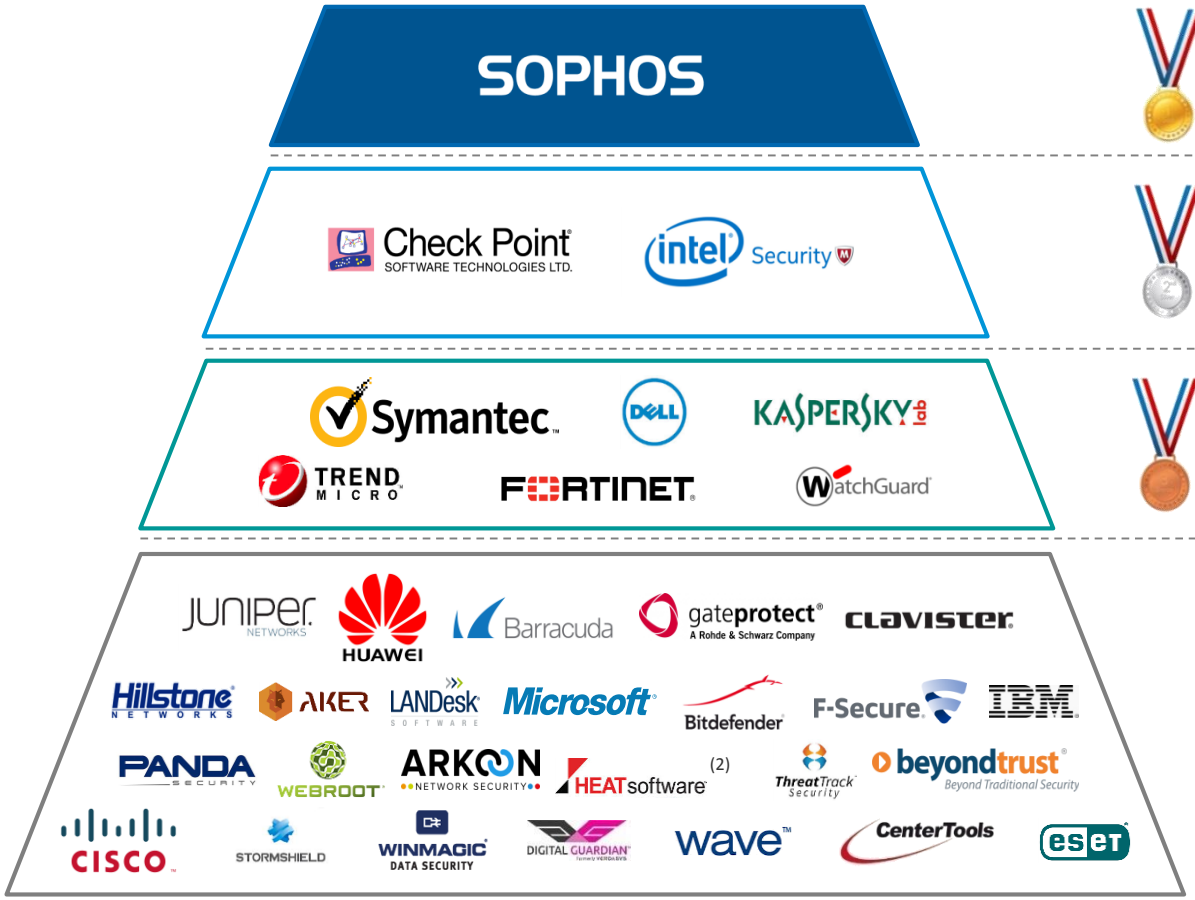
Sophos
Security made simple.

Walter Narisoni
Sales Engineer Manager

Dicembre 2015

SOPHOS

Only Vendor Ranked as a Leader in Endpoint, UTM and Encryption



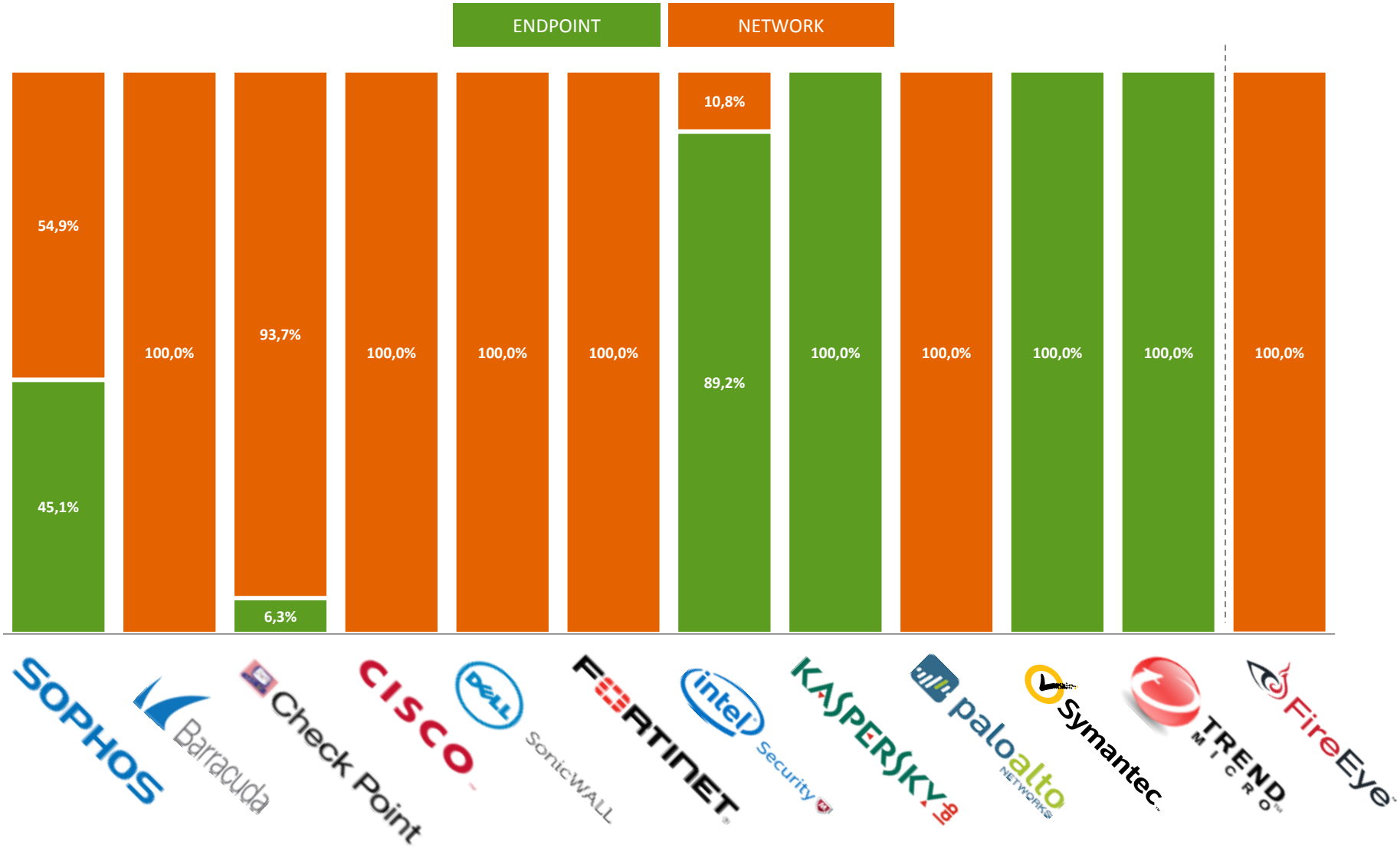
LEADER in all **3** of these Gartner Magic Quadrants

