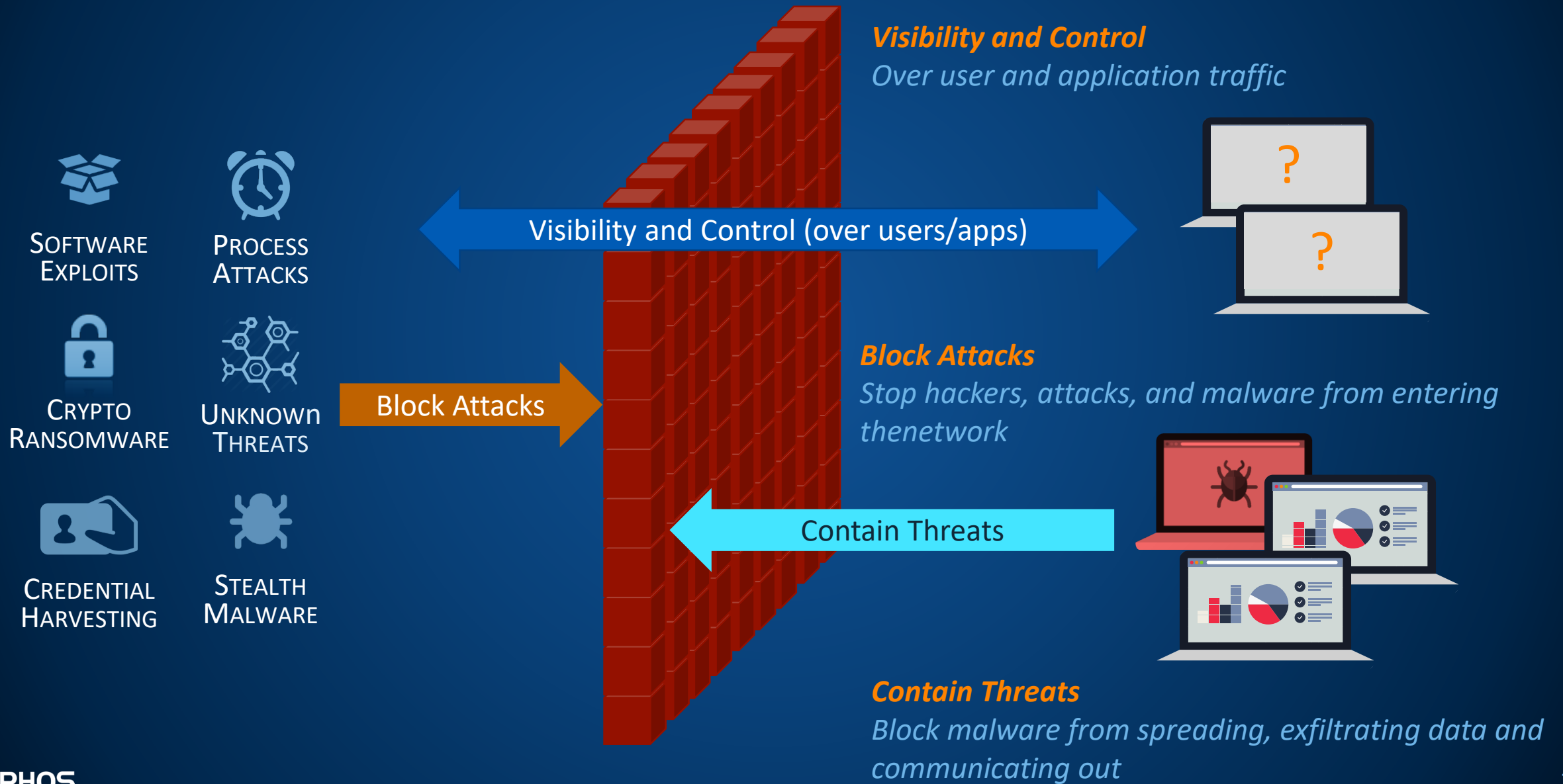


XG Firewall



필수적으로 요구되는 차세대 방화벽의 역할



시작하기전에- 현재의 어려움...

Giving you an opportunity to talk about our exclusive advantages



Visibility



Protection



Response

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-box 리포팅
- ✓ 위험도 높은 유저와 의심스러운 payload의 식별
- ✓ 알려지지 않은 클라우드 및 네트워크 어플리케이션 식별

2. 알려지지 않은 위협의 방어

- ✓ 전체 보안을 아우르는 Full suite – 쉬운 관리
- ✓ Deep learning
- ✓ 최고 성능의 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

현재의 방화벽들 - 활성화된 위협을 식별할 방법은?

Dashboard

System

Network

3G/4G/Modem

SonicPoint

Firewall

Firewall Settings

DPI-SSL

DPI-SSH

Capture ATP

VoIP

Anti-Spam

VPN

SSL VPN

Virtual Assist

Users

High Availability

Security Services

WAN Acceleration

AppFlow

Log

Log Monitor

Settings

Syslog

Automation

Name Resolution

Reports

Analyzer

Dashboard / **Log Monitor**

+ Filter View

Filter: Display: Last 5 minutes

CSV txt

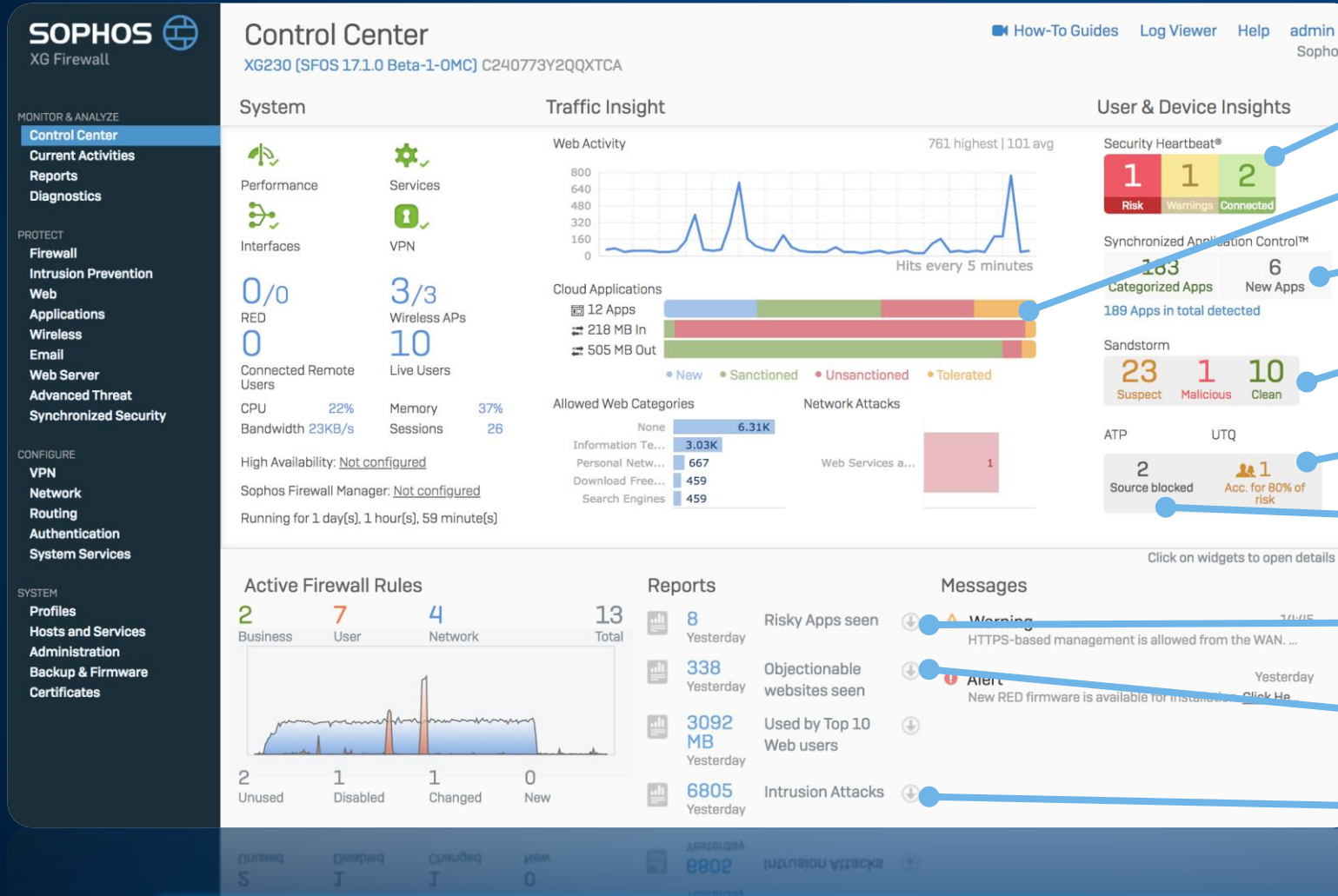
Status

Refresh: 60 sec.

UTC Time	ID	Category	Priority	Message	Source	Destination	IP Protocol	Notes	
16:23:22 Sep 20	791	Security Services	Inform	DPI-SSL: SSL connection aborted during negotiation with server: connection between 74.126.144.110:443 and 192.168.150.214:59786				[Some details are no longer available]	
16:23:22 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: PROTOCOLS SSL -- TLSv1.2, SID: 7927, AppID: 1279, CatID: 74	74.126.144.110, 443, X1	192.168.150.214, 61401, X0	tcp		
16:23:22 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: WEB-BROWSER OpenSSL Client -- HTTPS Activity, SID: 6427, AppID: 1895, CatID: 88	192.168.150.214, 59786, X0	74.126.144.110, 443, X1	tcp		
16:23:21 Sep 20	526	Network	Notice	Web management request allowed	70.91.35.237, 14501, X1	173.240.215.242, 443, X1	tcp		
16:23:16 Sep 20	175	Network	Notice	ICMP packet from LAN dropped	192.168.150.224, X0	192.168.150.242	icmp		
16:23:15 Sep 20	1073	Users	Warning	SSO agent returned error	192.168.150.6, 2258, X0	192.168.150.212, X0		Error communicating with...	
16:23:11 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: FILETYPE-DETECTION Image -- GIF 2 (HTTP Download), SID: 4239, AppID: 990, CatID: 72	54.243.160.36, 80, X1	192.168.150.210, 62512, X0	tcp		
16:23:11 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: WEB-BROWSER HTTP User-Agent -- Microsoft Windows 7, SID: 10293, AppID: 1901, CatID: 88	192.168.150.210, 62512, X0	54.243.160.36, 80, X1	tcp		
16:23:11 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: BROWSING-PRIVACY Chart Beat -- Client Activity 1, SID: 3767, AppID: 1325, CatID: 75	192.168.150.210, 62512, X0	54.243.160.36, 80, X1	tcp		
16:23:08 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: PROTOCOLS HTTP Protocol -- GET, SID: 5147, AppID: 1277, CatID: 74	192.168.150.213, 57744, X0	165.227.251.68, 80, X1	tcp		
16:23:07 Sep 20	791	Security Services	Inform	DPI-SSL: SSL connection aborted during negotiation with server: connection between 74.126.144.110:443 and 192.168.150.214:59785				[Some details are no longer available]	
16:23:04 Sep 20	41	Network	Notice	Unknown protocol dropped	192.168.150.180, 17, X0	239.192.0.0, 17	igmp		
16:23:04 Sep 20	97	Log	Inform	Web site hit	192.168.150.213, 57742, X0	77.234.41.56, 80, X1	tcp	Policy: CFS Default Policy Info: 6148	
16:23:01 Sep 20	1154	Firewall	Alert	Application Control Detection Alert: PROTOCOLS HTTP Protocol -- POST, SID: 5148, AppID: 1277, CatID: 74	192.168.150.213, 57742, X0	77.234.41.56, 80, X1	tcp		
16:23:01 Sep 20	1235	Network	Inform	Packet allowed: matched Access Rule	192.168.150.213, 57742, X0	77.234.41.56, 80, X1	tcp		
16:22:59 Sep 20	537	Network	Inform	Connection Closed	8.29.229.2, 56026, X1	173.240.215.242, 443, X1	tcp		
16:22:57 Sep 20	38	Network	Notice	ICMP packet dropped due to Policy	144.223.242.33, X1	173.240.215.242	icmp		

last update: UTC 16:23:27 Sep 20

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

SOPHOS

XG Firewall

MONITOR & ANALYZE

Control Center

Current Activities

Reports

Diagnostics

PROTECT

Firewall

Intrusion Prevention

Web

Applications

Wireless

Email

Web Server

Advanced Threat

Synchronized Security

CONFIGURE

VPN

Network

Routing

Authentication

System Services

SYSTEM

Profiles

Hosts and Services

Administration

Backup & Firmware

Certificates

Applications

How-To Guides Log Viewer Help admin Sophos

Cloud Applications

Synchronized Application Control

Application List

Application Filter

Traffic Shaping Default

From: 2018-03-21 To: 2018-03-21

Unsanctioned

All Categories

Sort by Bytes Transferred

Results: 3

Hotmail WebMail

Web Mail Medium Risk Unsanctioned

Classify Traffic Shaping

1.27 MB Traffic

1 Users

0 Uploads

0 Downloads

0 File Types

+ Facebook Website

Social Networking Medium Risk Unsanctioned

Classify Traffic Shaping

3.27 MB Traffic

5 Users

0 Uploads

0 Downloads

0 File Types

- Dropbox Base

Storage and Backup Medium Risk Unsanctioned

Classify Traffic Shaping

226 MB Traffic

3 Users

0 Uploads

0 Downloads

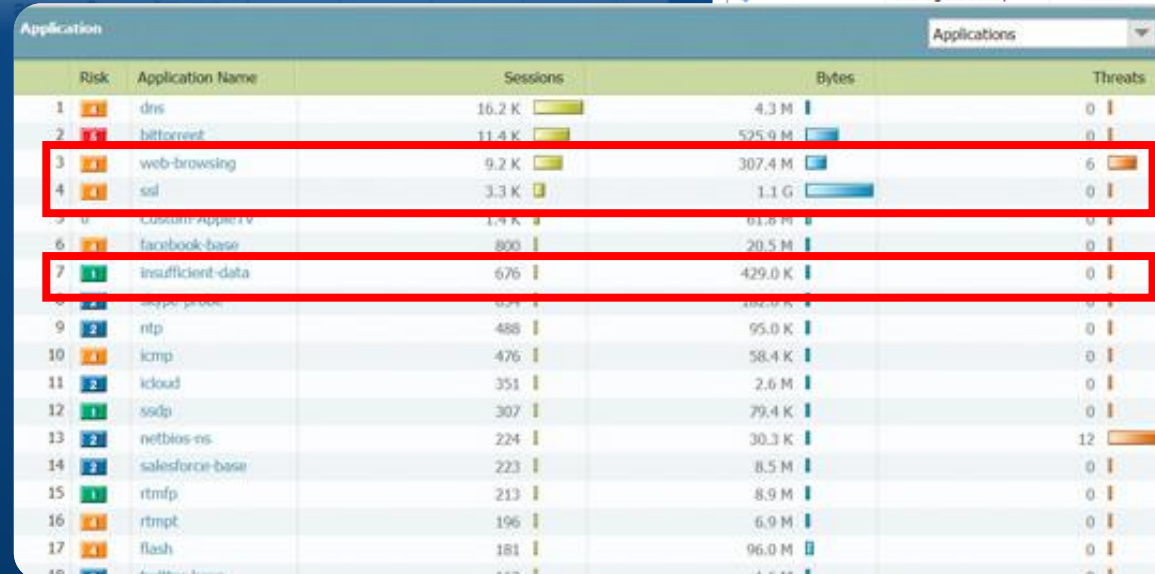
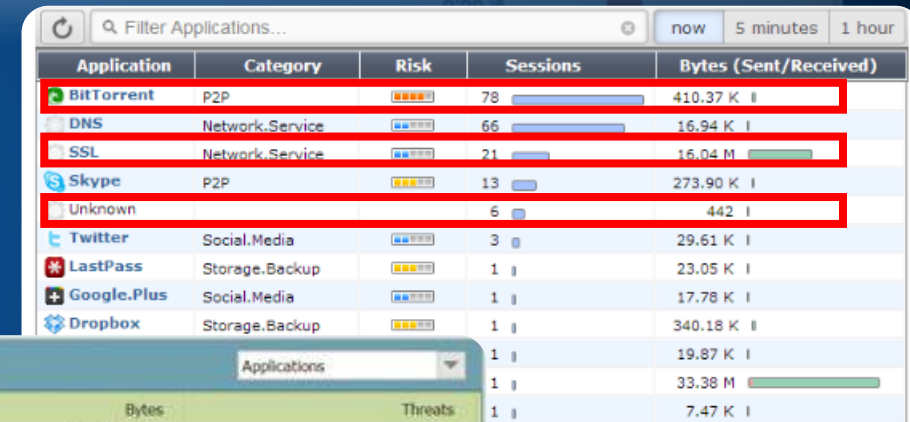
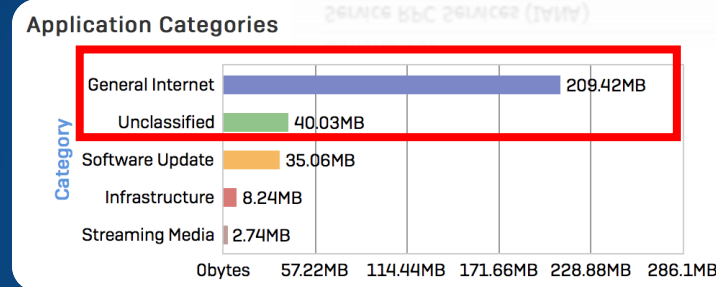
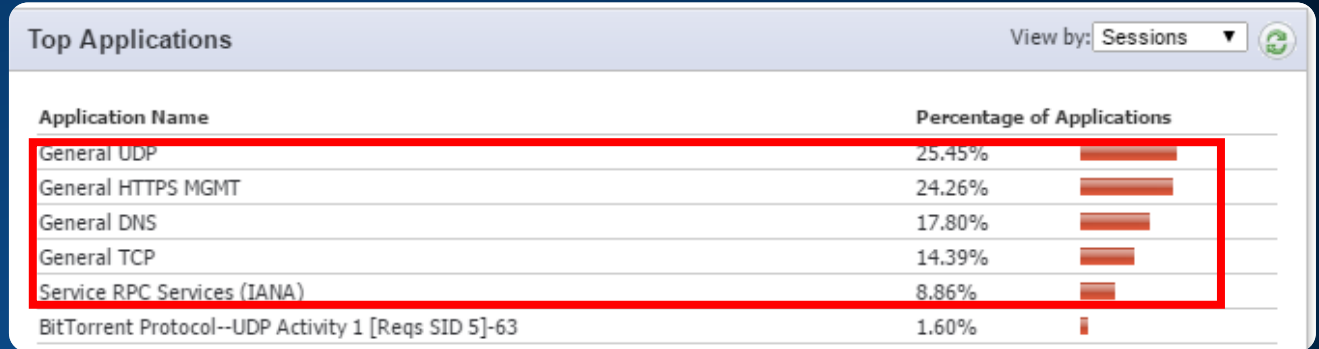
0 File Types

User	Host	Uploads	Upload Data	File Type	Downloads	Download Data	File Type
joe	192.168.1.2	0	200 MB		0	20 MB	
chris	10.0.1.15	0	1.79 MB		0	1.03 MB	
Unauthenticated User	192.168.1.2	0	1.67 MB		0	813 KB	
Unauthenticated User	10.0.1.61	0	3.13 KB		0	11.8 KB	

업계 최고의 앱 가시성이 더욱 향상되었습니다.

