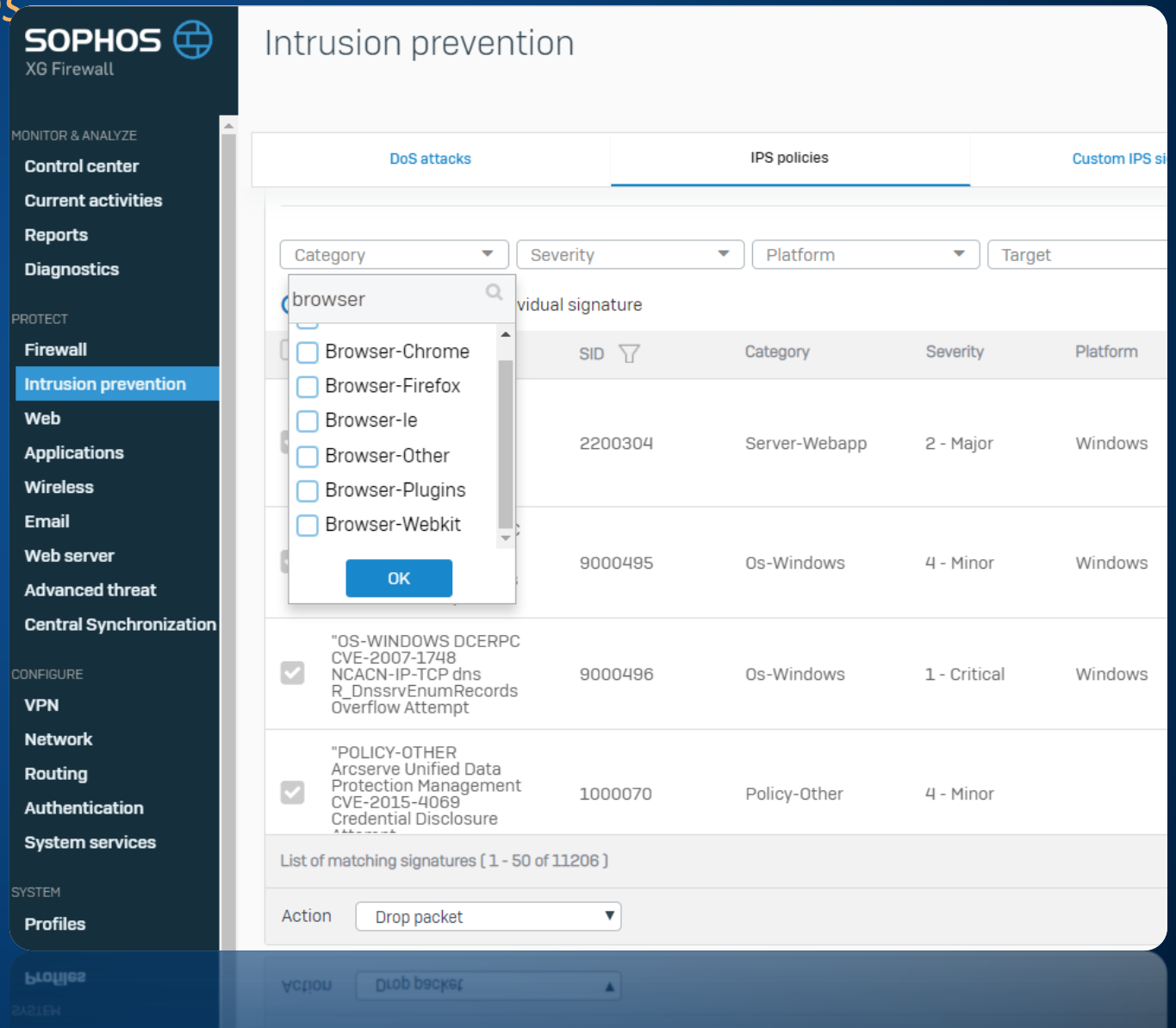
SOPHOS

IPS Enhancements

Enterprise pattern integration - Talos

새로워진 부분

- 엔터프라이즈 카테고리 : IPS 패턴 강화
- 깊고, 넓고, 세분화된 커버리지
- 60개의 카테고리(기존21개)
- 정책의 세밀화 증가

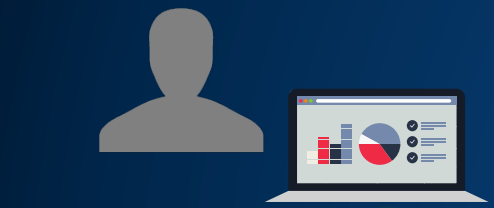


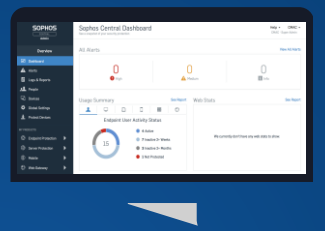
Enabling Added Clarity and Control or Introducing Sophos Security Fabric?