LEADER in **2** of these Gartner Magic Quadrants

LEADER in **1** of these Gartner Magic Quadrants

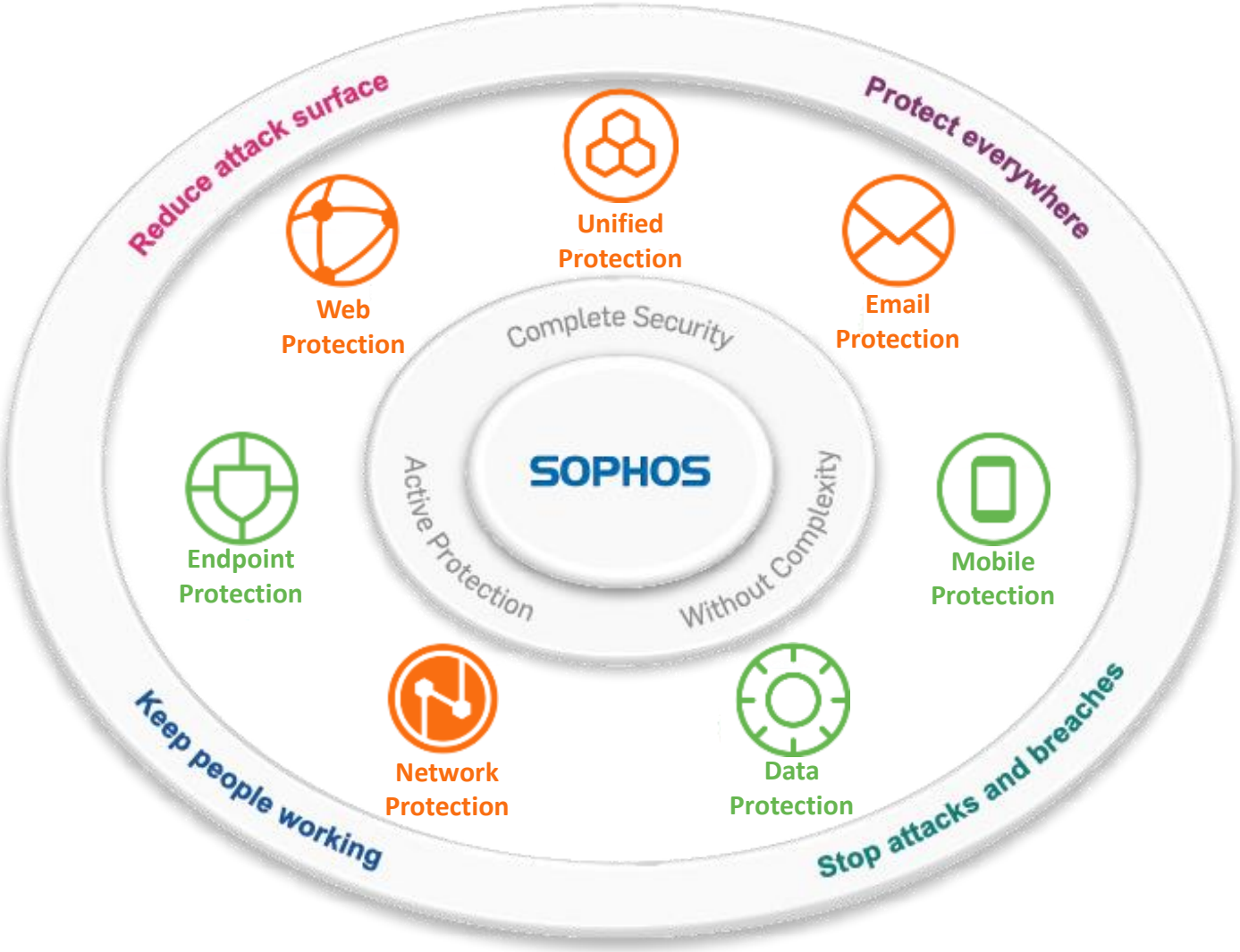
PRESENT in **1** of these Gartner Magic Quadrants

Unique Balance Between Endpoint and Network



Complete Security

Protecting every part of your business



Agenda

- Sophos Next –Gen Data Protection
- Sophos UTM & Cyberoam
- Sophos Cloud

SOPHOS

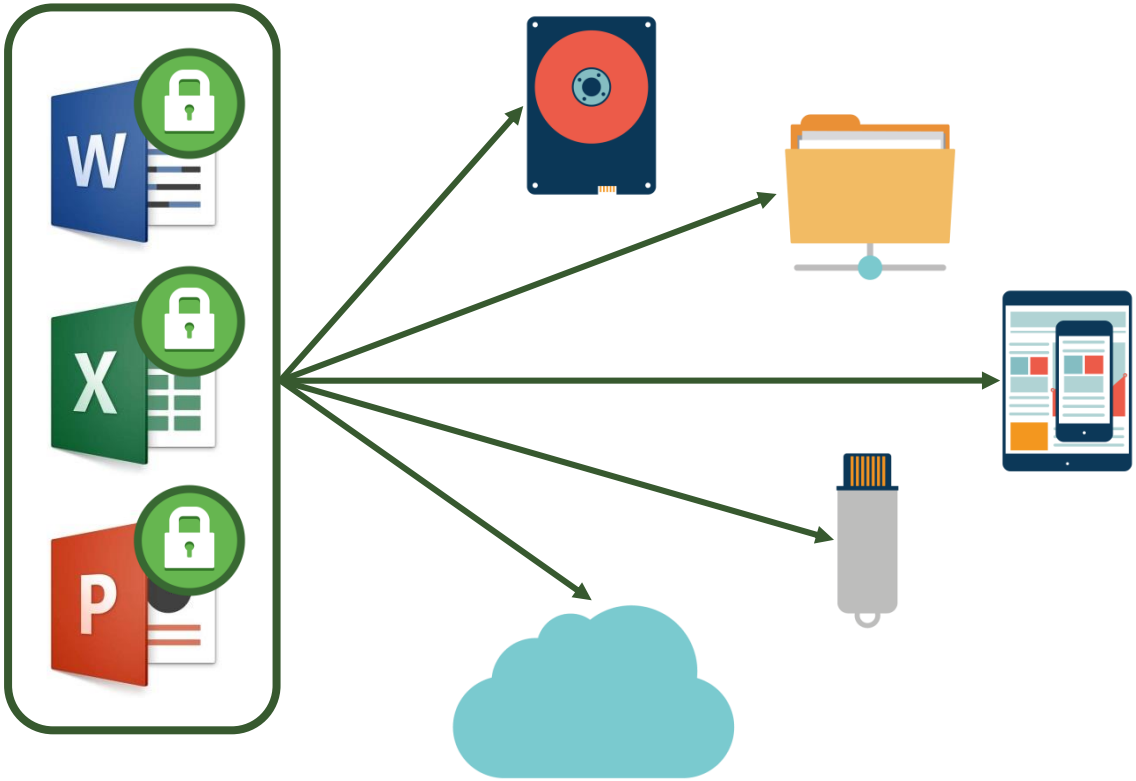
Next-Gen Data Protection

Sophos SafeGuard Enterprise

Protecting Data wherever it goes!