Application 문제 해결

- 방화벽 어플리케이션은 시그니처 기반입니다.
- 어플리케이션의 최대 90%가 인식되지 않습니다.
- 일부 앱들은 절대 시그니처를 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

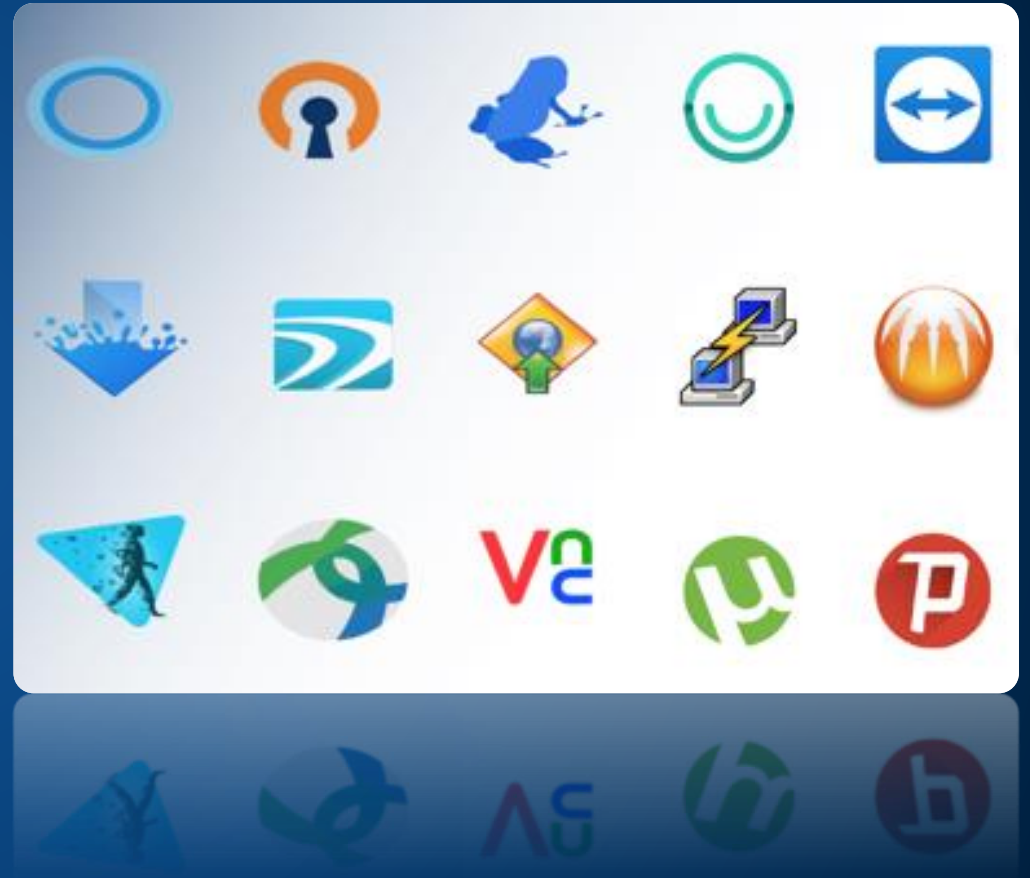
(uTorrent, Vuze, Freenet)

Proxy and Tunnel Clients

(Ultrasurf, Hotspot Shield, Psiphon)

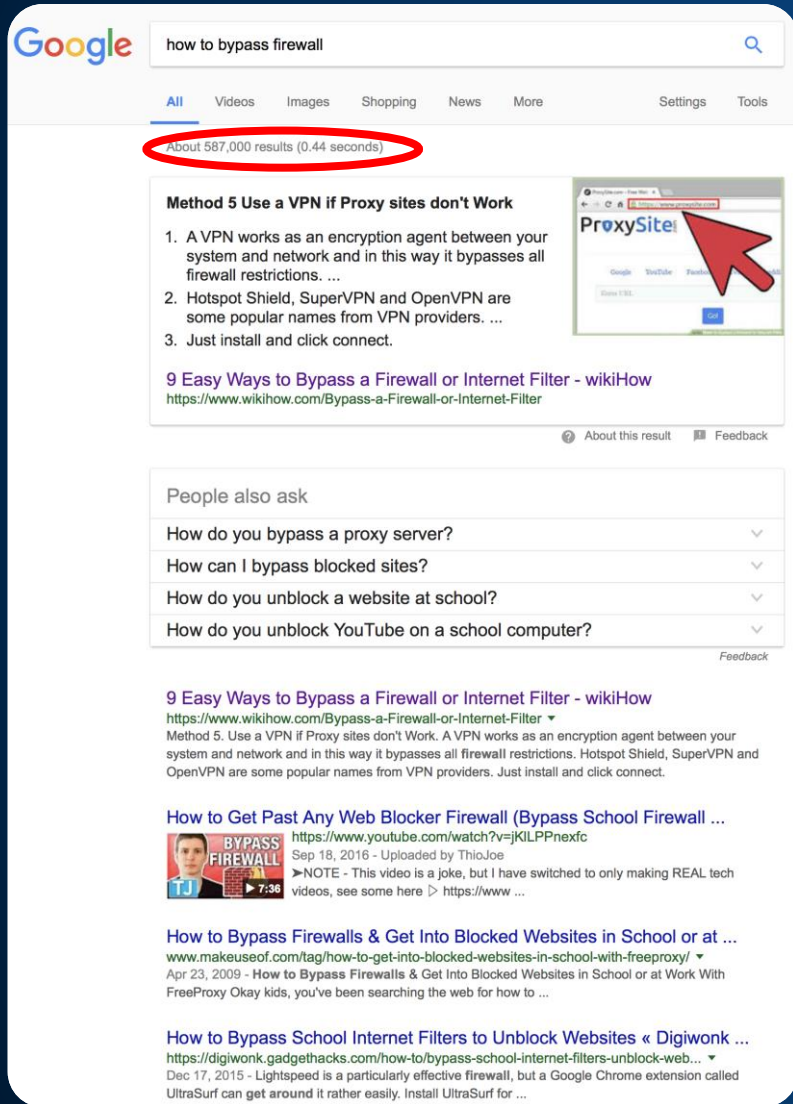
Games

(Valve and Steam)

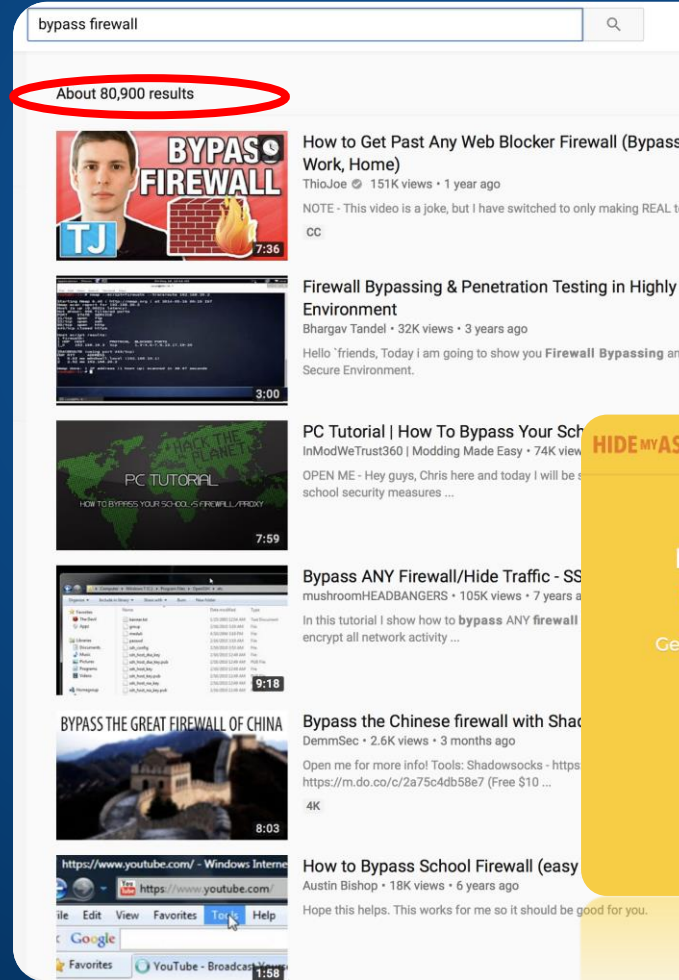


악성 사용자 – 방화벽의 제어를 회피중인

사용자, 어플리케이션, 심지어 멀웨어가 탐지를 회피하는 방법



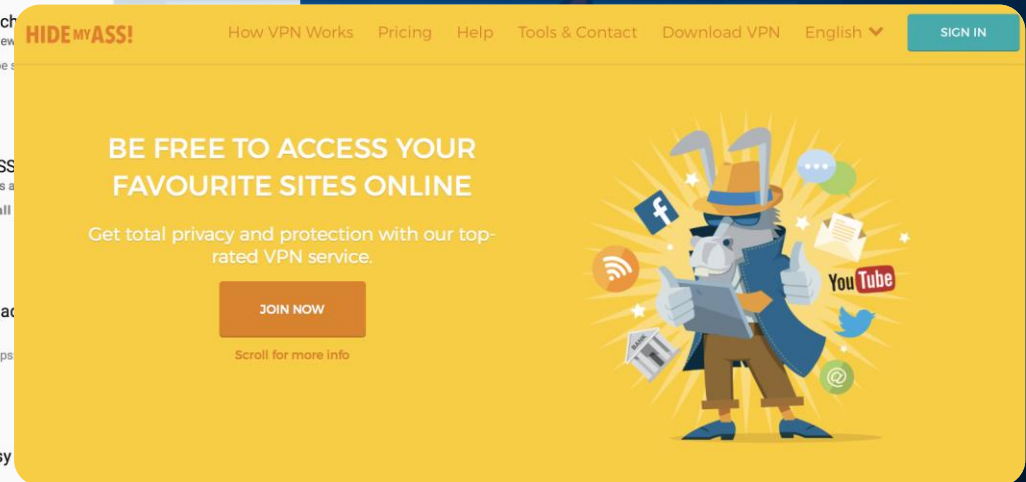
Google search results for "how to bypass firewall". The search bar shows "how to bypass firewall" and the results are filtered by "All". A red circle highlights the result count: "About 587,000 results (0.44 seconds)". The first result is "Method 5 Use a VPN if Proxy sites don't Work" with a list of steps. A red arrow points to a "ProxySite" link. Below this is a "9 Easy Ways to Bypass a Firewall or Internet Filter - wikiHow" result. Further down, there are "People also ask" questions and more search results, including "How to Get Past Any Web Blocker Firewall (Bypass School Firewall ...)" and "How to Bypass Firewalls & Get Into Blocked Websites in School or at ...".



YouTube search results for "bypass firewall". The search bar shows "bypass firewall" and the results are filtered by "All". A red circle highlights the result count: "About 80,900 results". The first result is "How to Get Past Any Web Blocker Firewall (Bypass Work, Home)" by ThioJoe. Below this is "Firewall Bypassing & Penetration Testing in Highly Secure Environment" by Bhargav Tandel. Further down, there are "PC Tutorial | How To Bypass Your School Firewall" and "Bypass ANY Firewall/Hide Traffic - SS". At the bottom, there is a "BYPASS THE GREAT FIREWALL OF CHINA" video.

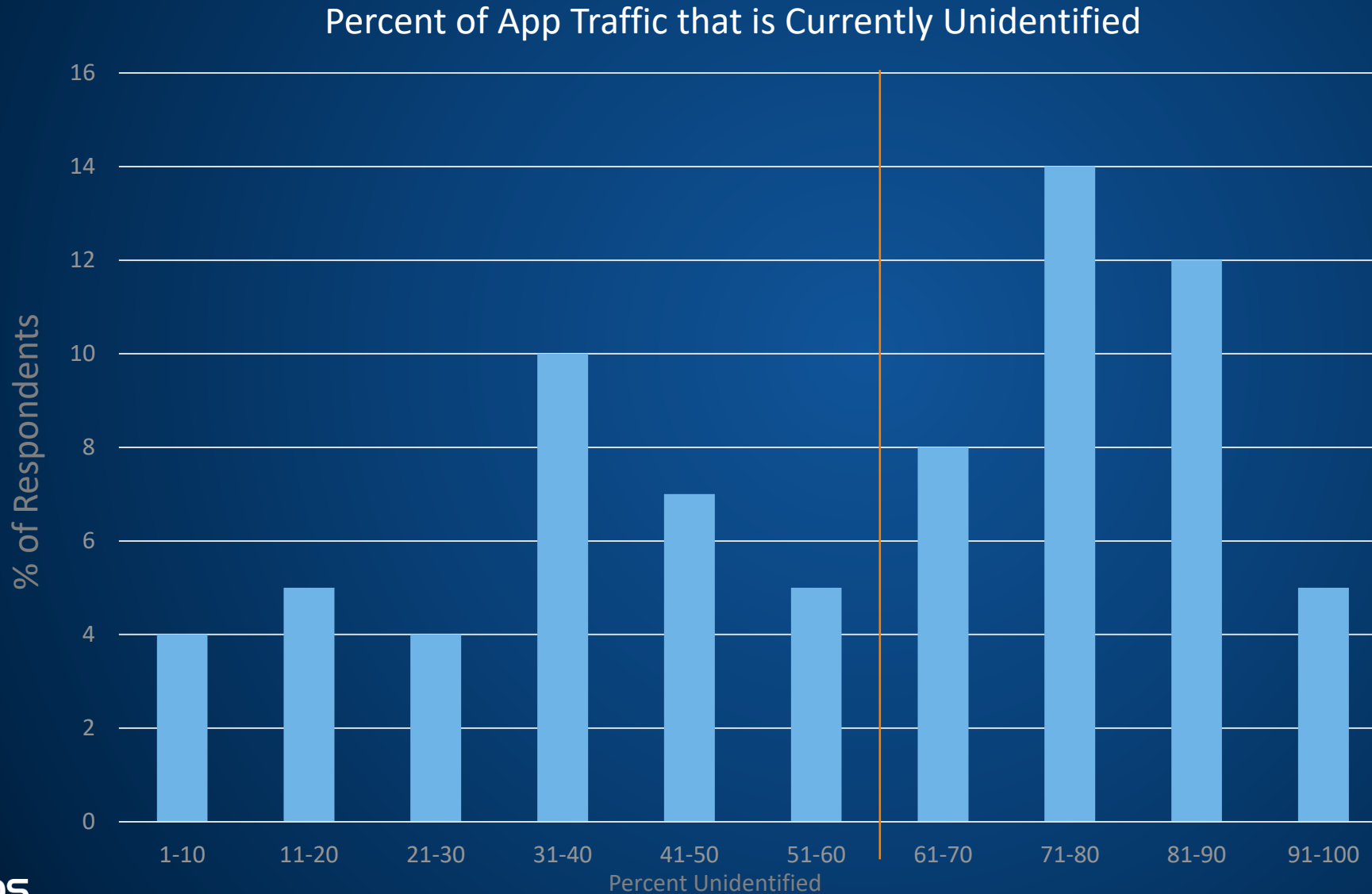


Hotspot Shield website interface. The top section is blue with the Hotspot Shield logo. Below this is a red banner with the word "UNPROTECTED" and a green "CONNECT" button. A large red arrow points from the "CONNECT" button towards the right. Below the banner is a blue section with the text "Welcome to Hotspot Shield" and "Hotspot Shield Elite is ad-free and more". There are links for "Sign In" and "Take a Tour". The bottom section is blue with the text "wikiHow to Bypass a Firewall or Internet Filter".