User Identity
Obtain User ID from EP for authentication

IoT Identification
Device detection and ID with Deep Learning, Improve visibility and ability to control use of cloud services

Sophos Central Integration
Cloud Management and Reporting for XG Firewall



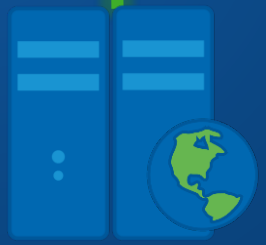


Endpoint Health

Endpoint Stonewalling
Prevent lateral movement even on the same network segment

Device Access and Onboarding
Redirect and enforce network and application level access for un-managed devices

Server Health



CASB
Cloud Access Security Broker for visibility and control

SOPHOS

Networking

SOPHOS

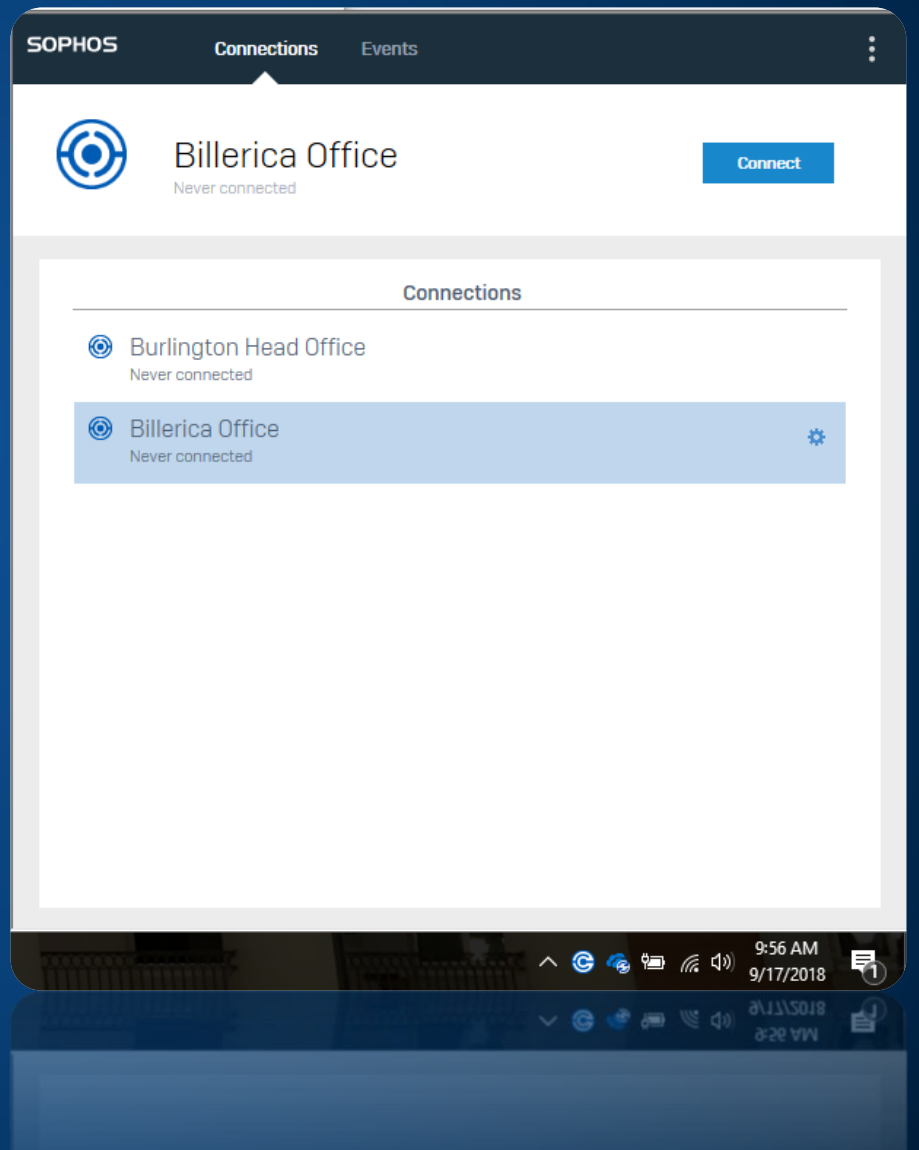
Synchronized Security via Remote VPN

안전한 외부 연결을 위한 가장 쉬운 무료 클라이언트

What's New

- IPSec VPN client for Windows/Mac
- 외부 사용자를 위한 Synchronized Security 지원
- 쉬운 배포와 관리
- 사용자 교육이 필요없는 간편한 사용

무료제공!