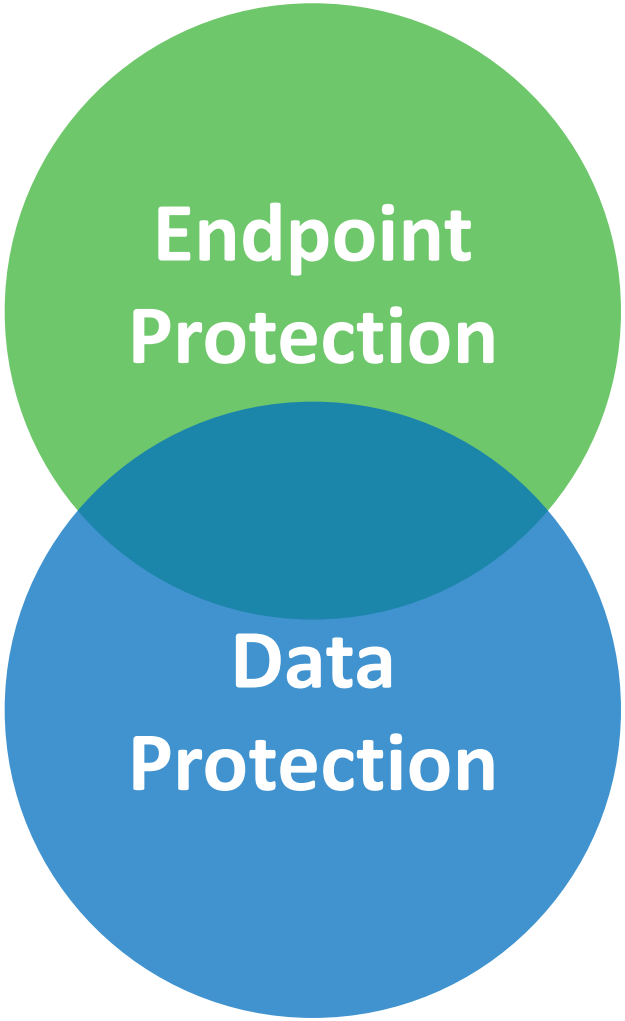
Assertion - All data is important

- By default data must be protected
- Encryption must be persistent

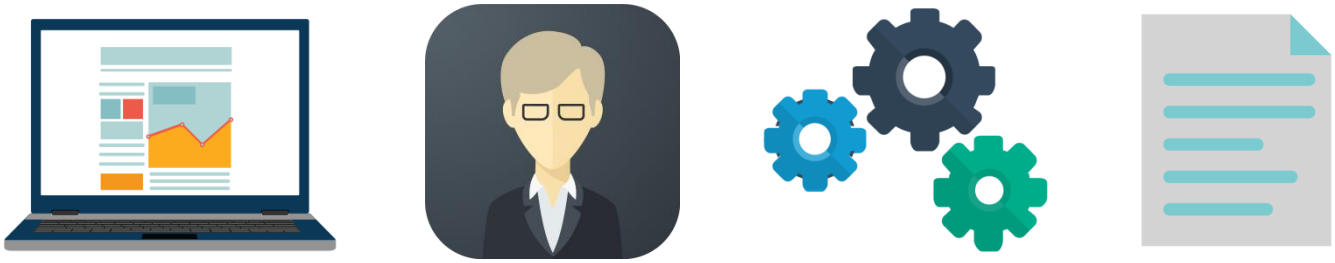


Encryption as a Threat Protection Technology

- Protecting key access becomes paramount
- Protect data in the event of a compromise!
  - Integrate Endpoint and Data Protection Technology
- Pillars for key access
  - Trusted device
  - Trusted user
  - Trusted process



Reactive to Integrity



Collaboration

Simplicity!

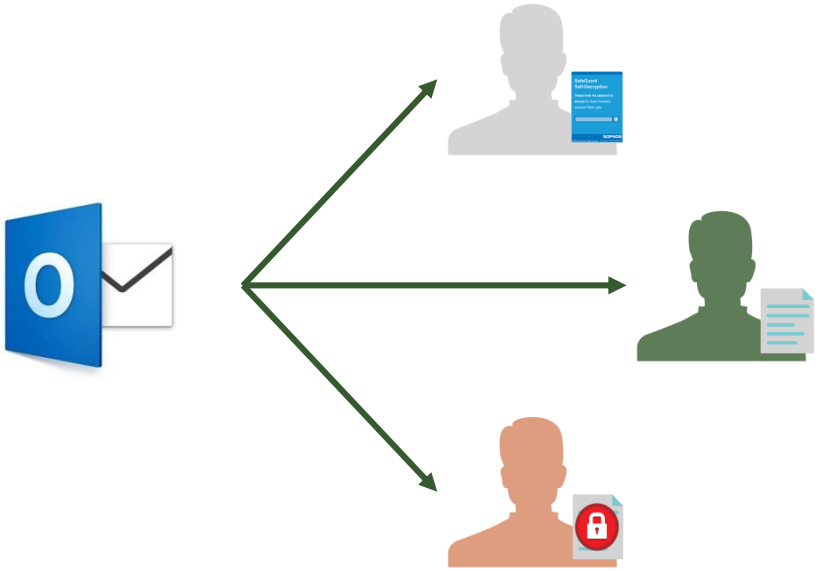
- Don’t change End User behavior or workflow

Internally, everyone has access

- Files can be shared encrypted with internal employees

Options for external collaboration

- Encrypted file
- Plain Text file
- Wrapped in a HTML5 wrapper



Continuous Productivity

Work across devices

- Windows, OS X, iOS & Android

Users remain productive

- In the office, on the road, with any device

Still protected

- Device integrity determines access to data. One device compromised? Work on another

Next-Gen Threat & Data Protection

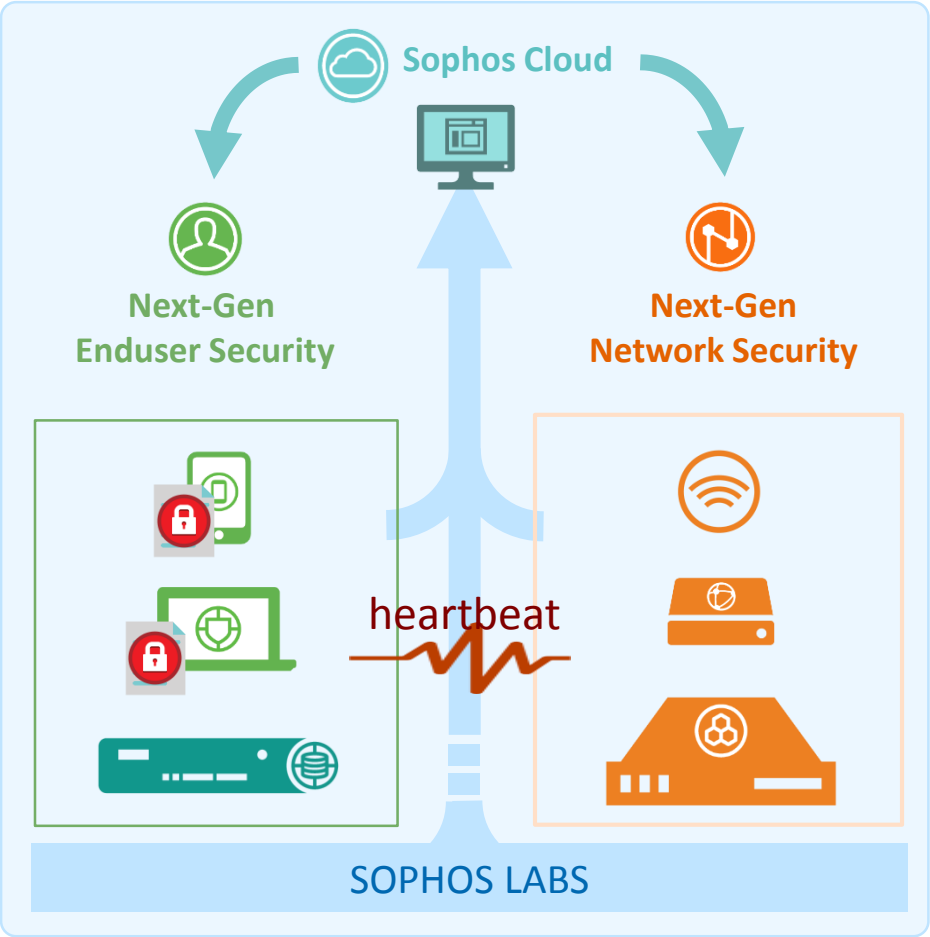
Security must be comprehensive
The capabilities required to fully satisfy customer need

Security can be made simple
Platform, deployment, licensing, user experience

Security is more effective as a system
New possibilities through technology cooperation

Your data, encrypted and protected
Trusted User + Device + Process to access encrypted data

Protected in the Event of a Compromise
Integrated with Project Galileo to lock down a Device