HIDEmyASS! website interface. The top section is yellow with the HIDEmyASS! logo and navigation links: "How VPN Works", "Pricing", "Help", "Tools & Contact", "Download VPN", "English", and "SIGN IN". Below this is a large yellow section with the text "BE FREE TO ACCESS YOUR FAVOURITE SITES ONLINE" and "Get total privacy and protection with our top-rated VPN service." There is a "JOIN NOW" button and a "Scroll for more info" link. On the right side, there is a cartoon illustration of a person wearing a hat and holding a laptop, surrounded by social media icons like Facebook, Twitter, and YouTube.

이것이 얼마나 큰 문제인가요?



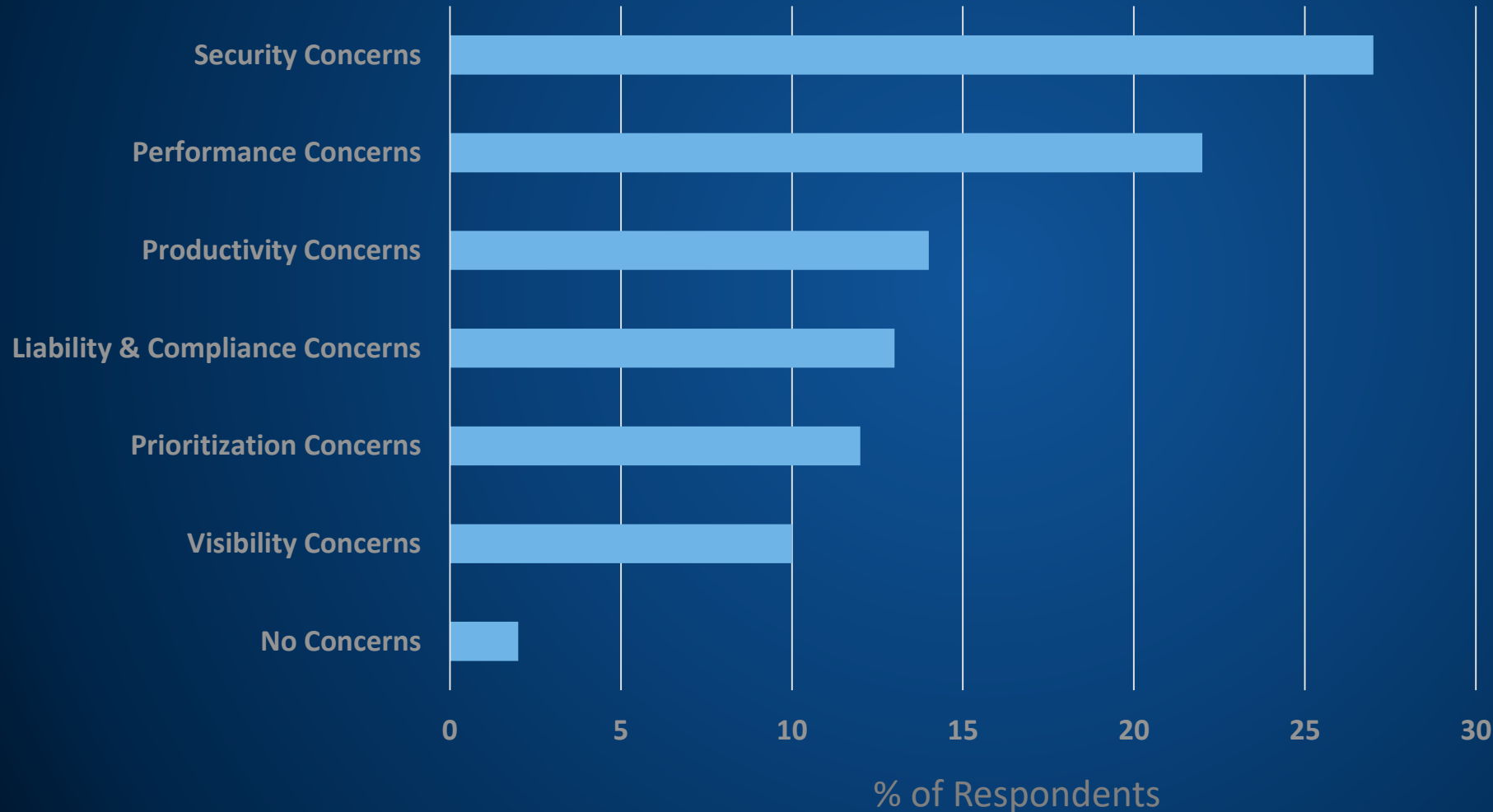
평균 트래픽의

60%
가 인식되지 않음

80%
의 트래픽을
방화벽의 ¼이
분류하지 못함

Top Concerns

어플리케이션 가시성의 부족으로 인한 Concerns



99%
의 관리자가 동의

54%
의 관리자는 염려중

Retake control of your network

Synchronized Application Control

What Firewalls See Today

SOPHOS
ED Firewall

MONITOR & ANALYZE
Control Center
Current Activities
Reports
Logs
Diagnostics

PRODUCT
Firewall
Intrusion Prevention
Web
Applications
Email
Web Server
Advanced Threat
Synchronized Security

COMPONENTS
VPN
Network
Routing
Authentication
System Services
EXTENSIVE
Profiles
Hosts and Services
Administration

Applications

Log Viewer Help Admin
Tools

Application List	Application Filter	Traffic Shaping Default	Enhanced Application Control
------------------	--------------------	-------------------------	------------------------------

Enhanced Application Control

On this page you can and modify application details for applications discovered with Synchronized Security from Sophos managed devices. You can change the name and category for the applications, information for some applications is already provided automatically from Sophos. You can use these applications in the overall application control feature on ED Firewall or you can directly enable the discovered applications to application filters to control the applications.

New Applications					
APPLICATION	STATUS	ENDPOINTS	OCCURRENCES	LAST OCCURRENCE	MANAGE
 Puget	✓	Found on 12 Endpoints	12	2018-10-22T16:44	Modify
 Dropbox Desktop	✓	Found on 6 Endpoints	34	2018-10-22T16:42	Modify
		ther.corp	2	2018-10-22T16:42	
		heindall.corp	8	2018-10-22T16:30	
		treja.corp	10	2018-10-22T14:20	
		hodor.corp	10	2018-10-22T14:15	
		lali.corp	2	2018-10-22T12:20	
		fggg.corp	2	2018-10-22T09:30	
 Evernote Desktop	✓	Found on 3 Endpoints	17	2018-10-22T16:36	Modify

What Synchronized App Control Sees

오늘날의 어플리케이션 제어문제를 해결할 솔루션

1

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

100%

어플리케이션 식별 및 제어

2

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



소포스는 이 레벨의 가시성을 제공하는 유일한 벤더

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

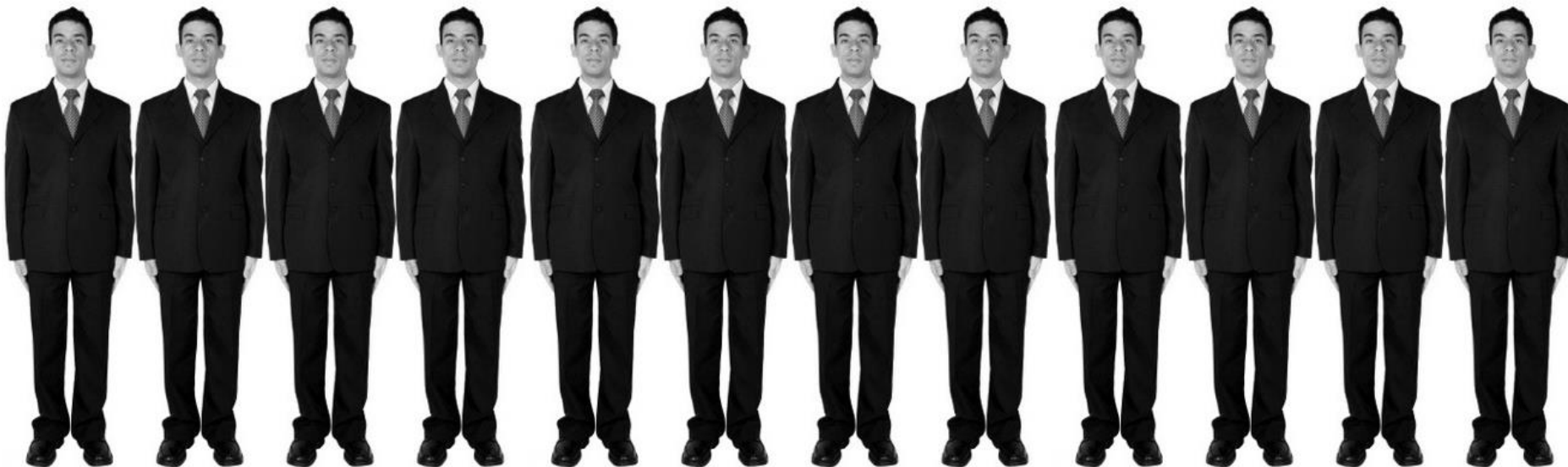
The screenshot displays the Sophos XG Firewall web interface. On the left is a navigation menu with sections: MONITOR & ANALYZE (Control Center, Current Activities, Reports, Diagnostics), PROTECT (Firewall, Intrusion Prevention, Web, Applications, Wireless, Email, Web Server, Advanced Threat), CONFIGURE (VPN, Network, Routing, Authentication, System Services), and SYSTEM (Profiles). The 'Current Activities' section is active, showing 'Live Users' with 9 concurrent users. A table lists users with checkboxes, User ID, and Username. A dropdown menu is open, listing various authentication methods: Authentication Agent (checked), Web Client, SSO, Clientless, L2TP VPN, IPsec VPN, PPTP VPN, Thin Client, SSL VPN Tunnel, NTLM Client, Android Client, iOS Client, iOS Web Client, Android Web Client, Radius SSO, API, and WiFi SSO. On the right, there are tabs for 'Ipssec Connections' and 'Remote Users'. The 'Remote Users' tab is active, showing a table with columns: Family, MAC, Start Time, and Upload. A 'Disconnect' button is visible.

User ID	Username
14	chrismobile
22	chrisipadm
15	mindyipad
16	mindymobile
17	xuxin
18	xuxinmobile
19	xuxinimac
12	serveradmin
9	chris

Family	MAC	Start Time	Upload
4	-	2017-03-08 23:45	0.00 KB
4	-	2017-03-08 23:45	44636.78 KB
4	-	2017-03-08 23:45	1952.41 KB
4	-	2017-03-08 23:45	1153.64 KB
4	-	2017-03-08 23:45	0.00 KB
4	-	2017-03-08 23:45	0.00 KB
4	-	2017-03-08 23:45	0.00 KB
4	-	2017-03-08 11:48	64770.92 KB
4	-	2017-03-08 11:53	151686.95 KB

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

현재 방화벽들은 사용자를 다음처럼 식별

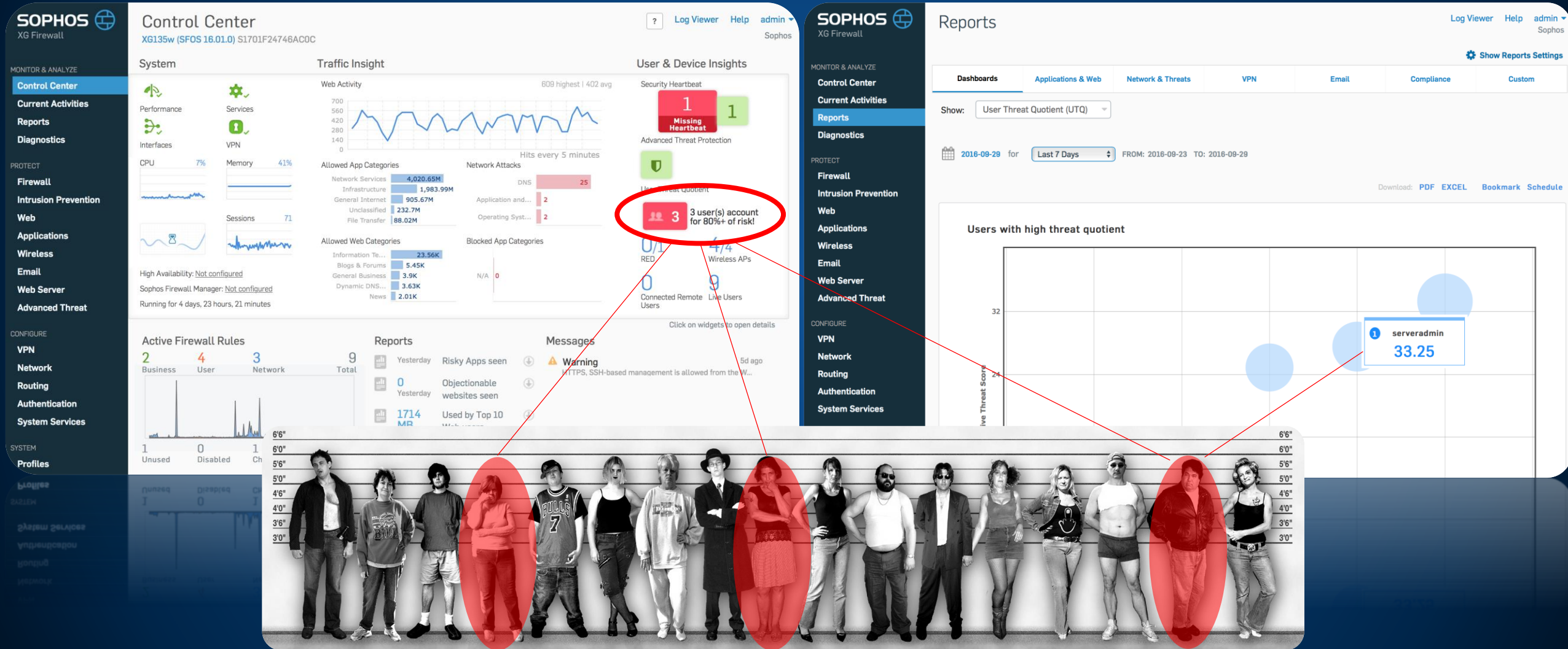


실제로는, 사용자는 이것보다도 다양합니다.