Management & Trouble-shooting

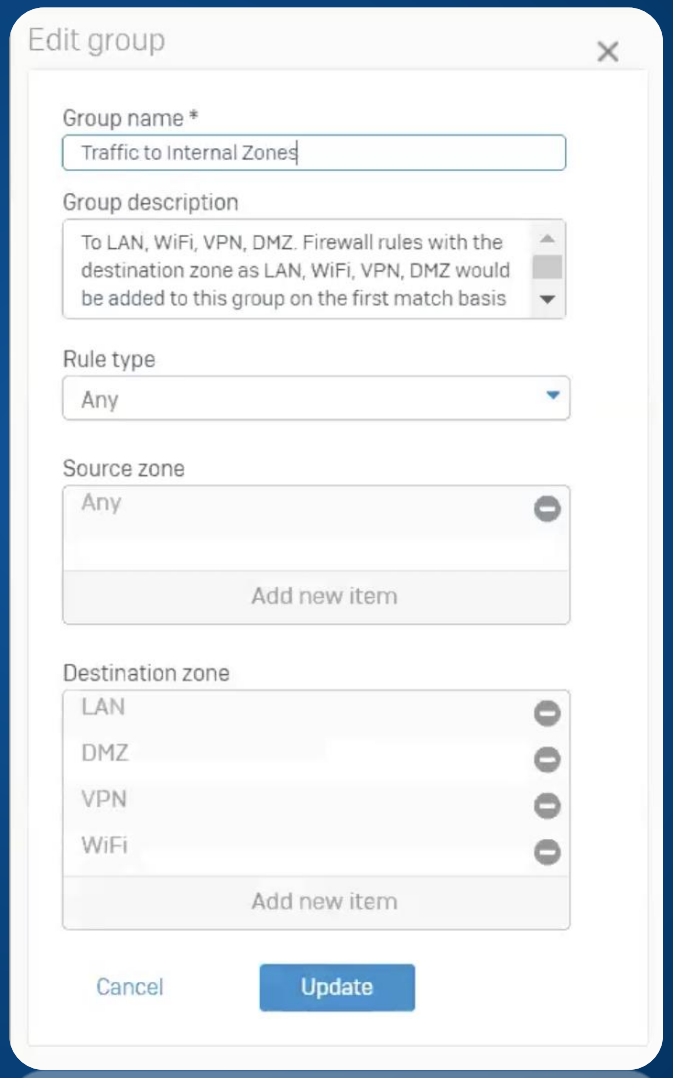
SOPHOS

Firewall Rule Grouping

대형 방화벽 규칙 설정을 위한 이상적인 변경

What's New

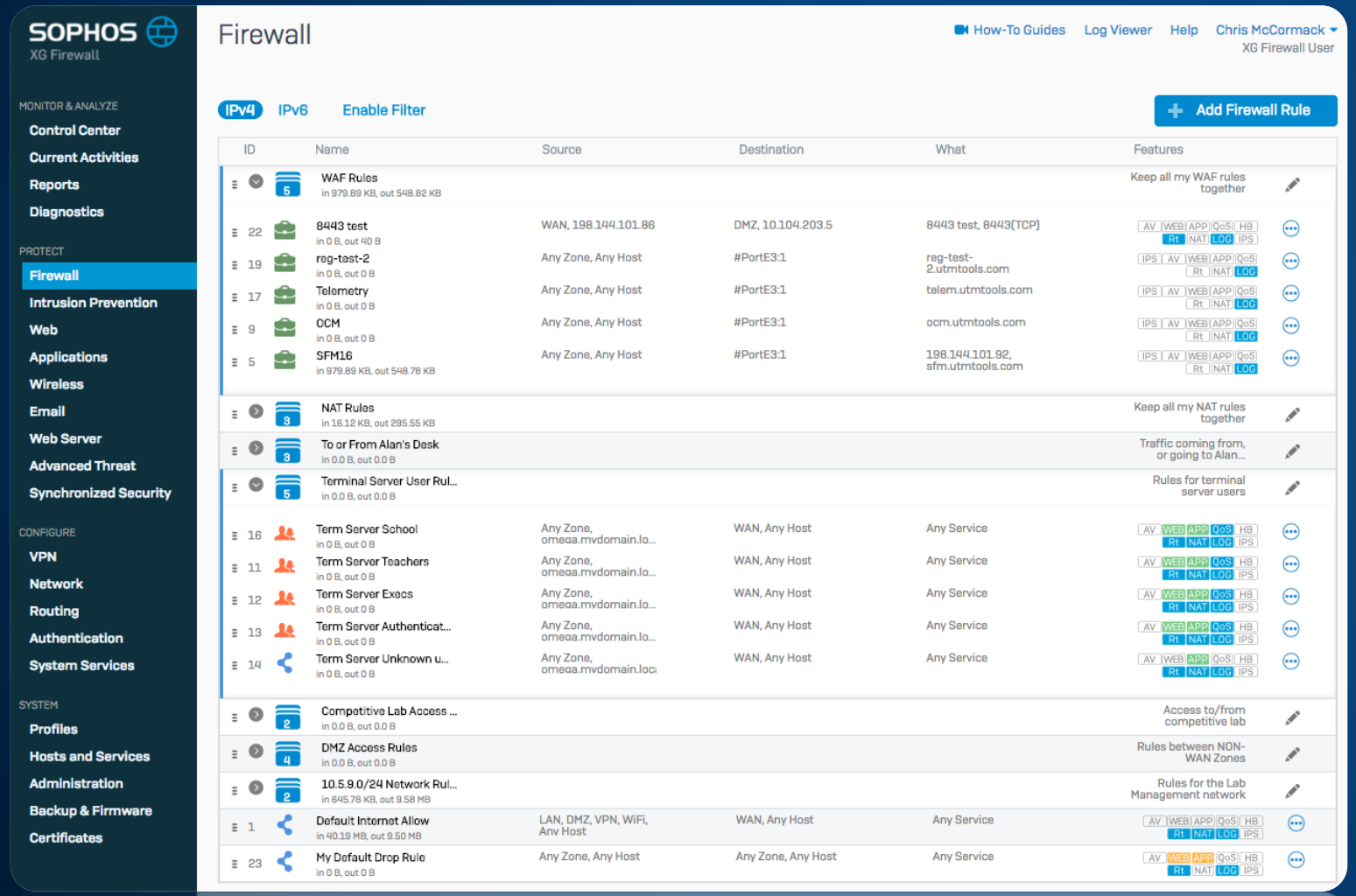
- Setup matching criteria as part of the group definition for auto group assignment