SOPHOS

Sophos UTM & Cyberoam

Project Copernicus

SOPHOS

Leading Threat Protection
RED for Distributed Networks

Secure Wi-Fi & Access Points
Web Protection Technologies

Cyberoam

Layer 8 User Identity Policies
Leading Application Control

Accelerated Packet Filtering
iView Logging & Reporting

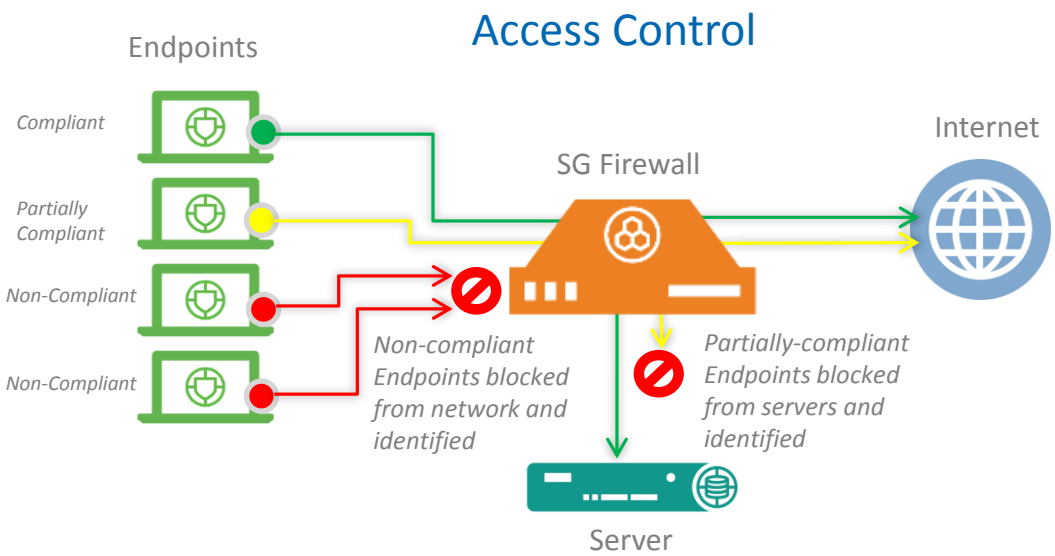
Comprehensive Management

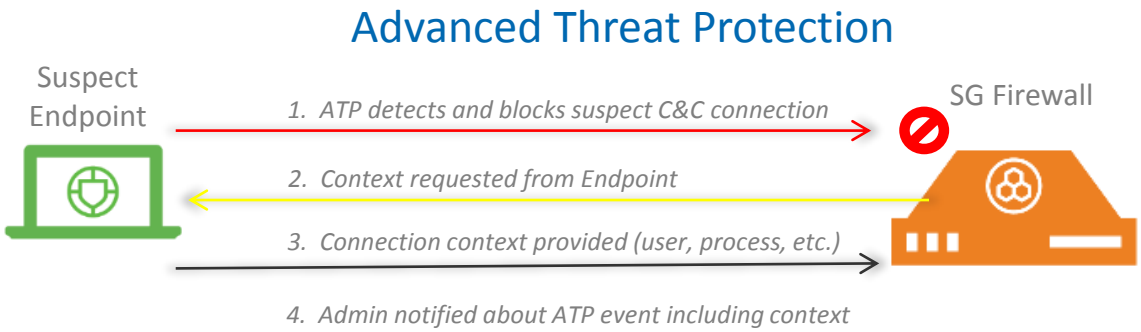
Simple to Use

Secured by Galileo

Security Heartbeat

Network and Endpoint share heartbeat and context to work better together





Heartbeat & Context

- Devices on the network share heartbeat and context
- Firewall enforces access policy based on level of compliance
- Firewall requests context from Endpoints in the event of suspicious network traffic
- Two products work better together to provide enhanced protection and improve response times to incidents

Network Security Control Center

xgfw.west.mountainoutfitters.com
SG125 R2 (v15.1.2), C1200114EE22E5C

Alerts 2 | Help | Heidi Miller, Mountain Outfitters

System

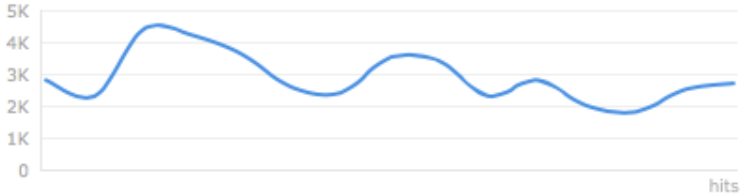
Performance
Services
Connections
VPN

Memory 21%
CPU 31%
Bandwidth 34k
Sessions 4.8k

High Availability: A-A (M)
Sophos Firewall Manager: sfm_1
Running for 10w 3d 12h

Traffic Insight

Web Activity — 4400 highest | 2900 avg



Top Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Top Blocked Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Top Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Top Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insight

Security Heart Beat
3 Warnings | 1 System at risk | 12

Advanced Threat Protection
3 — 3 Sources blocked!

User Threat Quotient
6 — 6 users account for 80% of risk!

3/6 RED
5/6 (2) Wireless APs
12 Connected Remote Users
3 Countries

Click on widgets to open details

Active Policies

3 Business | 14 User | 27 Network | 44 Total

3 Unused | 8 Disabled | 76 Changed | 12 New

Reports

16 Yesterday — Risky Apps Seen
136 Yesterday — Inappropriate Websites Seen
3.4TB Yesterday — Used by Top Users
58 Yesterday — Intrusion Attacks

Messages

2 | 1 | 11 | 14

Alert — 12.03.15 – 12:30
Password change reminder. The default Password ...

Alert — 12.03.15 – 12:30
HTTP management is allowed. HTTP based manage...

Warning — 12.03.15 – 12:30
CA Cert replaced. For security reasons the default ...

Notification — 12.03.15 – 12:30
New Firmware is available. Refer to release notes ...

Network Security Control Center

xgfw.west.mountainoutfitters.com
SG125 R2 (v15.1.2), C1200114EE22E5C

Alerts 2 | Help | Heidi Miller, Mountain Outfitters

System

Performance
Services
Connections
VPN

Memory 21%
CPU 31%
Bandwidth 34k
Sessions 4.8k

High Availability: A-A (M)
Sophos Firewall Manager: sfm_1
Running for 10w 3d 12h

Traffic Insight

Web Activity — 4400 highest | 2900 avg

5K, 4K, 3K, 2K, 1K, 0 — hits

Top Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Top Blocked Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Top Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Top Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insight

Security Heart Beat
3 Warnings | 1 System at risk | 12

Advanced Threat Protection
3 — 3 Sources blocked!

User Threat Quotient
6 — 6 users account for 80% of risk!

3/6 RED
5/6 (2) Wireless APs
12 Connected Remote Users
3 Countries

Click on widgets to open details

Active Policies

3 Business | 14 User | 27 Network | 44 Total

3 Unused | 8 Disabled | 76 Changed | 12 New

Reports

16 Yesterday — Risky Apps Seen
136 Yesterday — Inappropriate Websites Seen
3.4TB Yesterday — Used by Top Users
58 Yesterday — Intrusion Attacks

Messages

2 | 1 | 11 | 14

Alert — 12.03.15 - 12:30
Password change reminder. The default Password ...

Alert — 12.03.15 - 12:30
HTTP management is allowed. HTTP based manage...

Warning — 12.03.15 - 12:30
CA Cert replaced. For security reasons the default ...

Notification — 12.03.15 - 12:30
New Firmware is available. Refer to release notes ...