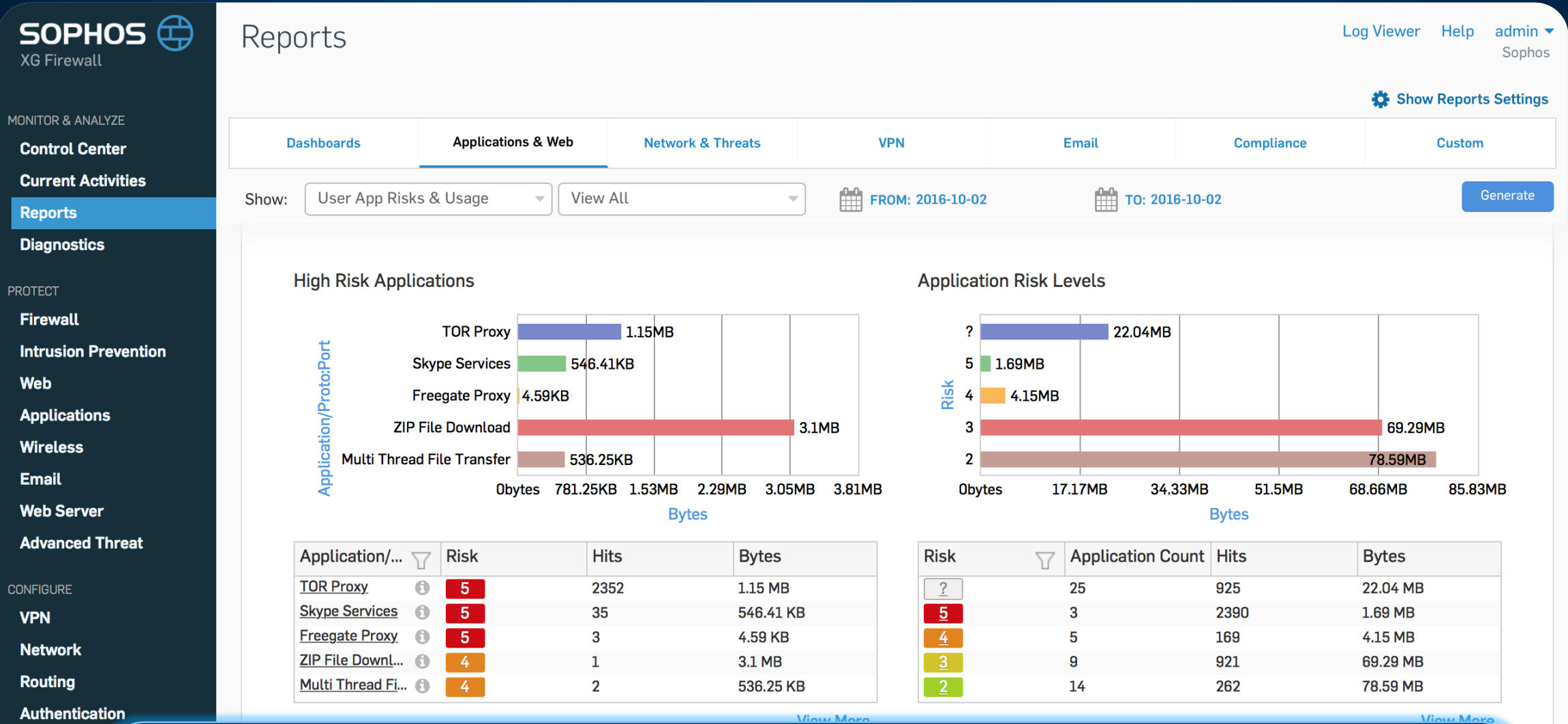


문제가 발생되기전 위험을 식별

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

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

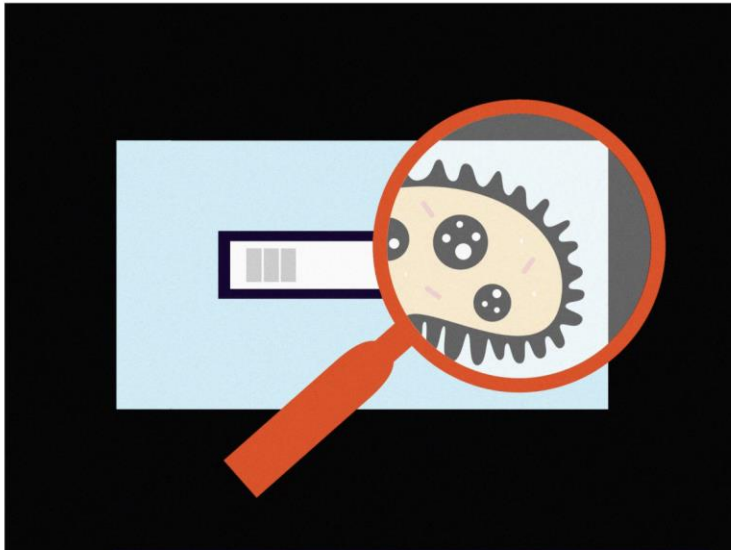


스팸과 오피스 문서로 전달되며,
네트워크를 걸쳐 전파됩니다.
아웃룩 데이터나 개인정보를
가로채 계좌에 접근하기위한
페이로드를 전달합니다.

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



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 might not want to go 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

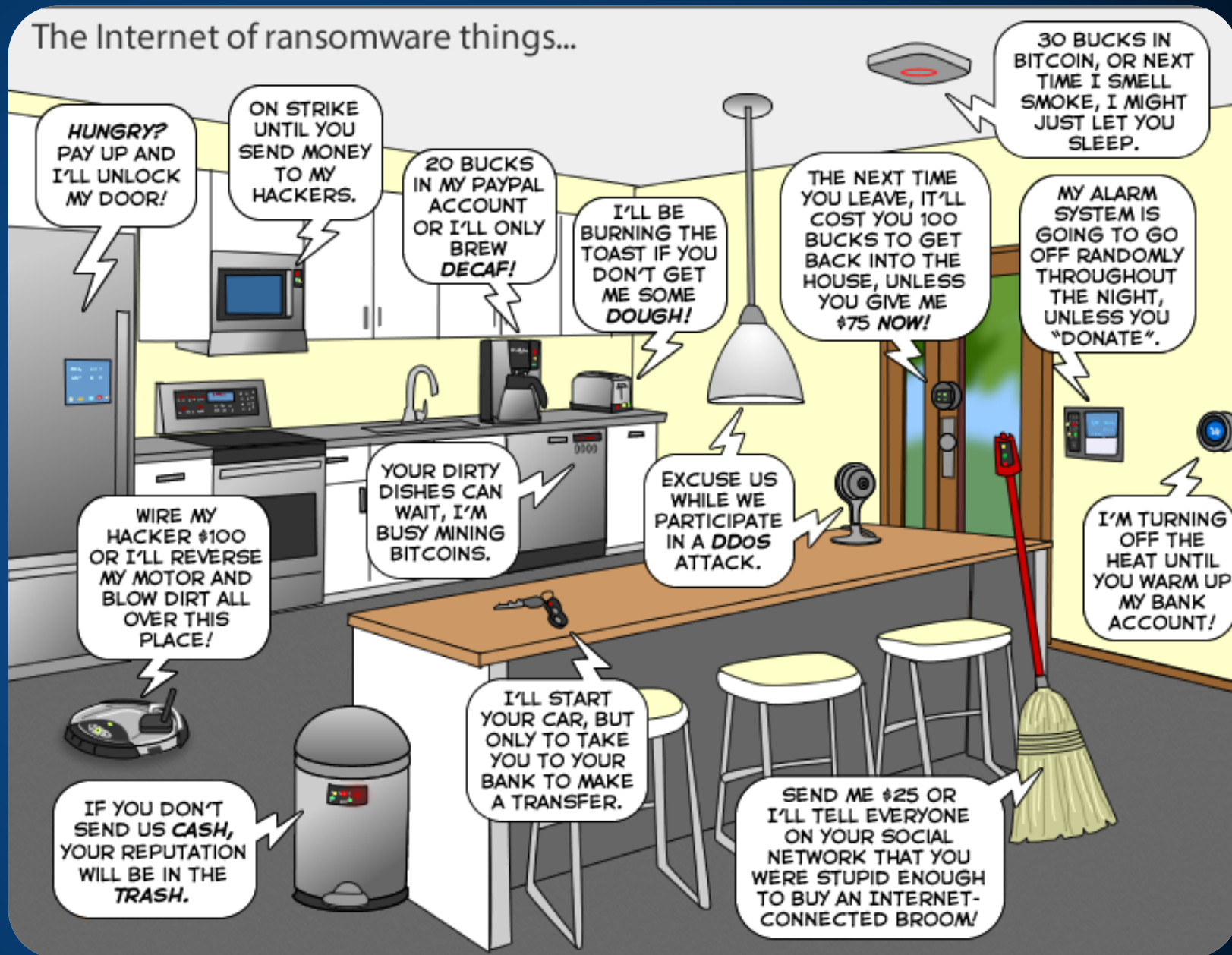


56 shares



What's Next?

IoT Ransomware?



Data Science + 소포스 랩=

자신있는 적극적인, 공격적인 탐지



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

Malware Scanning

- ☒ Scan HTTP
- ☒ Decrypt & Scan HTTPS
- ☒ Detect zero-day threats with Sandstorm
- ☒ Scan FTP

Advanced

User Applications

Intrusion Prevention

LAN TO WAN

Traffic Shaping Policy

User's policy applied

Web Policy

Default Workplace Policy

☐ Apply Web Category based Traffic Shaping Policy

Application Control

Block very high risk (Risk Level 5) apps

☐ Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

- ☒ GREEN ☐ YELLOW ☐ No Restriction
- ☐ Block clients with no heartbeat

Minimum Destination HB Permitted:

- ☐ GREEN ☐ YELLOW ☒ No Restriction
- ☐ Block request to destination with no heartbeat

NAT & Routing

☒ Rewrite source address (Masquerading)

☐ Use Gateway Specific Default NAT Policy

Use Outbound Address

MASQ
MASQ (Interface Default IP)

Primary Gateway

WAN Link Load Balance

Backup Gateway

None

DSCP Marking

Select DSCP Marking



간결하고 강력한 XG Firewall의 하나의 룰 설정

A full suite of technologies easily managed from a single screen

The screenshot displays the 'Malware Scanning' and 'Advanced' configuration sections of the Sophos XG Firewall. The interface is clean and organized, with various settings grouped into sections. Blue lines with circular endpoints point from descriptive labels to specific configuration options.

Malware Scanning

- ☒ Scan HTTP
- ☒ Decrypt & Scan HTTPS
- ☒ Detect zero-day threats with Sandstorm
- ☒ Scan FTP

Advanced

User Applications

- Intrusion Prevention: LAN TO WAN
- Traffic Shaping Policy: User's policy applied
- Web Policy: Default Workplace Policy
- ☐ Apply Web Category based Traffic Shaping Policy
- Application Control: Block very high risk (Risk Level 5) apps
- ☐ Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

- ☒ GREEN
- ☐ YELLOW
- ☐ No Restriction
- ☐ Block clients with no heartbeat

Minimum Destination HB Permitted:

- ☐ GREEN
- ☐ YELLOW
- ☒ No Restriction
- ☐ Block request to destination with no heartbeat

NAT & Routing

- ☒ Rewrite source address (Masquerading)
- ☐ Use Gateway Specific Default NAT Policy
- Use Outbound Address: MASQ
- MASQ (Interface Default IP)
- Primary Gateway: WAN Link Load Balance
- Backup Gateway: None
- DSCP Marking: Select DSCP Marking

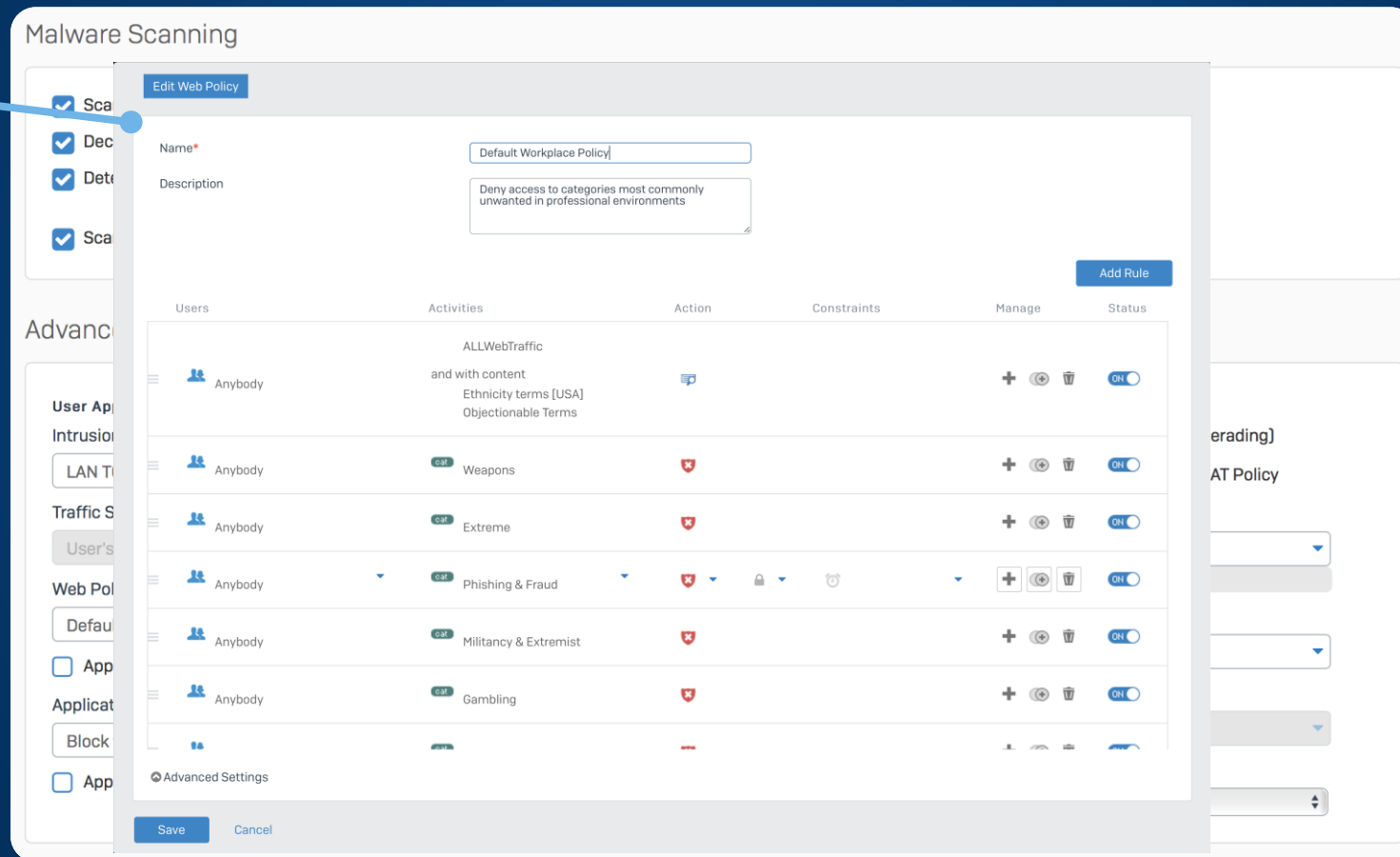
Labels and Callouts:

- Dual AV
- SSL Inspection
- Sandboxing
- IPS
- QoS
- Web Filtering
- App Control
- Heartbeat
- NAT
- Routing
- Prioritization