SOPHOS

Firewall Rule Management

Solving the problem of managing large rule sets



New Firewall Rule Management

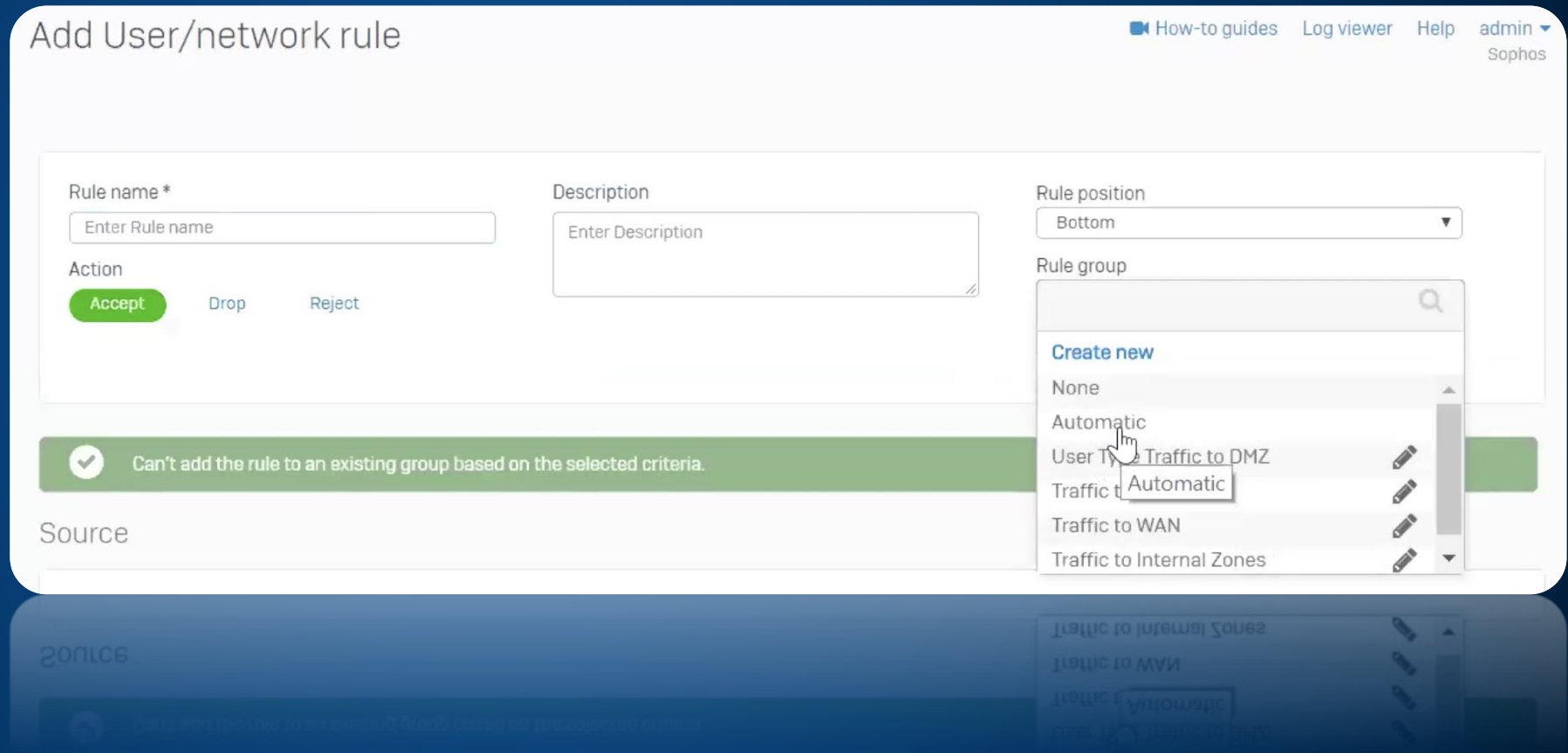
- Solves a problem many organizations have with managing large rule sets
- More powerful firewall rule management that's intuitive
- More compact rules with great visibility at-a-glance
- Support for groups, drag and drop, and mouse-over pop-ups

Firewall Rule Grouping

대형 방화벽 규칙 설정을 위한 이상적인 변경

What's New

- Setup matching criteria as part of the group definition for auto group assignment
- Select a group when creating a rule or set to automatically be assigned a group