Network Security Control Center

xgfw.west.mountainoutfitters.com
SG125 R2 (v15.1.2), C1200114EE22E5C

Alerts 2 | Help | Heidi Miller, Mountain Outfitters

System

Performance | Services | Connections | VPN

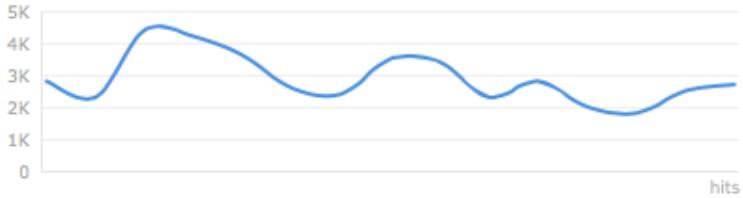
Memory 21% | CPU 31%

Bandwidth 34k | Sessions 4.8k

High Availability: A-A (M)
Sophos Firewall Manager: sfm_1
Running for 10w 3d 12h

Traffic Insight

Web Activity — 4400 highest | 2900 avg



Top Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Top Blocked Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Top Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Top Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insight

Security Heart Beat: 3 Warnings | 1 System at risk | 12

Advanced Threat Protection: 3 — 3 Sources blocked!

User Threat Quotient: 6 — 6 users account for 80% of risk!

3/6 RED | 5/6 (2) Wireless APs

12 Connected Remote Users | 3 Countries

Click on widgets to open details

Active Policies

3 Business | 14 User | 27 Network | 44 Total

3 Unused | 8 Disabled | 76 Changed | 12 New

Reports

16 Yesterday — Risky Apps Seen
136 Yesterday — Inappropriate Websites Seen
3.4TB Yesterday — Used by Top Users
58 Yesterday — Intrusion Attacks

Messages

2 | 1 | 11 | 14

Alert — 12.03.15 – 12:30
Password change reminder. The default Password ...

Alert — 12.03.15 – 12:30
HTTP management is allowed. HTTP based manage...

Warning — 12.03.15 – 12:30
CA Cert replaced. For security reasons the default ...

Notification — 12.03.15 – 12:30
New Firmware is available. Refer to release notes ...

Network Security Control Center

xgfw.west.mountainoutfitters.com
SG125 R2 (v15.1.2), C1200114EE22E5C

Alerts 2 | Help | Heidi Miller, Mountain Outfitters

System

Performance
Services
Connections
VPN

Memory 21%
CPU 31%
Bandwidth 34k
Sessions 4.8k

High Availability: A-A (M)
Sophos Firewall Manager: sfm_1
Running for 10w 3d 12h

Traffic Insight

Web Activity — 4400 highest | 2900 avg

Top Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Top Blocked Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Top Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Top Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insight

Security Heart Beat

3 Warnings | 1 System at risk | 12

Advanced Threat Protection

3 — 3 Sources blocked!

User Threat Quotient

6 — 6 users account for 80% of risk!

3/6 RED
5/6 (2) Wireless APs
12 Connected Remote Users
3 Countries

Click on widgets to open details

Active Policies

3 Business | 14 User | 27 Network | 44 Total

3 Unused | 8 Disabled | 76 Changed | 12 New

Reports

16 Yesterday — Risky Apps Seen
136 Yesterday — Inappropriate Websites Seen
3.4TB Yesterday — Used by Top Users
58 Yesterday — Intrusion Attacks

Messages

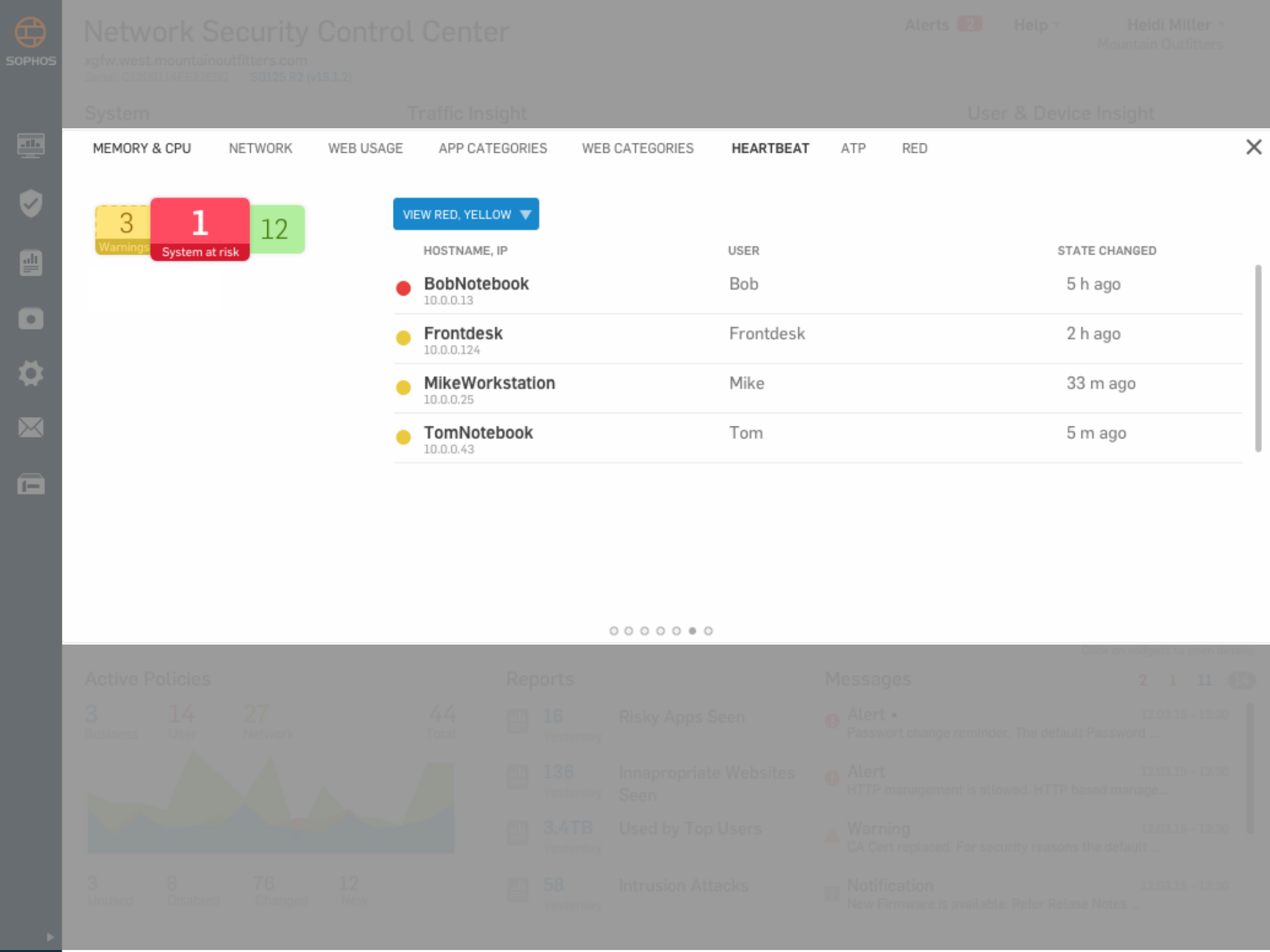
2 | 1 | 11 | 14

Alert — 12.03.15 – 12:30
Password change reminder. The default Password ...

Alert — 12.03.15 – 12:30
HTTP management is allowed. HTTP based manage...

Warning — 12.03.15 – 12:30
CA Cert replaced. For security reasons the default ...

Notification — 12.03.15 – 12:30
New Firmware is available. Refer to release notes ...