간결하고 강력한 XG Firewall의 하나의 룰 설정

*IPS, Web, App Control and Traffic-Shaping and Edit-in-place*을 위한 스냅인 정책

Edit-in-place



Sophos is the only vendor providing this level of integration

Sandstorm Deep Threat Prevention

zero day 위협으로 부터 가장 안전하게

Deep Memory Analysis

01010000101001010011
10011010010000001010
01010010010010010100

초기 및 실행 이후
메모리 감지 및
분석

적극적이고 빈번한
런타임 분석

Deep Behavioural Analysis



Sandbox 회피 기술,
API & File 시스템
동작

Intercept X 취약점
공격 탐지와
크립토가드 엔진

Deep Network Analysis



모든 포트와
프로토콜을 분석

IPS detections
추가예정

Deep Learning Analysis



보내진 모든
실행파일들 분석

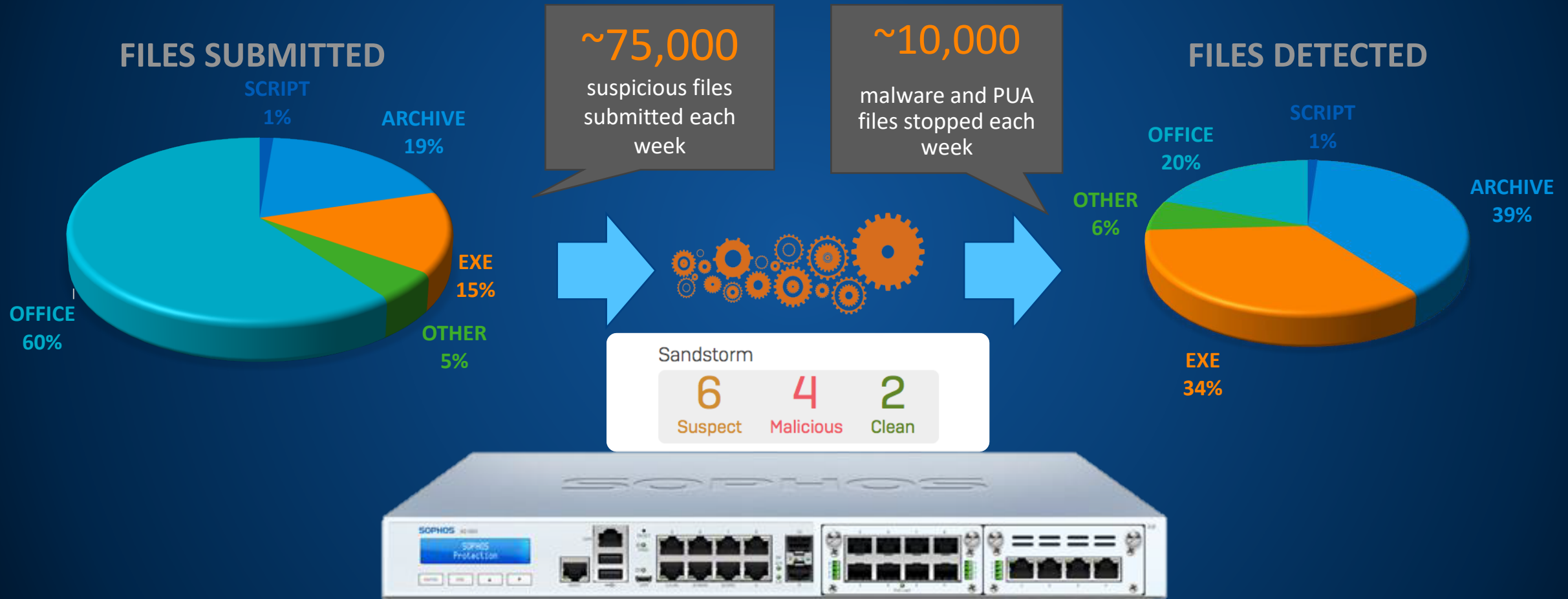
지속적 적응 학습
모델

Sophos Labs의 실시간 위협 인텔리전스

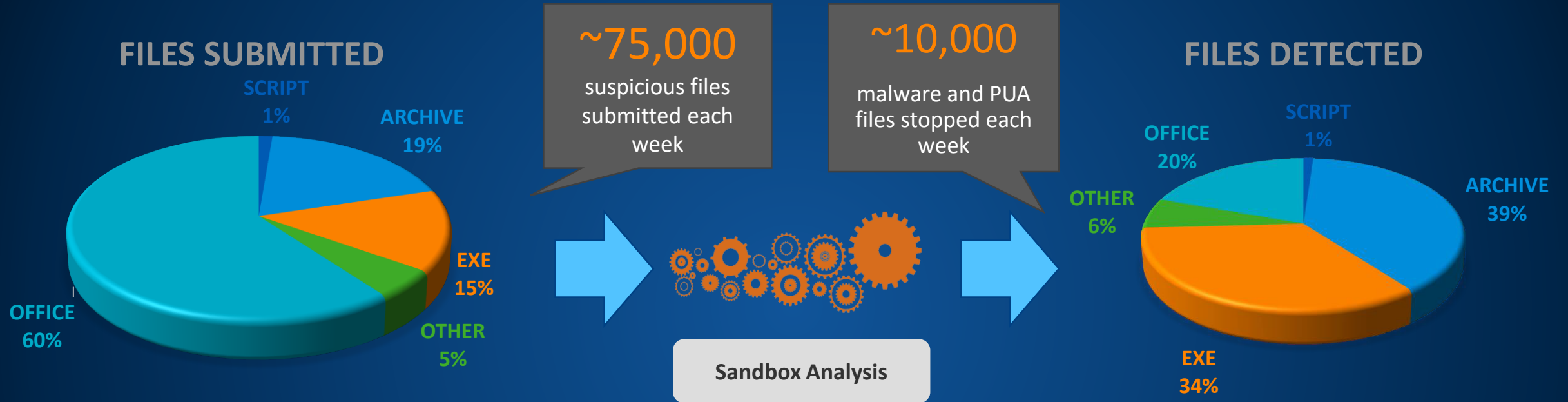


Sandstorm의 보호력은 엔드포인트와 방화벽을 뛰어넘습니다

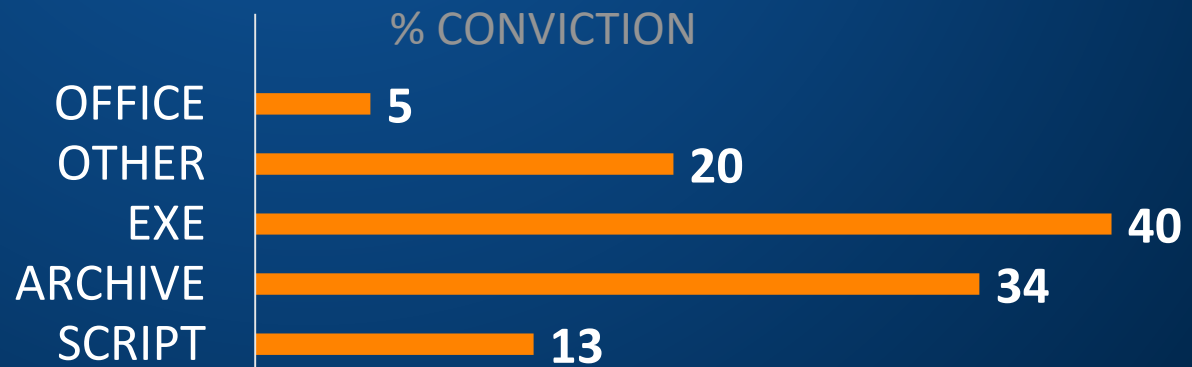
이전 보다 더 높아진 보호 – Powered by Deep Learning



파일 유형 분류



파일 타입별 멀웨어 호근
PUA로 식별되고 차단된
제출된 파일 비율

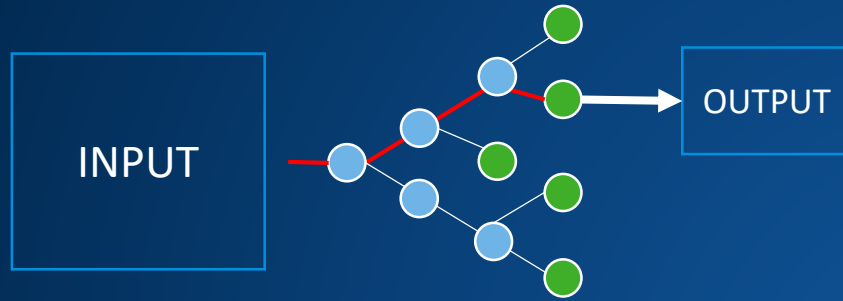


행위적인 탐지 + 딥러닝 (Deep learning)



Machine learning Vs. deep learning

MACHINE LEARNING

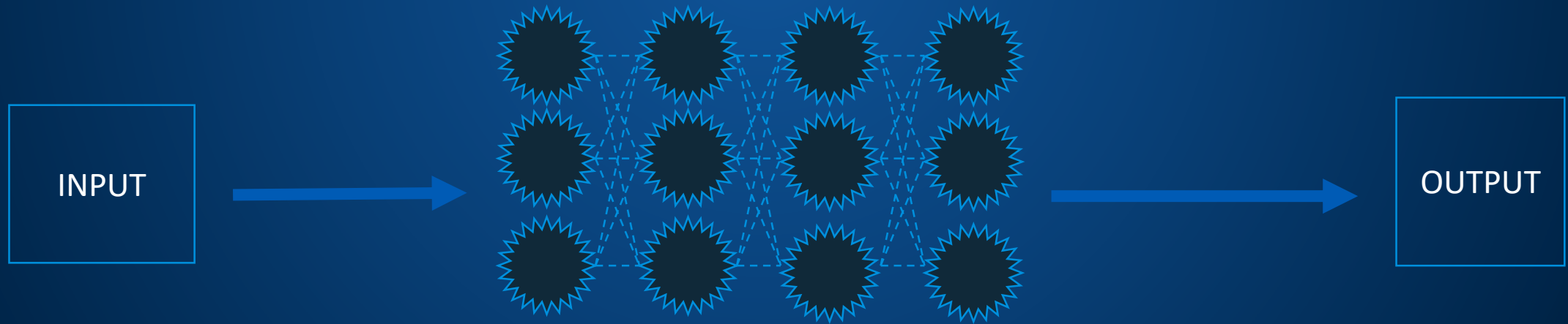


Decision Tree



Random Forest

DEEP LEARNING



Interconnected Layers of Neurons, Each Identifying More Complex Features

Sophos deep learning advantages

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

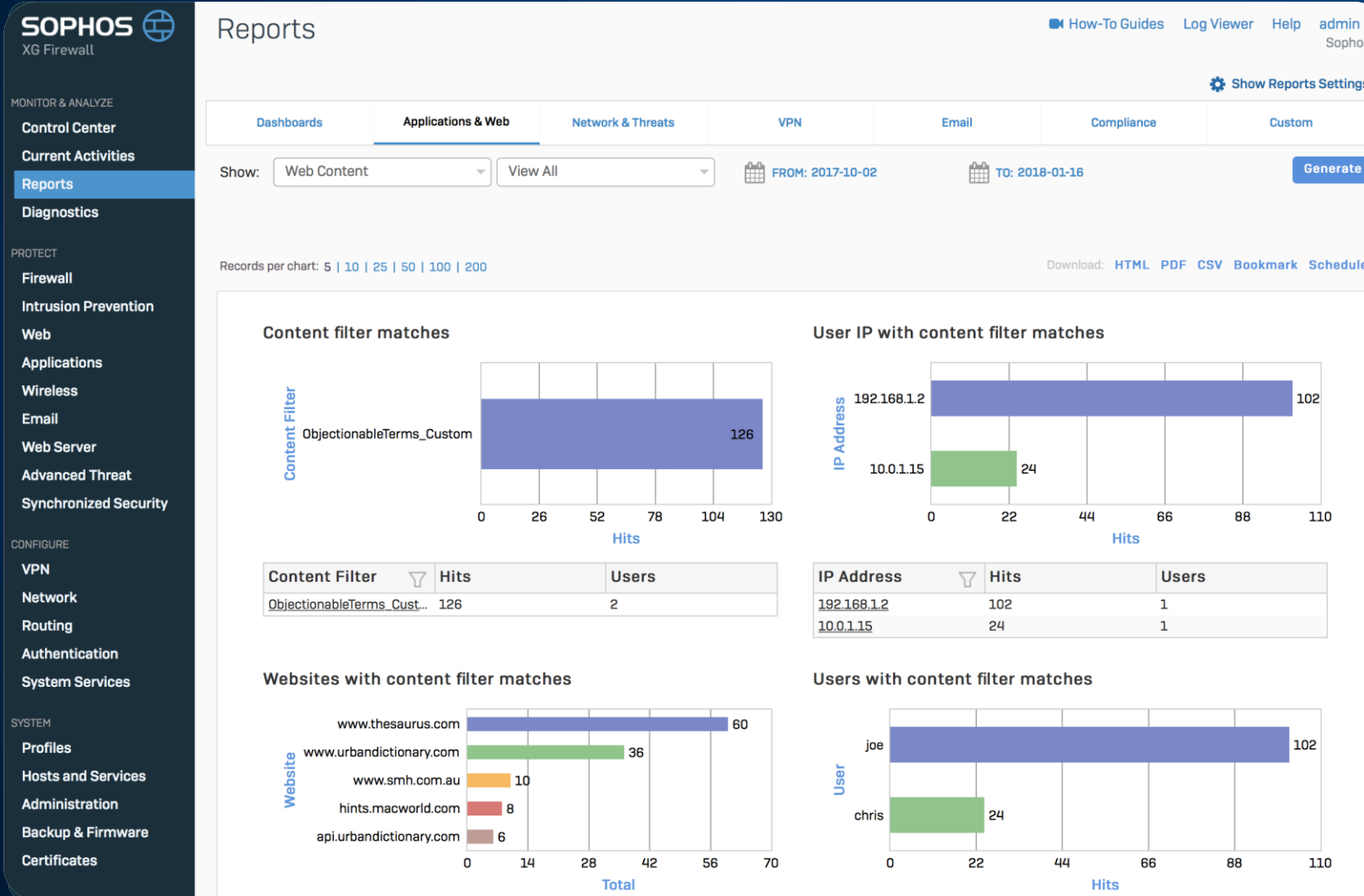
“ One of the *best performance scores* we have ever seen in our tests ”

Maik Morgenstern, CTO, AV-TEST



Web Content Filtering (v17)

Enabling child safety in education



동적 콘텐츠 모니터링과 필터링

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

JavaScript CryptoJacking 보호

단지 한번의 클릭으로


XG Firewall

MONITOR & ANALYZE

Control Center

Current Activities

Reports

Diagnostics

PROTECT

Firewall

Intrusion Prevention

Web

Applications

Wireless

Email

Web Server

Advanced Threat

Synchronized Security

CONFIGURE

VPN

Network

Routing

Authentication

Web

How-To Guides Log Viewer Help Demo User ▼
Sophos Inc

Policies User Activities Categories URL Groups Exceptions General Settings File Types Surfing Quotas User Notifications Content Filters

XG Firewall protects you by scanning HTTP and HTTPS traffic for unwanted content or malware, and enforcing SafeSearch restrictions. Use this page to modify protection settings, as well as settings for the proxy and web cache.

Protection

Malware and Content Scanning

Scan Engine Selection

Single Engine (Optimal Performance)

Single scan engine is set to [Sophos](#).

Sandstorm and content filters require use of the Sophos engine, either as the single scan engine or in Dual Engine mode.

Scanning Mode

Batch (Maximum Protection)

Real-time mode improves performance by allowing parts of a file to be downloaded before the scan is complete.

Action on Malware Scan Failure

Block (Best Protection)

Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats.

Do not scan files larger than

10 MB

Authorized PUAs

Search / Add

+

Block potentially unwanted applications

Protect users against downloading potentially unwanted applications. For more information about PUAs, please refer to the [Sophos website](#).

Advanced Settings ▲

Policy Test Simulator

Making troubleshooting quicker and easier

Log Viewer

Policy Test

Connection Details

URL

playboy.com

User

☐ Authenticated User

cmac

Time and Day

20 : 02 Thursday

Test Method

Test Web Policy

Web Policy

Default Workplace Policy

Clear

Test

Connection

Test Time

Destination

Destination IP

User

Result

Web Protection

Category

Web Policy

Matched Web Rule

20:02:46 Thursday

http://playboy.com

204.74.99.100, port 80, TCP

User Unauthenticated

Blocked

Sexually Explicit

Default Workplace Policy

Users	Activities	Action	Constraints
Anybody	Sexually Explicit		

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

Web Keyword Monitoring

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

The screenshot displays the Sophos XG Firewall Reports interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE' (Control Center, Current Activities, Reports, Diagnostics), 'PROTECT' (Firewall, Intrusion Prevention, Web, Applications, Wireless, Email, Web Server, Advanced Threat, Synchronized Security), 'CONFIGURE' (VPN, Network, Routing, Authentication, System Services), and 'SYSTEM' (Profiles, Hosts and Services, Administration, Backup & Firmware, Certificates). The main 'Reports' section has tabs for Dashboards, Applications & Web (selected), Network & Threats, VPN, Email, Compliance, and Custom. Under 'Applications & Web', the 'Web Content' report is selected. It shows filters for 'Web Content' and 'View All', with date ranges from 2017-08-28 to 2017-08-28. The report displays four tables, all showing 'No Record Found': 'Content filter matches', 'User IP with content filter matches', 'Websites with content filter matches', and 'Users with content filter matches'. The interface also includes options for 'Records per chart' (5, 10, 25, 50, 100, 200) and 'Download' (HTML, PDF, CSV, Bookmark, Schedule).

Dynamic Content Blocking

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

Benefits

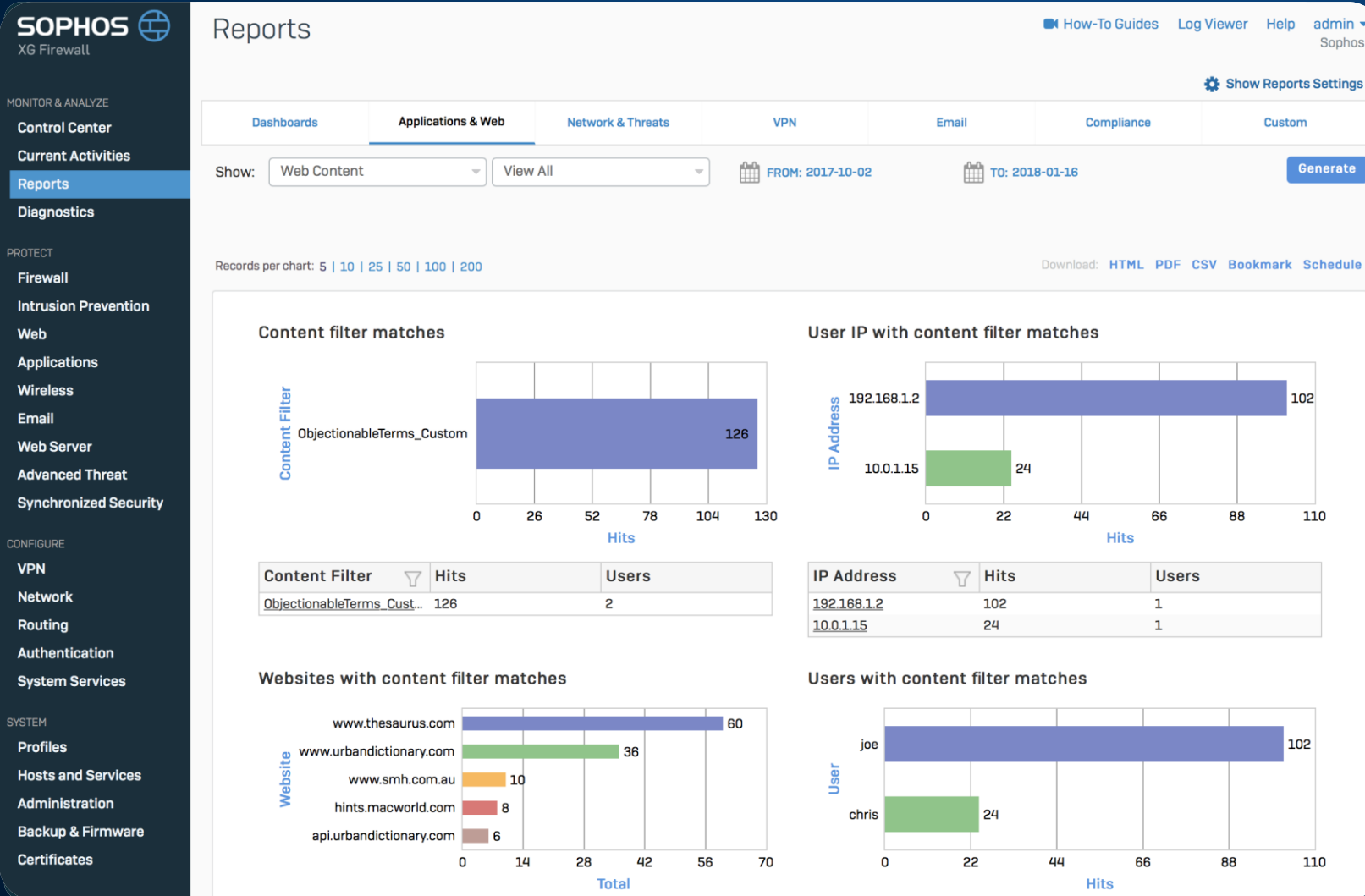
- Quickly identify signs of bullying, radicalization, abuse or self-harm before they become a problem
- A key requirement for the UK Education market
- Dynamically block websites based on content regardless of their category – block sites that otherwise might be allowed

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 콘텐츠 기반으로 웹사이트를 차단할 수 있습니다.