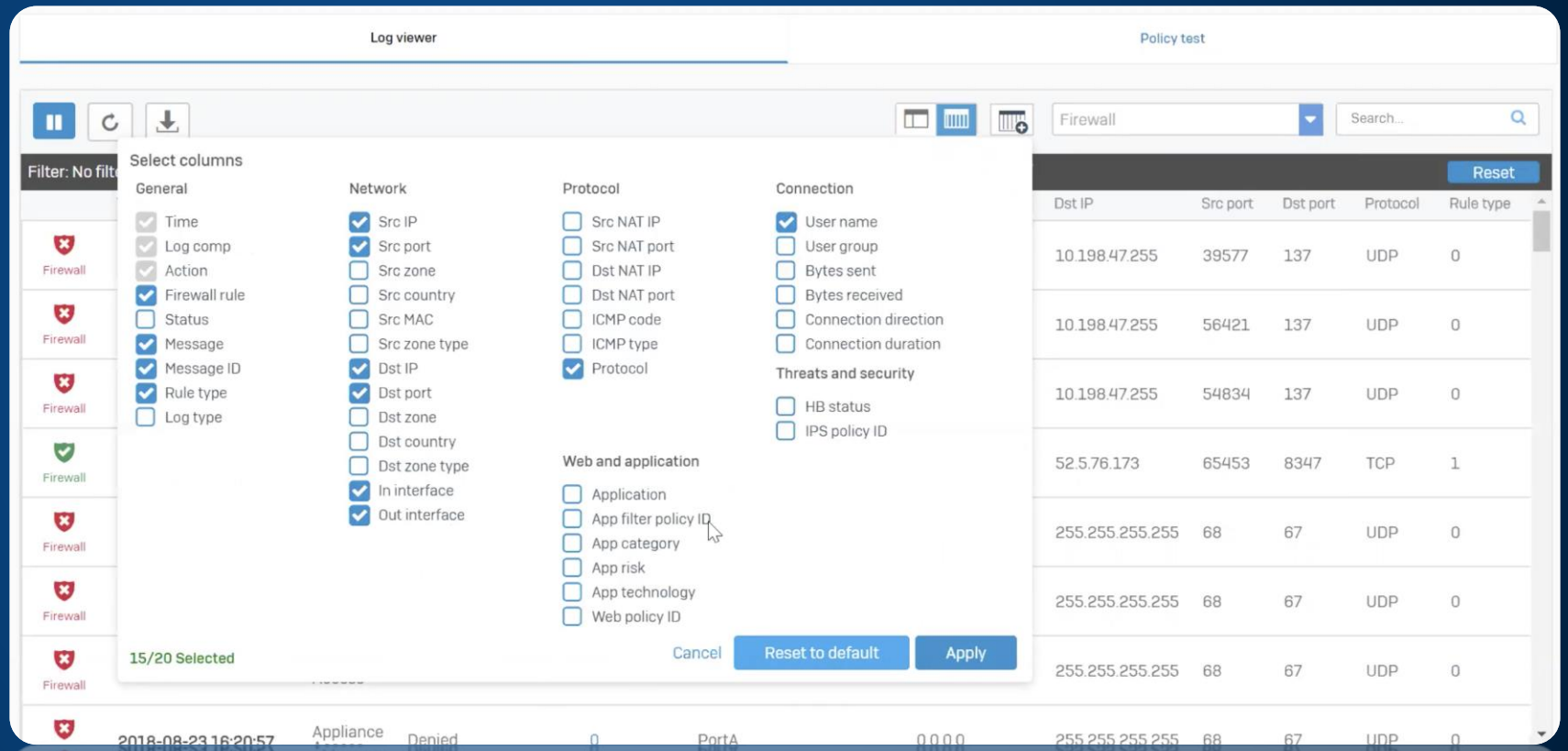
Log Viewer 향상

More powerful and streamlined trouble-shooting

What's New

- 컬럼 선택기 - 44개 필드 중 17개를 선택적으로 확인

- 로그에 참조된 Rule IDs은 하이퍼링크로 기재됨 메인 윈도우에서 관련된 룰을 클릭시 자동 오픈됨



SOPHOS

Sophos Central Management

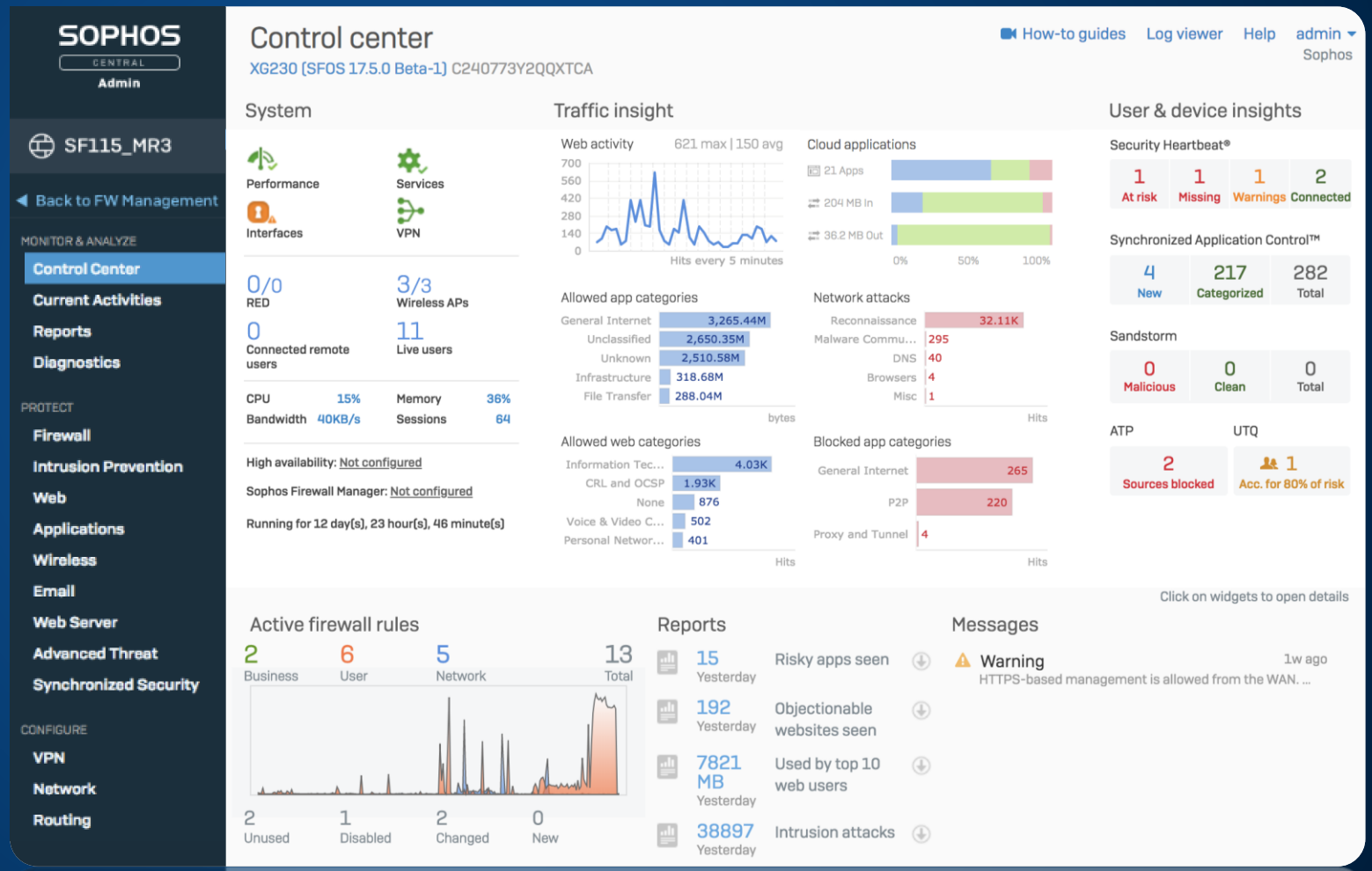
SOPHOS

Sophos Central Management for XG Firewall

XG Firewall을 Sophos Central에서 관리하세요.