SOPHOS
Network Security Control Center
xgfw.west.mountainoutfitters.com
Alerts
Help
Heidi Miller
Mountain Outfitters
System
Traffic Insight
User & Device Insight
MEMORY & CPU
NETWORK
WEB USAGE
APP CATEGORIES
WEB CATEGORIES
HEARTBEAT
ATP
RED
3
Warnings
1
System at risk
12
VIEW RED, YELLOW
HOSTNAME, IP
USER
STATE CHANGED
BobNotebook
10.0.0.13
Bob
5 h ago
Frontdesk
10.0.0.124
Frontdesk
2 h ago
MikeWorkstation
10.0.0.25
Mike
33 m ago
TomNotebook
10.0.0.43
Tom
5 m ago
Active Policies
Reports
Messages
Risky Apps Seen
Innapropriate Websites Seen
Used by Top Users
Intrusion Attacks

Network Security Control Center

xgfw.west.mountainoutfitters.com
SG125 R2 (v15.1.2), C1200114EE22E5C

Alerts 2 | Help | Heidi Miller, Mountain Outfitters

System

Performance
Services
Connections
VPN

Memory 21%
CPU 31%
Bandwidth 34k
Sessions 4.8k

High Availability: A-A (M)
Sophos Firewall Manager: sfm_1
Running for 10w 3d 12h

Traffic Insight

Web Activity — 4400 highest | 2900 avg

5K, 4K, 3K, 2K, 1K, 0 — hits

Top Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Top Blocked Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Top Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Top Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insight

Security Heart Beat
3 Warnings | 1 System at risk | 12

Advanced Threat Protection
3 — 3 Sources blocked!

User Threat Quotient
6 — 6 users account for 80% of risk!

3/6 RED
5/6 (2) Wireless APs
12 Connected Remote Users
3 Countries

Click on widgets to open details

Active Policies

3	14	27	44
Business	User	Network	Total

3	8	76	12
Unused	Disabled	Changed	New

Reports

16 Yesterday	Risky Apps Seen
136 Yesterday	Inappropriate Websites Seen
3.4TB Yesterday	Used by Top Users
58 Yesterday	Intrusion Attacks

Messages

2 | 1 | 11 | 14

- Alert — 12.03.15 – 12:30 — Password change reminder. The default Password ...
- Alert — 12.03.15 – 12:30 — HTTP management is allowed. HTTP based manage...
- Warning — 12.03.15 – 12:30 — CA Cert replaced. For security reasons the default ...
- Notification — 12.03.15 – 12:30 — New Firmware is available. Refer to release notes ...

Add Policy

This ia a list of all security policies on the system.

About This Policy

Policy Position
Set position compared to other policies

Bottom

Application Template
Choose the type of application

Type to search

- Sharepoint 2013
- Outlook Web Access
- Lync
- Exchange ActiveSync
- General Web Application
- General Port-Based Application

Policy Name
Give a friendly name for this policy

Descriptoion
Optional Description

Cancel

SAVE

Hosted Server

Configure how this service will be made available to clients

Hosted Address
198.144.101.93

HTTPS
Will the service accept HTTPS connections
ON

Redirect HTTP
Are all connections redirected to HTTPS
ON

HTTPS Certificate
Which certificate should be used for HTTPS
Default Application Certificate

Domains
List the domain names that should be used
- sharepoint.mountaineering.com
- sharepoint.mocorp.local

Forward requests to sharepoint.mountaneering.com and sharepoint.mocorp.local to sharepoint1 and sharepoint2, while applying "Sharepoint Policy1"

Cancel

SAVE

Network Security Control Center

xgfw.west.mountainoutfitters.com

Serial: C1200114EE22E5C SG125 R2 (v15.1.2)

Alerts 2 Help Heidi Miller Mountain Outfitters

System

Performance Services

Traffic Insight

Web Activity 4400 highest | 2900 avg

5K 4K 3K

User & Device Insight

Security Heart Beat

3 Warnings 1 System at risk 12

Advanced Threat Protection

3 Sources blocked!

User Threat Quotient

6 users account for 80% of risk!

3/6 RED

5/6 (2) Wireless APs

12 Connected Remote Users

3 Countries

Click on widgets to open details

2 1 11 14

12.03.15 – 12:30

rt change reminder. The default Password ...

12.03.15 – 12:30

anagement is allowed. HTTP based manage...

12.03.15 – 12:30

Warning

CA Cert replaced. For security reasons the default ...

12.03.15 – 12:30

Notification

New Firmware is available. Refer Relase Notes ...

3 Unused 8 Disabled 76 Changed 12 New

Yesterday

58 Yesterday Intrusion Attacks

- Current Activity
- Administration
- Routing
- System Services
- Configuration
- VPN
- Diagnostics
- Network
- Maintenance

System

- Web Proxy
- HA
- Traffic Shaping (QoS)
- Quarantine Digest Settings
- Trusted Domain
- SPX Email Encryption
- RED
- Wireless

High Availability (HA) allows a second system to be used for redundancy or scalability.

Actions Available:
- Enable/Disable HA
- Configure HA Mode (A-A/A-P)
- Switch an appliance to standby mode
- Synchronize HA peers

HELP

SOPHOS Reports

Alerts 2 Help Heidi Smith
Mountain Outfitters

Control Center / Reports / Web Reports

FROM: 21.04.2015
TO: 24.04.2015
SET PERIOD

Risk: HIGH 84
This is a risk meter. It shows how ...

Web Reports | Group

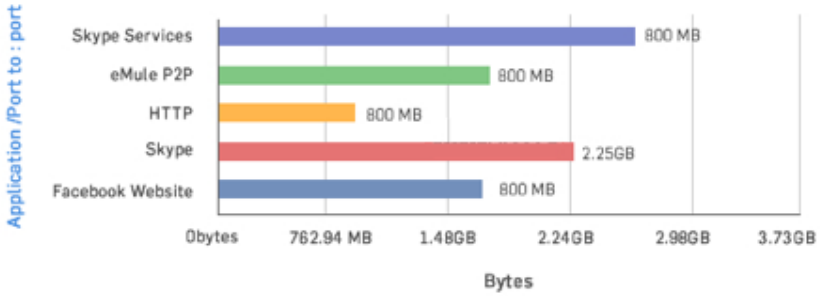
Web Reports > Application

Download: PDF HTML EXCEL

Records per page: 5 | 10 | 20 | 50 | 100

Bob

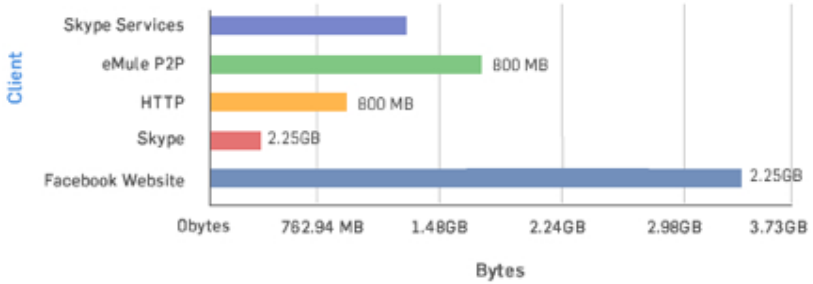
Application By Risk level



Application/Proto.	Risk	Hits	Bytes
Skype Services	5	165845	15.6 MB
eMule P2P	4	54	1.25 MB
HTTP	3	47458454	485.1 MB
Skype	2	41222	75.1 MB
Facebook website	1	5874584	12.1 MB

View All

Top Clients Accessing High Risk Application



Application/Proto.	Risk	Hits	Bytes
Skype Services	5	165845	15.6 MB
eMule P2P	4	54	1.25 MB
HTTP	3	47458454	485.1 MB
Skype	2	41222	75.1 MB
Facebook website	1	5874584	12.1 MB

View All

SOPHOS

SOPHOS Reports

Control Center / Reports / Web Reports

Alerts 2 Help Heidi Smith
Mountain Outfitters

84 Risk: HIGH

This is a risk meter. It shows how ...