3. Automatically Respond to Incidents

3. 자동화된 사고 대응

Synchronized Security – 즉각적인 위협의 식별

장치 및 사용자를 향하는 위협을 즉시 확인

Control Center

XG230 [SFOS 17.1.0 Beta-1-OMC] C240773Y2QQXTCA

How-To Guides Log Viewer Help admin ▼
Sophos

System



Performance



Interfaces



Services



VPN

0/0

RED

0

Connected Remote Users

CPU 22%
Bandwidth 23KB/s

3/3

Wireless APs

10

Live Users

Memory 37%
Sessions 26

High Availability: Not configured

Sophos Firewall Manager: Not configured

Running for 1 day(s), 1 hour(s), 59 minute(s)

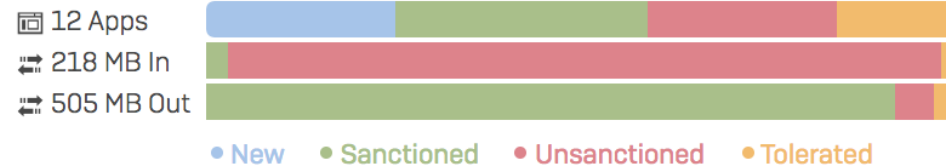
Traffic Insight

Web Activity

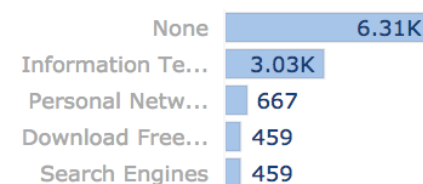
761 highest | 101 avg



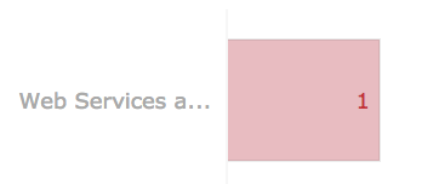
Cloud Applications



Allowed Web Categories



Network Attacks

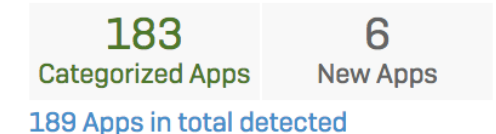


User & Device Insights

Security Heartbeat®



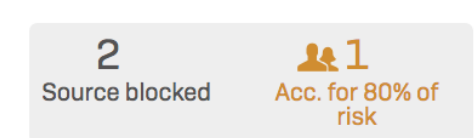
Synchronized Application Control™



Sandstorm



ATP



UTQ



Synchronized Security – 즉각적인 위협의 식별

Associating threats to a device and a user immediately

Control Center

XG135w [SFOS 16.05.1 MR-1] S1701F24746AC0C

?

Log Viewer

Help

admin ▾

Sophos

SYSTEM CPU & MEMORY NETWORK HEARTBEAT ATP RED ALERT CONNECTIONS & INTERFACES



Show: ☒ Missing ☒ Red ☒ Yellow ☐ Green

[Sophos Central](#)

Please refer to Sophos Central to remediate endpoint issues.

HOSTNAME, IP

USER

STATE CHANGED



Mac Server
10.0.1.10

Chris

4 minutes ago

Synchronized Security - 즉각적인 위협의 식별

Associating threats to a device and a user immediately

Control Center

XG135w [SFOS 16.05.1 MR-1] S1701F24746AC0C

Log Viewer Help admin ▼Sophos

SYSTEM CPU & MEMORY NETWORK HEARTBEAT ATP RED ALERT CONNECTIONS & INTERFACES

2
ATP Report

HOSTNAME, IP	THREAT	COUNT
Mac Server 10.0.1.10	C2/Generic-A /Users/Chris/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2
10.0.1.11 Unknown Hostname	C2/Generic-A /Users/Joe/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2

Reset

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

XG Firewall

Sophos Central

XG Firewall

Security Heartbeat™

Endpoints

Internet

Servers

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

Instant Identification

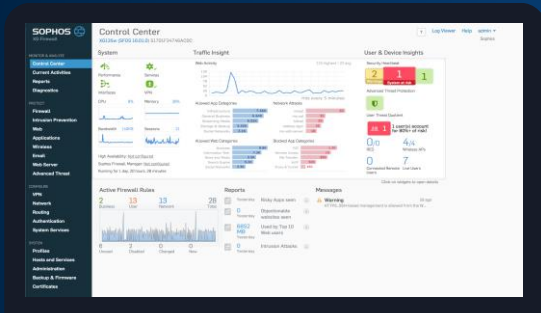
Security Heartbeat can instantly share telemetry about the user, systems and process responsible

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



Next-Gen
Firewall
and ATP

Synchronized
Security

UTM &
Deployment

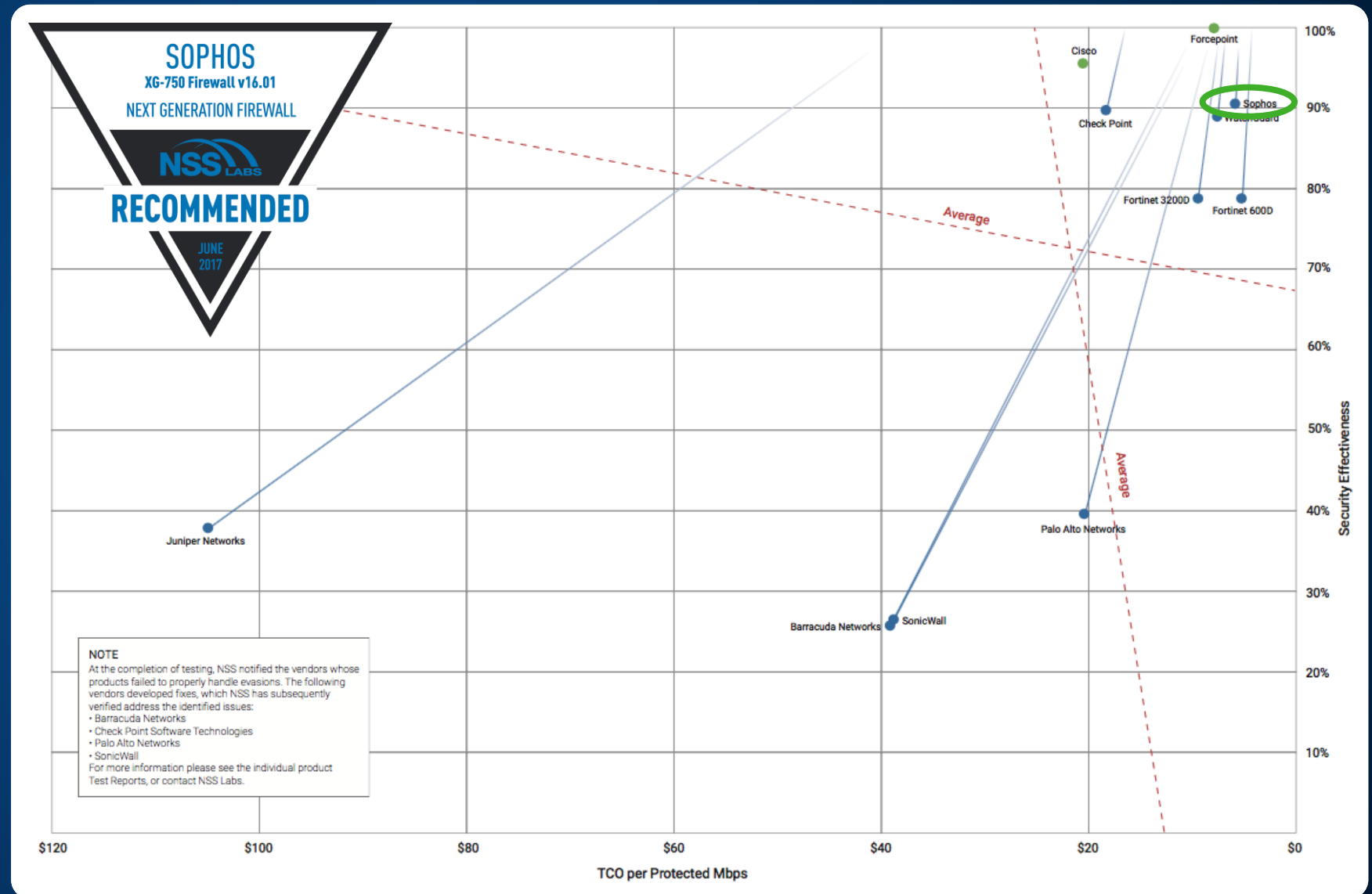
	Sophos XG Firewall	CheckPoint NGFW	WatchGuard Firebox	Fortinet FortiGate	SonicWALL NSA	Cisco Meraki
FastPath Packet Optimization	✓	✓		✓		
Dual AV Engines	✓					
IPS (NSS Recommended)	✓	✓	✓	✓		✓
Application Control	✓	✓	✓	✓	✓	✓ (partial)
Web Protection and Control	✓ +	✓	✓	✓	✓	✓
User and App Risk Assessment & Visibility	✓			✓ (partial)		
HTTPS Filtering	✓	✓	✓	✓	✓	✓
Advanced Threat Protection	✓	✓	✓	✓	✓	✓
Sandboxing	✓	✓	✓	✓	✓	✓
Identify Compromised Host, User, & Process	✓					
Compromised System Isolation	✓					
Unknown Application Identification	✓					
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

Top Rated by Industry Analysts

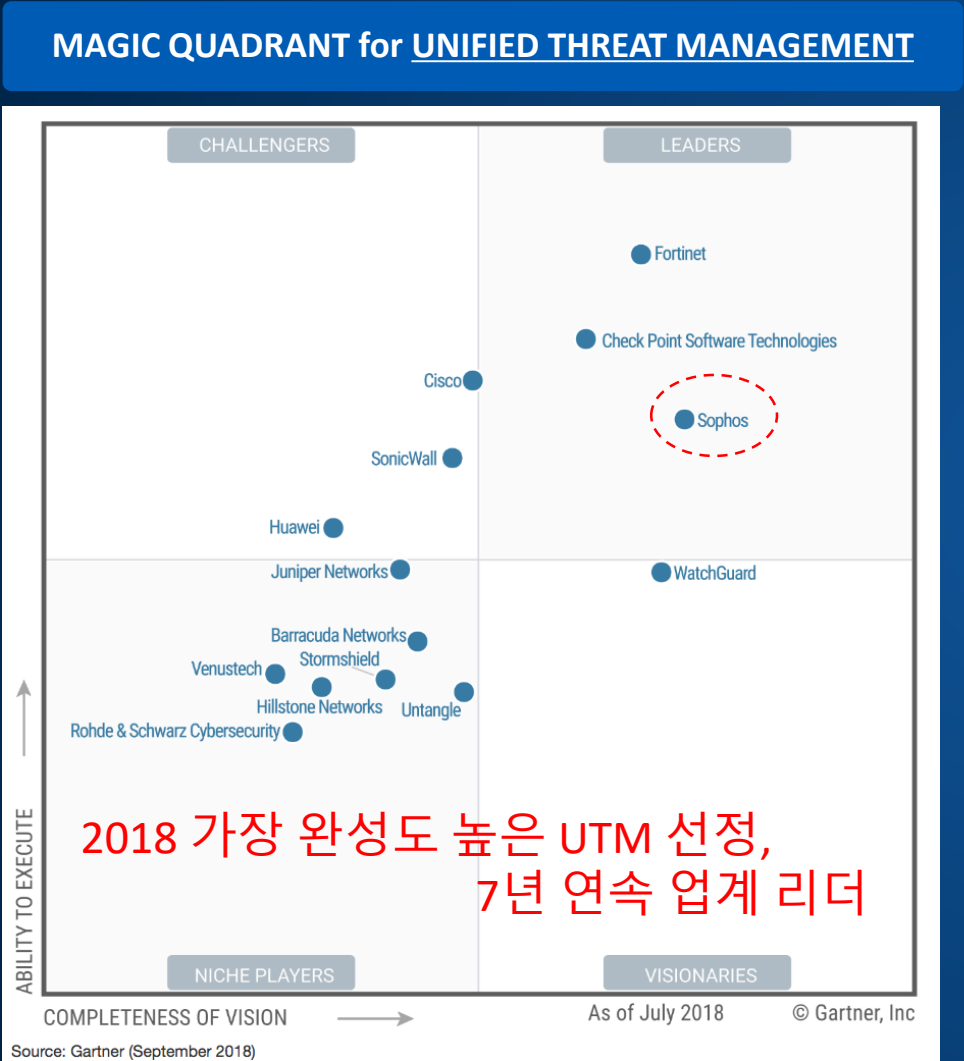
SOPHOS

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



2018년도 Magic Quadrant for Unified Threat Management,

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



2018년도 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.*

GROUP TEST UTM/SIEM/NGFW




Sophos XG Firewall

This product is a UTM that sells itself as a next-generation firewall. This was one that rather took us aback because we don't tend to think of UTM 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 includes 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 detection 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 UTM? We believe there is a very good case to be made for that. Time will tell, of course, but this is a marketplace that is certainly characterized by convergence.

— Peter Stephenson, technology editor

RATING BREAKDOWN

SC Lab Reviews
Reviews from our expert team

Features: ★★★★★	Documentation: ★★★★★	Value for Money: ★★★★★
Performance: ★★★★★	Support: ★★★★★	Ease of Use: ★★★★★

5/5

DETAILS

Vendor: Sophos
Product: XG Firewall
Website: sophos.com/AppFirewall
Price: Starting at \$249/year on a three-year term for TotalProtect Plus & Enhanced Support on an XG 885.

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 no downsides to cover no matter what requirements.