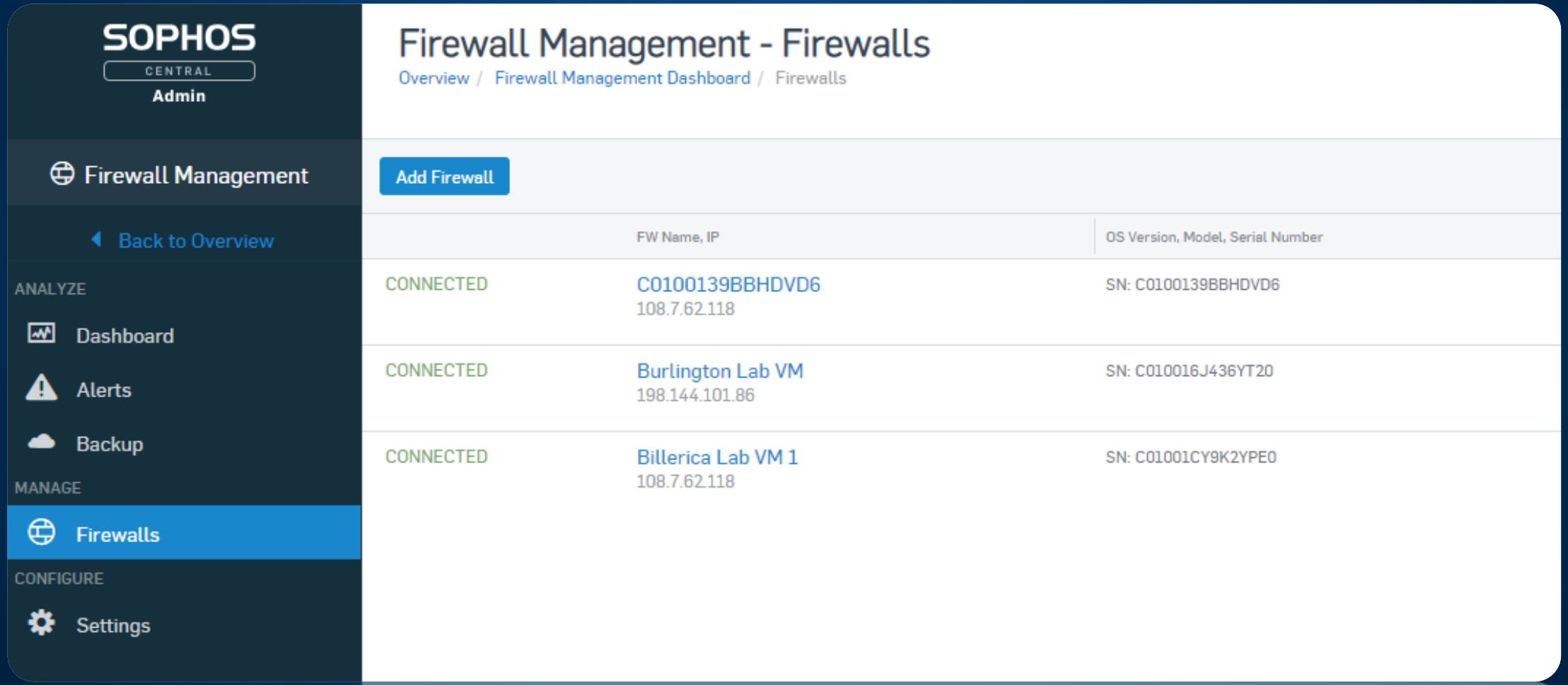
One Console

- 모든 Central 제품처럼 XG를 관리하고, 상태를 확인
- SSO를 통한 완전한 장치 관리
- 소포스 Central 을 통한 모든 XG장비를 안전하게 외부 접속
- 가용성, 라이센스, 퍼포먼스, 보안 상태 알람 및 상태보기 제공
- 펌웨어 업데이트 관리
- Central내에 백업파일 저장과 유지 옵션
- 새로운 장치 설치시 Zero-touch setup