Download: PDF HTML EXCEL

FROM: 21.04.2015

TO: 24.04.2015

SET PERIOD

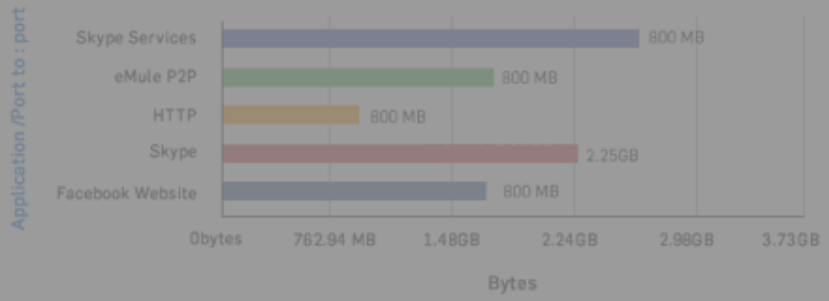
Web Reports | Group

Web Reports > Application

Records per page: 5 | 10 | 20 | 50 | 100

Bob

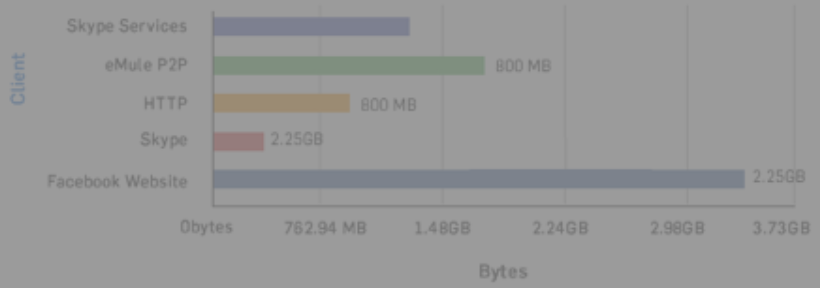
Application By Risk level



Application/Proto.	Risk	Hits	Bytes
Skype Services	5	165845	15.6 MB
eMule P2P	4	54	1.25 MB
HTTP	3	47458454	485.1 MB
Skype	2	41222	75.1 MB
Facebook website	1	5874584	12.1 MB

View All

Top Clients Accessing High Risk Application



Application/Proto.	Risk	Hits	Bytes
Skype Services	5	165845	15.6 MB
eMule P2P	4	54	1.25 MB
HTTP	3	47458454	485.1 MB
Skype	2	41222	75.1 MB
Facebook website	1	5874584	12.1 MB

View All

Network Security Control Center

xgfw.west.mountainoutfitters.com
SG125 R2 (v15.1.2), C1200114EE22E5C

Alerts 2 | Help | Heidi Miller, Mountain Outfitters

System

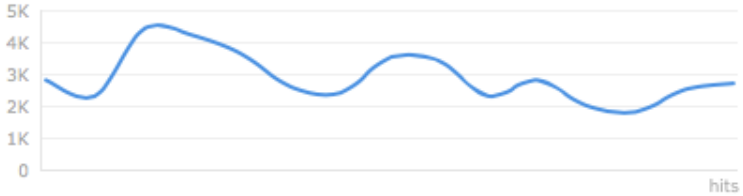
Performance
Services
Connections
VPN

Memory 21%
CPU 31%
Bandwidth 34k
Sessions 4.8k

High Availability: A-A (M)
Sophos Firewall Manager: sfm_1
Running for 10w 3d 12h

Traffic Insight

Web Activity — 4400 highest | 2900 avg



Top Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Top Blocked Network Attacks

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Top Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Top Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

User & Device Insight

Security Heart Beat
3 Warnings | 1 System at risk | 12

Advanced Threat Protection
3 — 3 Sources blocked!

User Threat Quotient
6 — 6 users account for 80% of risk!

3/6 RED
5/6 (2) Wireless APs
12 Connected Remote Users
3 Countries

Click on widgets to open details

Active Policies

3 Business | 14 User | 27 Network | 44 Total

3 Unused | 8 Disabled | 76 Changed | 12 New

Reports

16 Yesterday — Risky Apps Seen
136 Yesterday — Inappropriate Websites Seen
3.4TB Yesterday — Used by Top Users
58 Yesterday — Intrusion Attacks

Messages

2 | 1 | 11 | 14

Alert — 12.03.15 – 12:30
Password change reminder. The default Password ...

Alert — 12.03.15 – 12:30
HTTP management is allowed. HTTP based manage...

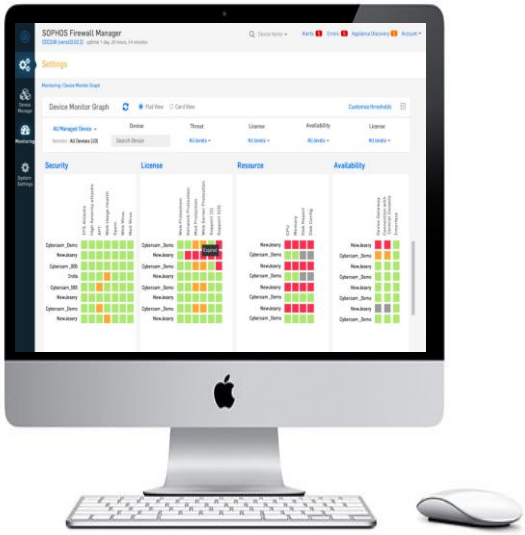
Warning — 12.03.15 – 12:30
CA Cert replaced. For security reasons the default ...

Notification — 12.03.15 – 12:30
New Firmware is available. Refer to release notes ...

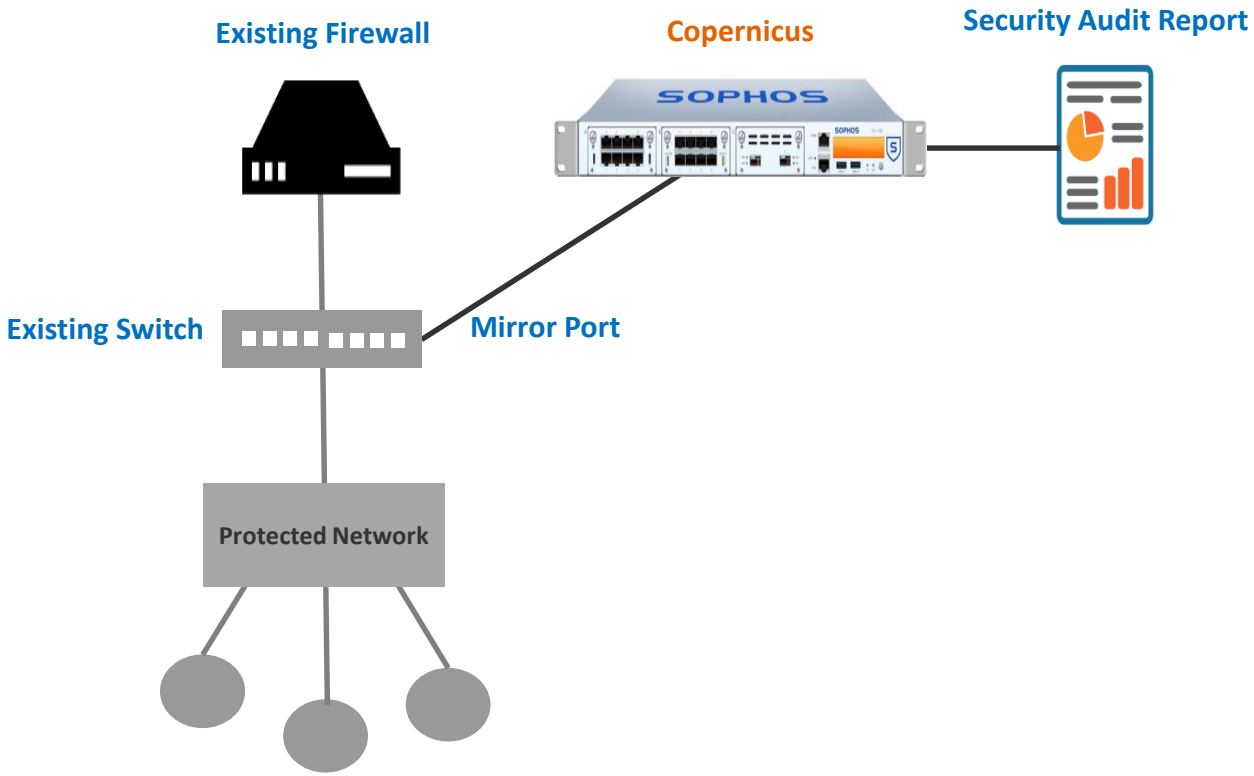
Copernicus - Central Management

Comprehensive Management

Full-featured multi-device management in the cloud or on-premise



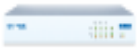
Copernicus – Discover Mode



Discover Mode

- Demonstrates value without changes to the network
- Discover Mode mirrors traffic through our UTM/NGFW
- Monitor only, no enforcement
- No need to disable existing protection
- Detailed Security Audit Report provided to evaluator to assess deficiencies