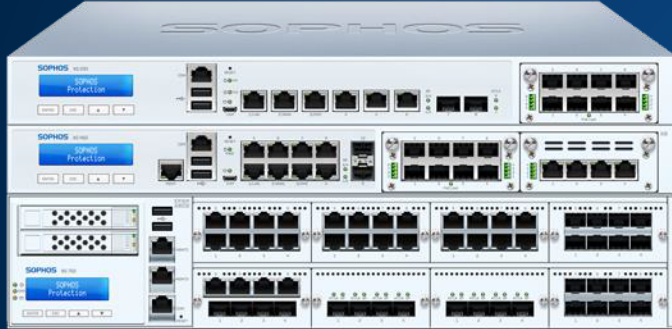
SOPHOS
Security made simple

Sophos
The Pinnacles, Abingdon Science Park
Abingdon OX14 3FP
United Kingdom
Toll Free: 1 866 866 2802 • Email: sales@sophos.com

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

타협이 없는 배포의 유연성

오늘날의 비즈니스에 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



Virtual/Software

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

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



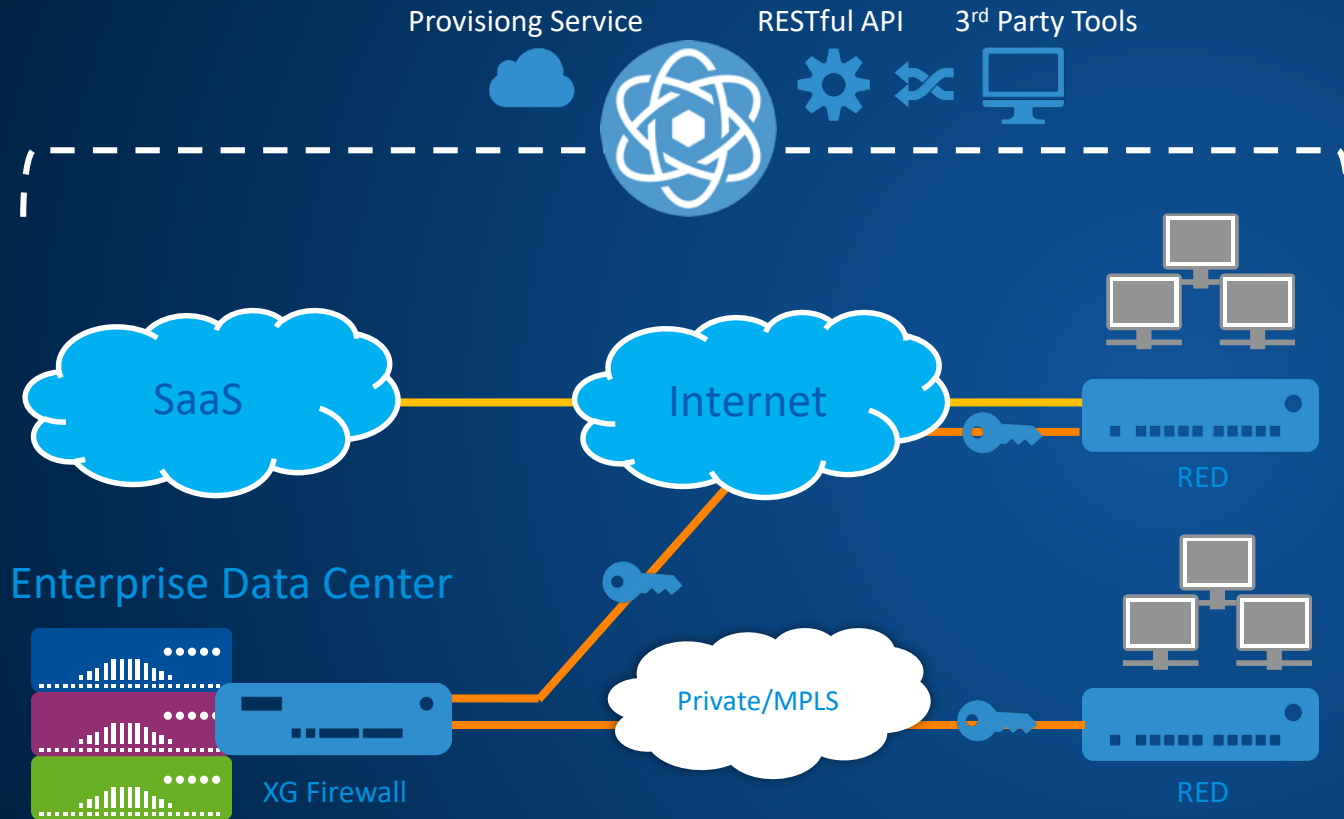
Sophos Firewall
Manager



Sophos iView

다수지점으로 분산된 환경 - Sophos RED

SD-WAN 구축시 고려 사항



Dynamic Path Selection

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



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

Three models:

- RED 15 / 15w and RED 50

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 다운로드



Sandboxing

Cryptojacking



가상화폐 마이닝을 수행하는
감염된 웹사이트들



Web Protection & PUAs

엔드포인트 격리 & Security Heartbeat

방화벽에서 자동시스템 격리

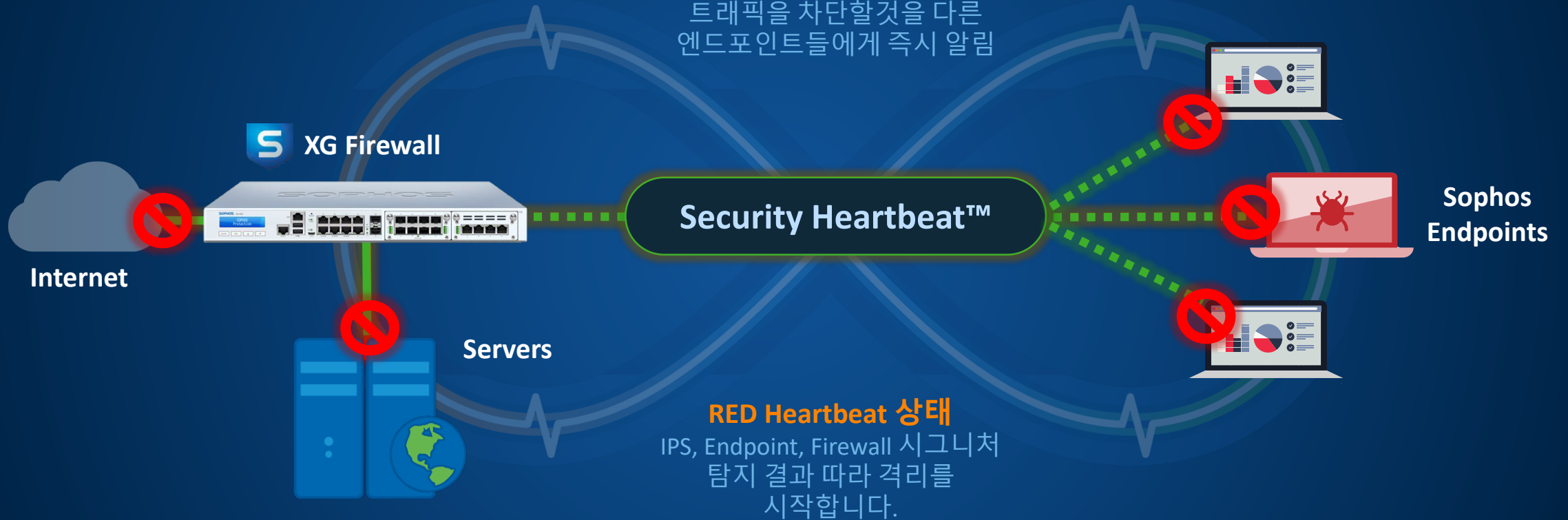


래터럴 무브먼트 보호

엔드포인트에서 자동으로 시스템 격리 - 동일한 네트워크에서도 적용

래터럴 무브먼트 보호

XG는 감염된 장치로부터의 모든 트래픽을 차단할것을 다른 엔드포인트들에게 즉시 알림

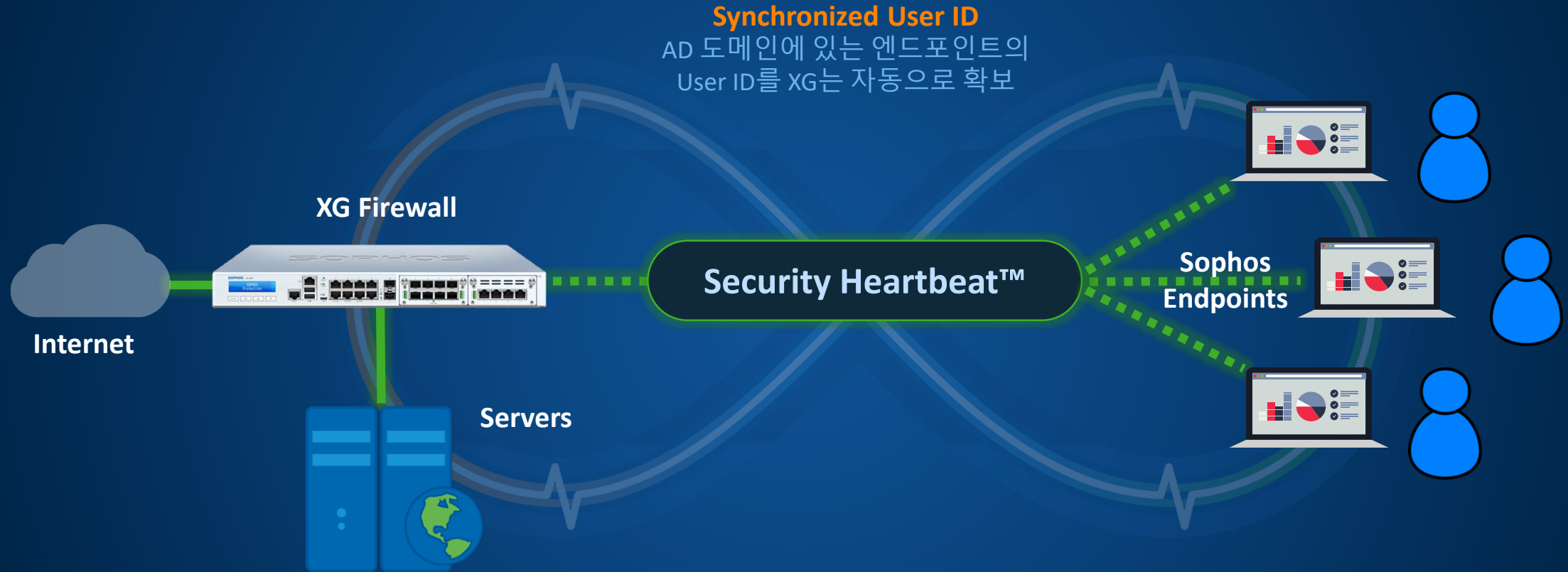


RED Heartbeat 상태

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

싱크로나이즈드 User ID

인증 에이전트 필요성 제거



AD 통합 없이도 전체 네트워크 유저 인식

IPS Enhancements

Enterprise pattern integration - Talos

새로워진 부분

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

SOPHOS XG Firewall

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion prevention**
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced threat
- Central Synchronization

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Profiles

Intrusion prevention

DoS attacks | **IPS policies** | Custom IPS si

Category: browser | Severity: | Platform: | Target: | Individual signature

SID	Category	Severity	Platform
2200304	Server-Webapp	2 - Major	Windows
9000495	Os-Windows	4 - Minor	Windows
9000496	Os-Windows	1 - Critical	Windows
1000070	Policy-Other	4 - Minor	

List of matching signatures [1 - 50 of 11206]

Action: Drop packet

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

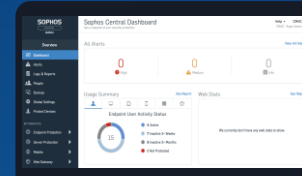


Device Access and Onboarding

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

Sophos Central Integration

Cloud Management and Reporting for XG Firewall

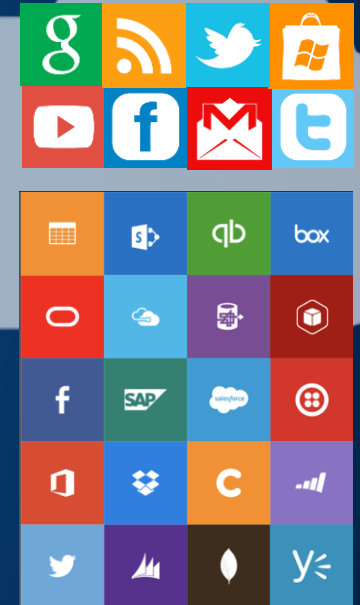


Server Health



CASB

Cloud Access Security Broker for visibility and control

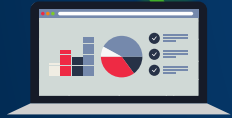


Endpoint Health



Endpoint Stonewalling

Prevent lateral movement even on the same network segment



Networking

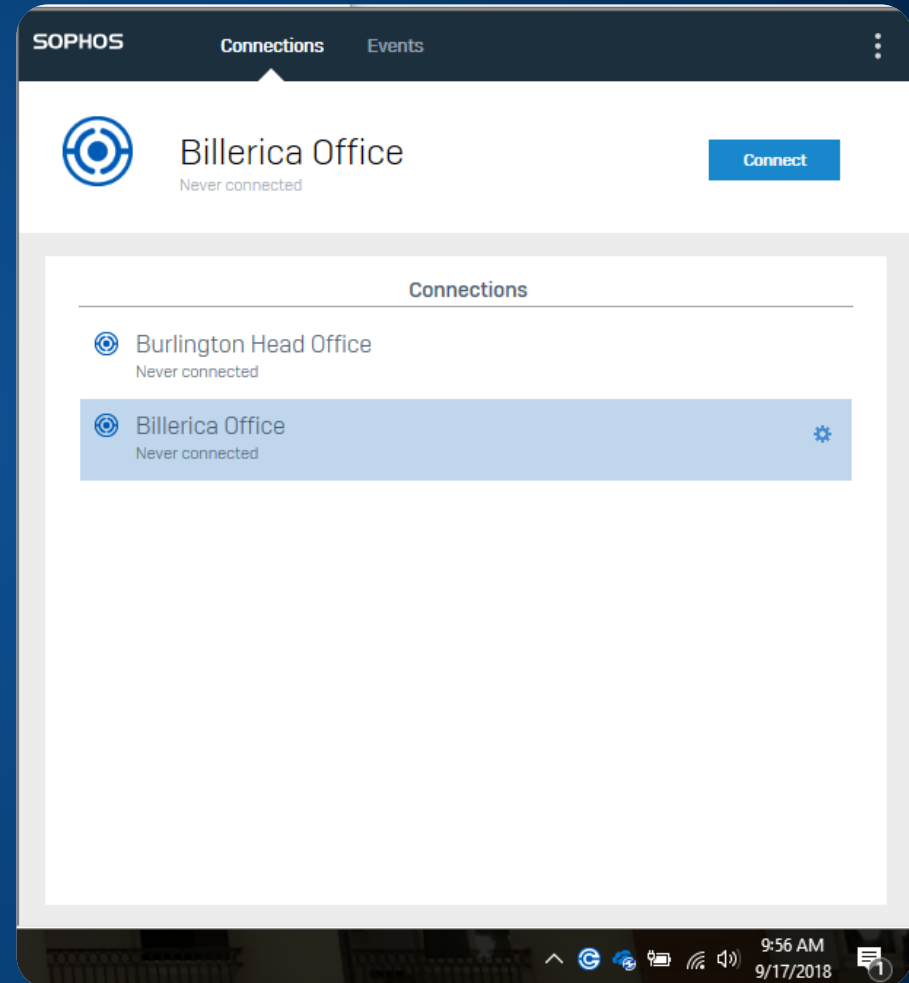
Synchronized Security via Remote VPN

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

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

Dialog box titled "Edit group" with a close button (X).

Group name *
Traffic to Internal Zones

Group description
To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis

Rule type
Any

Source zone
Any

Add new item

Destination zone
LAN
DMZ
VPN
WiFi

Add new item

Cancel Update

Firewall Rule Management

Solving the problem of managing large rule sets

SOPHOS XG Firewall

MONITOR & ANALYZE

Control Center

Current Activities

Reports

Diagnostics

PROTECT

Firewall

Intrusion Prevention

Web

Applications

Wireless

Email

Web Server

Advanced Threat

Synchronized Security

CONFIGURE

VPN

Network

Routing

Authentication

System Services

SYSTEM

Profiles

Hosts and Services

Administration

Backup & Firmware

Certificates

Firewall

IPv4 IPv6 Enable Filter

+ Add Firewall Rule

ID	Name	Source	Destination	What	Features
5	WAF Rules				Keep all my WAF rules together
22	8443 test	WAN, 198.144.101.88	DMZ, 10.104.203.5	8443 test, 8443(TCP)	AV WEB APP QoS HB RT NAT LOG IPS
19	reg-test-2	Any Zone, Any Host	#PortE3:1	reg-test-2.utmtools.com	IPS AV WEB APP QoS HB RT NAT LOG
17	Telometry	Any Zone, Any Host	#PortE3:1	telem.utmtools.com	IPS AV WEB APP QoS HB RT NAT LOG
9	OCM	Any Zone, Any Host	#PortE3:1	ocrm.utmtools.com	IPS AV WEB APP QoS HB RT NAT LOG
5	SFM16	Any Zone, Any Host	#PortE3:1	198.144.101.92, sfm.utmtools.com	IPS AV WEB APP QoS HB RT NAT LOG
3	NAT Rules				Keep all my NAT rules together
3	To or From Alan's Desk				Traffic coming from, or going to Alan...
5	Terminal Server User Rules				Rules for terminal server users
16	Term Server School	Any Zone, omega.mvdomain.io...	WAN, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS
11	Term Server Teachers	Any Zone, omega.mvdomain.io...	WAN, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS
12	Term Server Exces	Any Zone, omega.mvdomain.io...	WAN, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS
13	Term Server Authenticat...	Any Zone, omega.mvdomain.io...	WAN, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS
14	Term Server Unknown u...	Any Zone, omega.mvdomain.io...	WAN, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS
2	Competitive Lab Access ...				Access to/from competitive lab
4	DMZ Access Rules				Rules between NON-WAN Zones
2	10.5.9.0/24 Network Rules				Rules for the Lab Management network
1	Default Internet Allow	LAN, DMZ, VPN, WiFi, Any Host	WAN, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS
23	My Default Drop Rule	Any Zone, Any Host	Any Zone, Any Host	Any Service	AV WEB APP QoS HB RT NAT LOG IPS

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

Add User/network rule

How-to guides Log viewer Help admin ▼ Sophos

Rule name *
Enter Rule name

Description
Enter Description

Rule position
Bottom ▼

Action
Accept Drop Reject

Rule group
Create new
None
Automatic
User Traffic to DMZ
Traffic to Automatic
Traffic to WAN
Traffic to Internal Zones