XG Firewall in Sophos Central

관리중인 모든 방화벽을 소포스 Central 에서

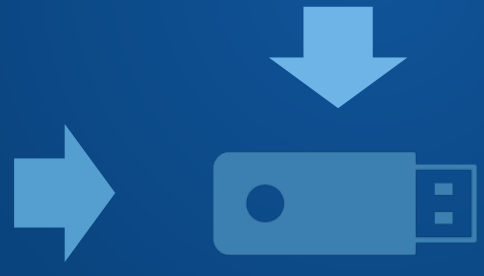


Rapid Deployment

현장 엔지니어 없이 외부 장치 배포

1. Sophos Central내의
Setup Wizard 사용

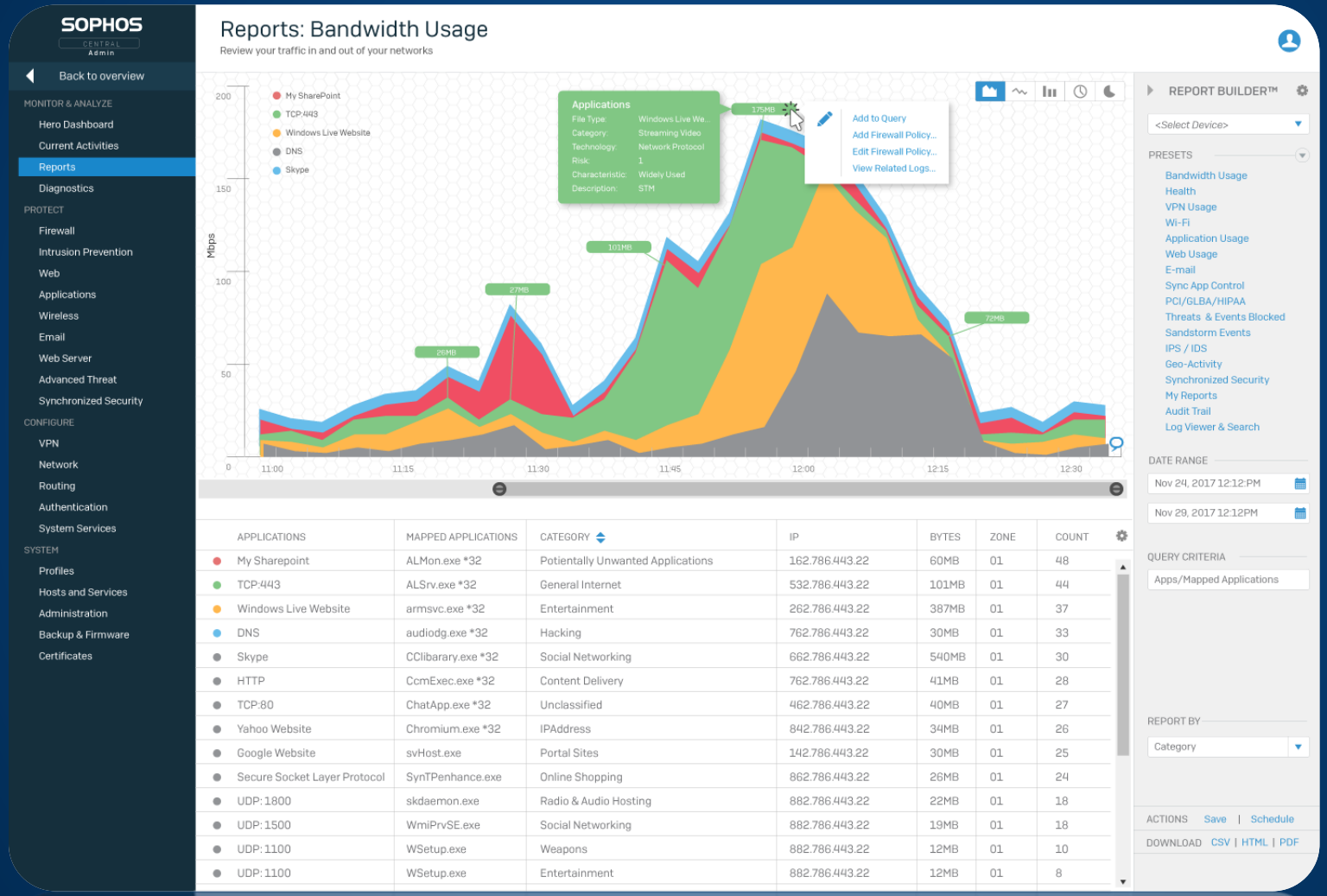