Source

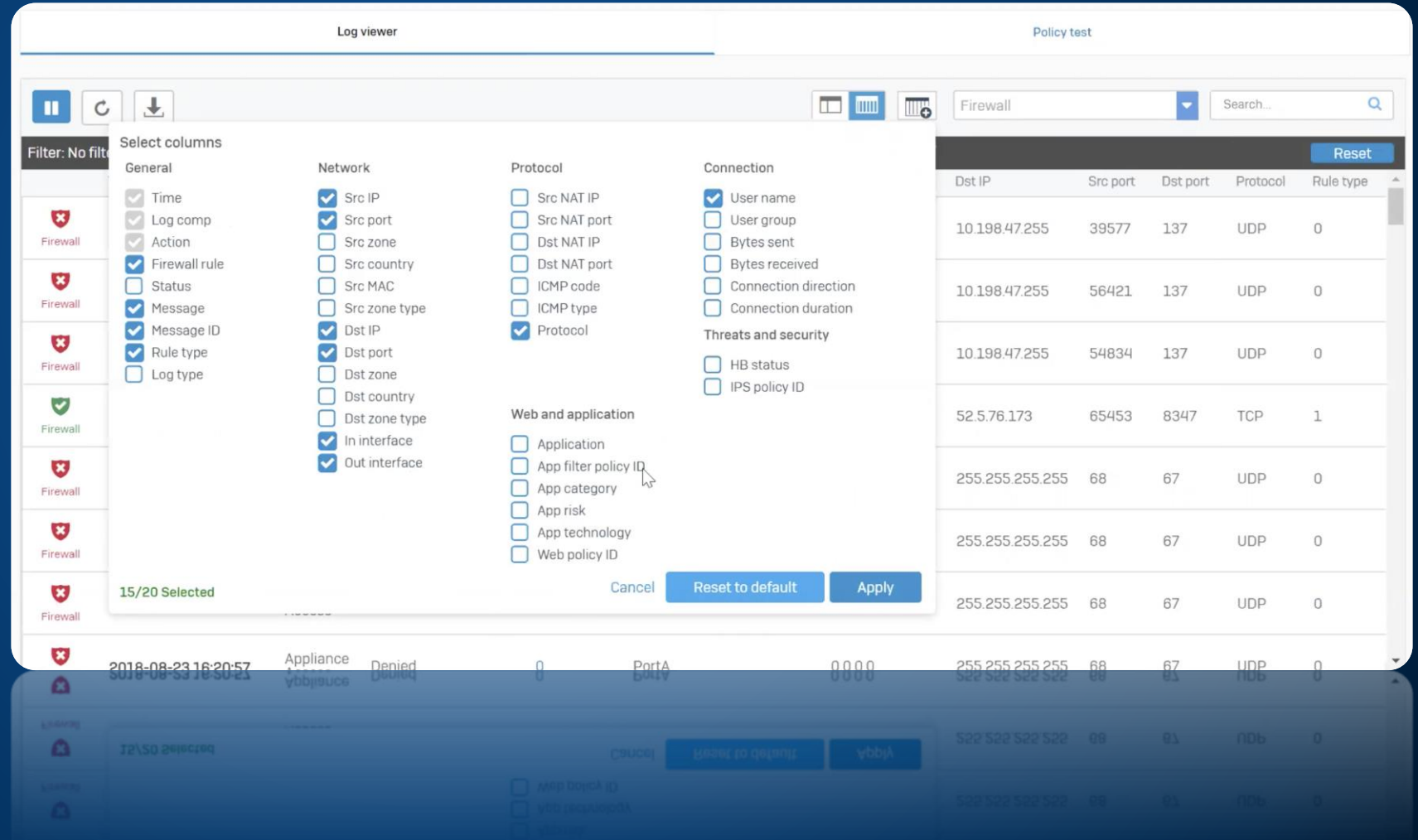
Can't add the rule to an existing group based on the selected criteria.

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



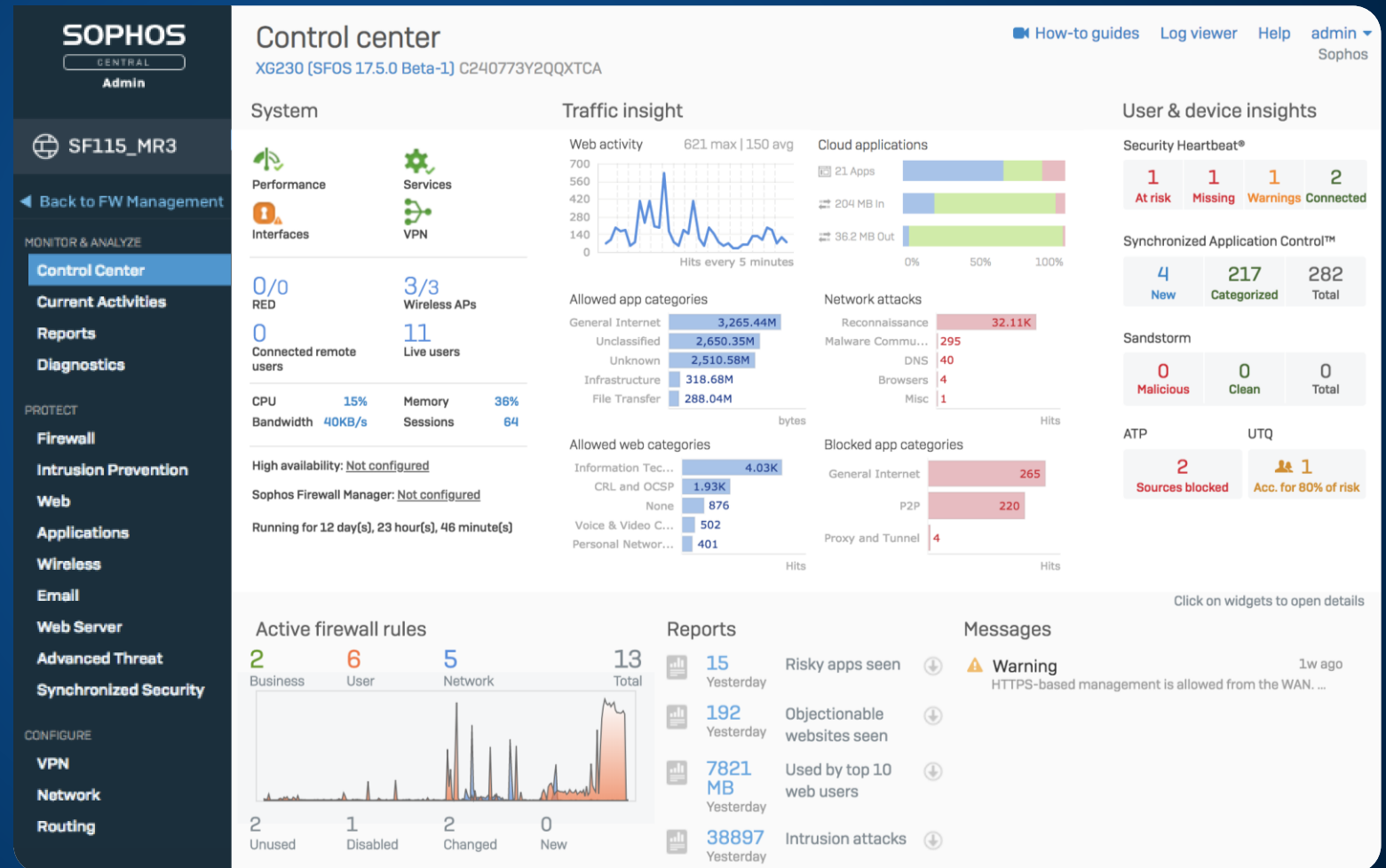
Sophos Central Management

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 Central을 통한 모든 XG장비를 안전하게 외부 접속
- 가용성, 라이선스, 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

관리 중인 모든 방화벽을 소포스 Central 에서

SOPHOS
CENTRAL
Admin

Firewall Management

[Back to Overview](#)

ANALYZE

Dashboard

Alerts

Backup

MANAGE

Firewalls

CONFIGURE

Settings

Firewall Management - Firewalls

Overview / Firewall Management Dashboard / Firewalls

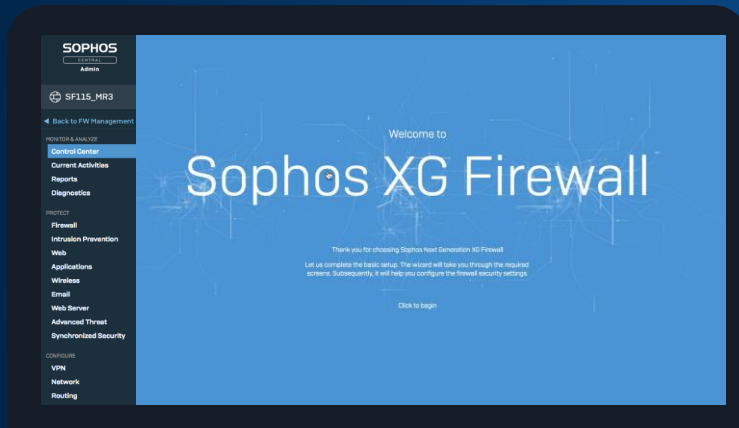
Add Firewall

	FW Name, IP	OS Version, Model, Serial Number
CONNECTED	C0100139BBHDVD6 108.7.62.118	SN: C0100139BBHDVD6
CONNECTED	Burlington Lab VM 198.144.101.86	SN: C010016J436YT20
CONNECTED	Billerica Lab VM 1 108.7.62.118	SN: C01001CY9K2YPE0

Rapid Deployment

현장 엔지니어 없이 외부 장치 배포

1. Sophos Central내의 Setup Wizard 사용



2. (Optional) 원격지에 Email로 설정파일 송신

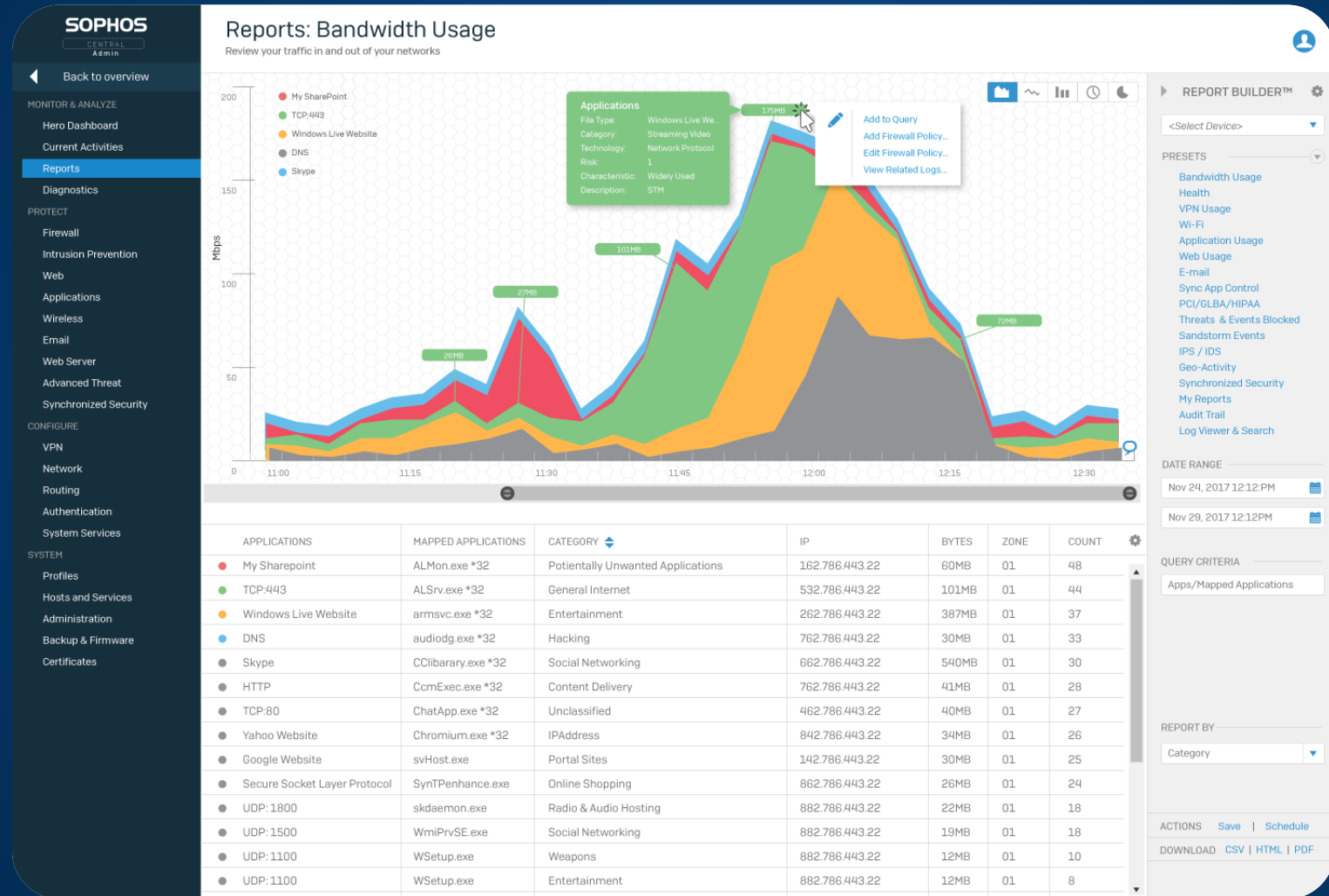


3. USB 스틱에 설정파일 복사

4. 연결된 USB 로 장비 부팅



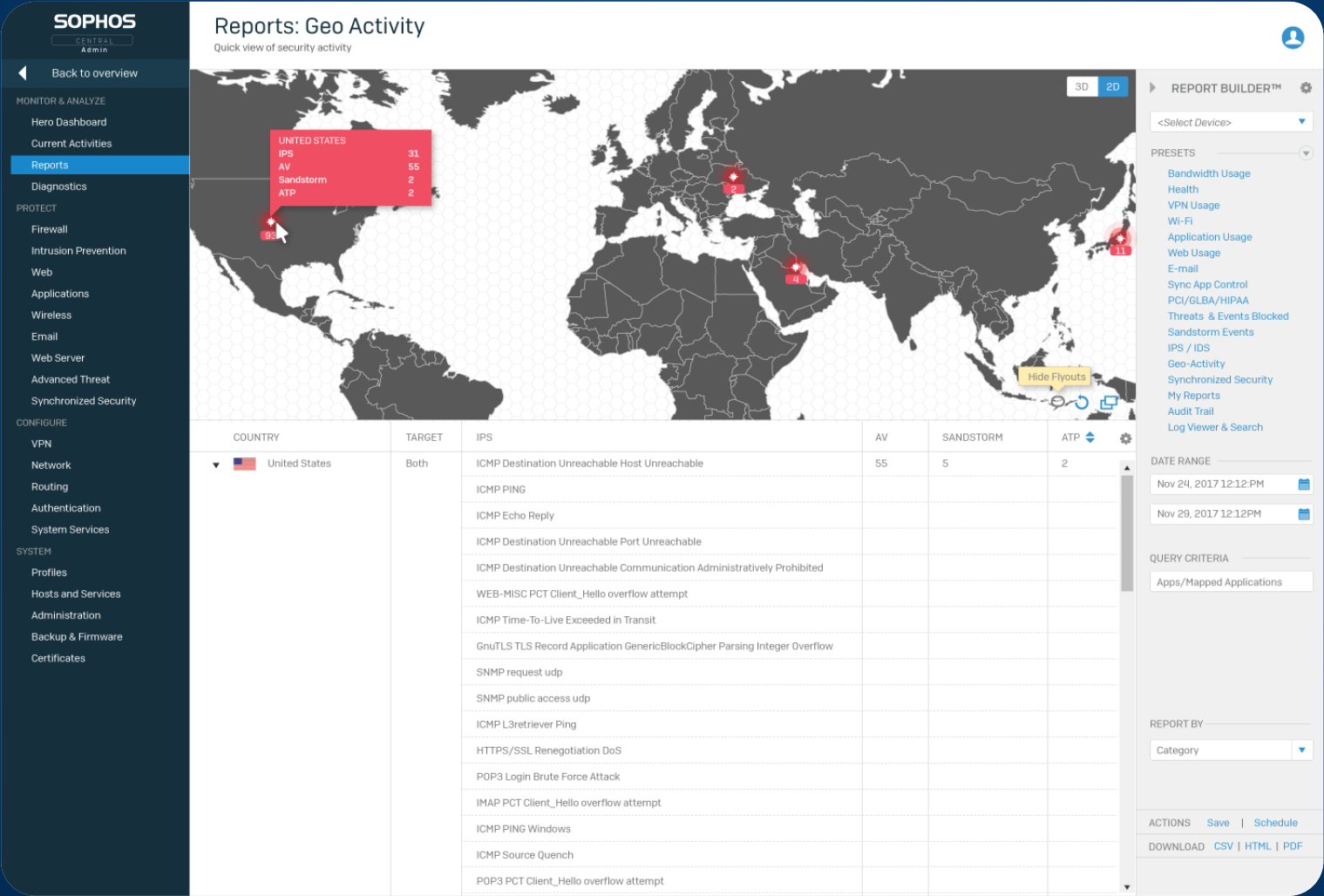
Reporting - Bandwidth Usage



Reporting - Health



Reporting - Geo Activity



SOPHOS
Security made simple.