2. (Optional)
원격지에 Email로 설정파일 송신



3. USB 스틱에 설정파일 복사

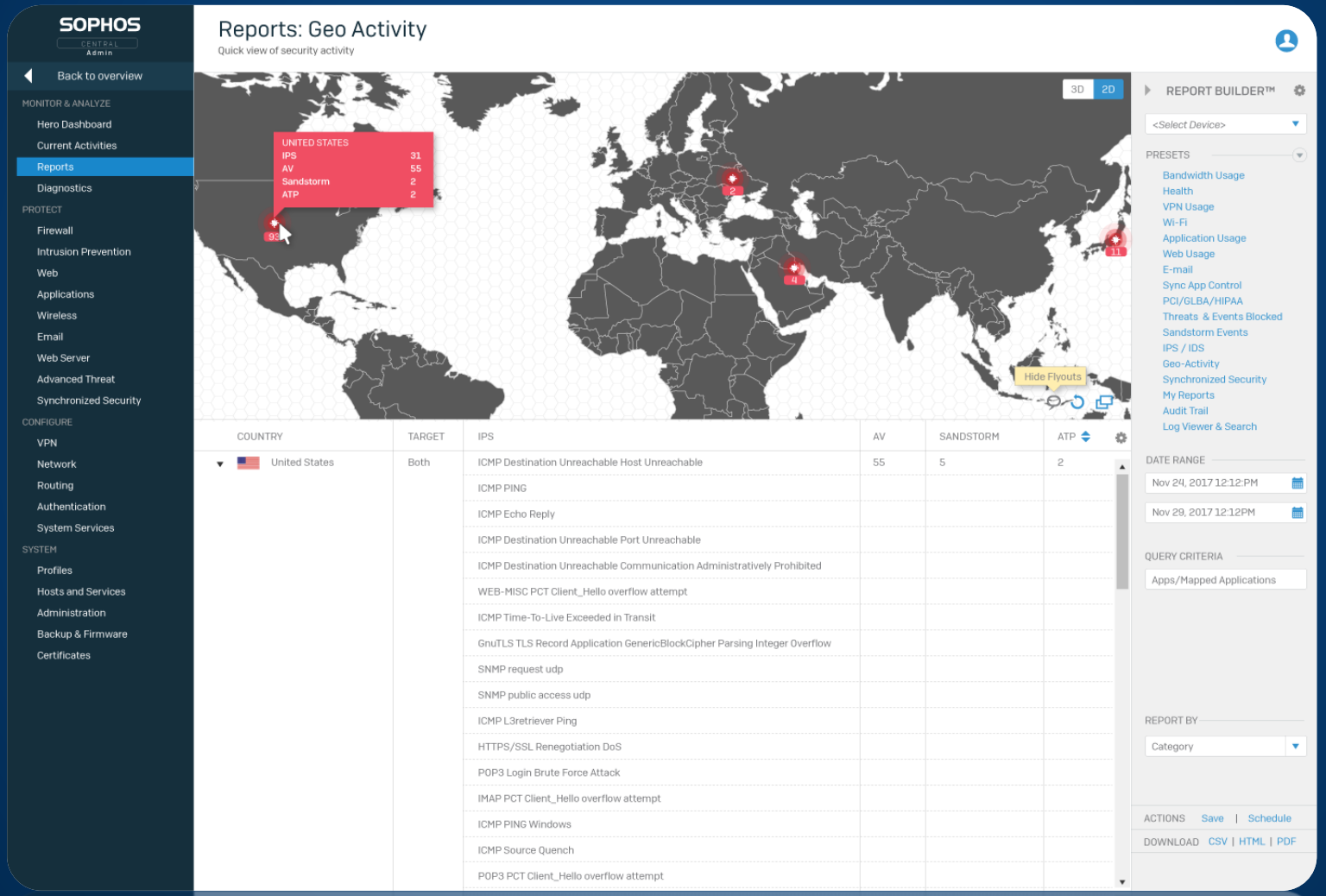
4. 연결된 USB 로 장비 부팅

Reporting - Bandwidth Usage



Reporting - Health

Reporting - Geo Activity



SOPHOS

Security made simple.