XG Series Appliance Portfolio

Hardware Appliance	XG 85	XG 105 / 115	XG 125 / 135	XG 210 / 230	XG 310 / 330	XG 430 / 450	XG 550	XG 650	XG 750
									
Category	Small Desktop	Small Desktop	Small Desktop	Medium Midrange 1U	Medium Midrange 1U	Medium Midrange 1U	Large High-end 2U	Large High-end 2U	Large High-end 2U
Network Ports (standard)	4	4	8	6	8 & 2 SFP	8 (FleXi Port)	8 (FleXi Port)	8 (FleXi Port)	8 (FleXi Port)
FleXi Port Expansion Bays	n/a	n/a	n/a	1	1	2	3	4	8
Maximum Ports	4	4	8	14	18	24	24	32	64
Redundancy	n/a	n/a	n/a	n/a	n/a	2 SSD (RAID) & 2nd hot-swap power optional (SG 450 only)	2 hot-swap SSD (RAID) 2 hot-swap power supplies	2 hot-swap SSD (RAID) 2 hot-swap power supplies	2 hot-swap SSD (RAID) 2 hot-swap power supplies
Wireless	Integr. 802.11n optional	Integr. 802.11n optional	Integr. 802.11ac optional	n/a	n/a	n/a	n/a	n/a	n/a

Core Protection

Base Firewall

Firewall & VPN & Wireless

Protection Modules:

- Network Protection
- Web Protection
- Email Protection
- Web Server Protect.

Next-Gen Protection

EnterpriseGuard

Firewall & VPN & Wireless

Included Protection:

- Network Protection
- Web Protection

✓Enhanced Support

+ XG Series Appliance

EnterpriseProtect

Total Protection

FullGuard

Firewall & VPN & Wireless

Included Protection:

- Network Protection
- Web Protection
- Email Protection
- Web Server Protect.

✓Enhanced Support

+ XG Series Appliance

TotalProtect

SOPHOS

Sophos Cloud

Cloud Security (Sophos Cloud) – Panoramica della soluzione e strategia

Sophos Cloud Per Amministratori

- Gestione e reporting unificato
- Semplice da distribuire – no server da gestire

Product Components by Q1 CY2016

- Endpoint Protection
- Mobile Security
- Server Protection
- Web Gateway
- Email Gateway

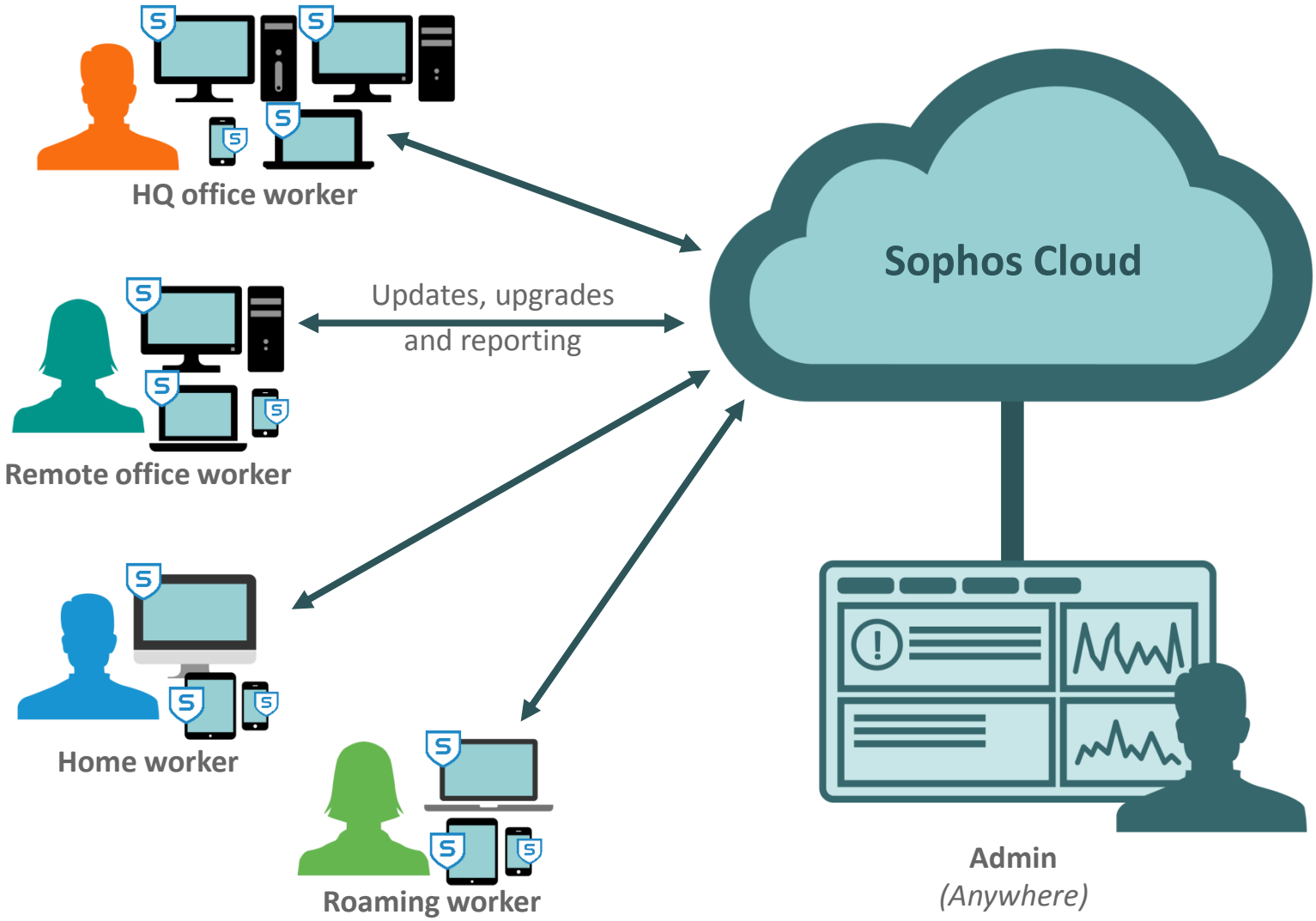
Sophos Cloud Per Partner

- Gestione dei clienti e delle licenze
- Gestione degli incidenti centralizzata

Strategia del prodotto

Integrate Sophos Portfolio	• Integrazione dei prodotti Sophos in un singolo pannello di controllo
Channel First	• Facile per i partner vendere e fare cross-sell • Disponibile con vari modelli di business • Fa diventare la gestione del contratto e della sicurezza del clinete facile
Semplice e veloce dal Discovery all'Acquisto	• Facile e veloce da far vedere, valutare e comprare

Unified Security per Windows, Mac e Dispositivi Mobile



Funzionalità Sophos Cloud

Usabilità . Simplicità . Protezione

- Cloud-based management console
- Anti-malware con Live Protection
- HIPS
- Web Security
- Device Control
- **Application Control**
- Server protection
- **Server Lockdown**
- Web Control (Web Content Filtering)
- Gestione e policy user-based
- **Multipiattaforma (protezione per Windows, Mac e Mobile)**
- Sincronizzazione con AD – delivery facile e gestione continua
- Partner Dashboard

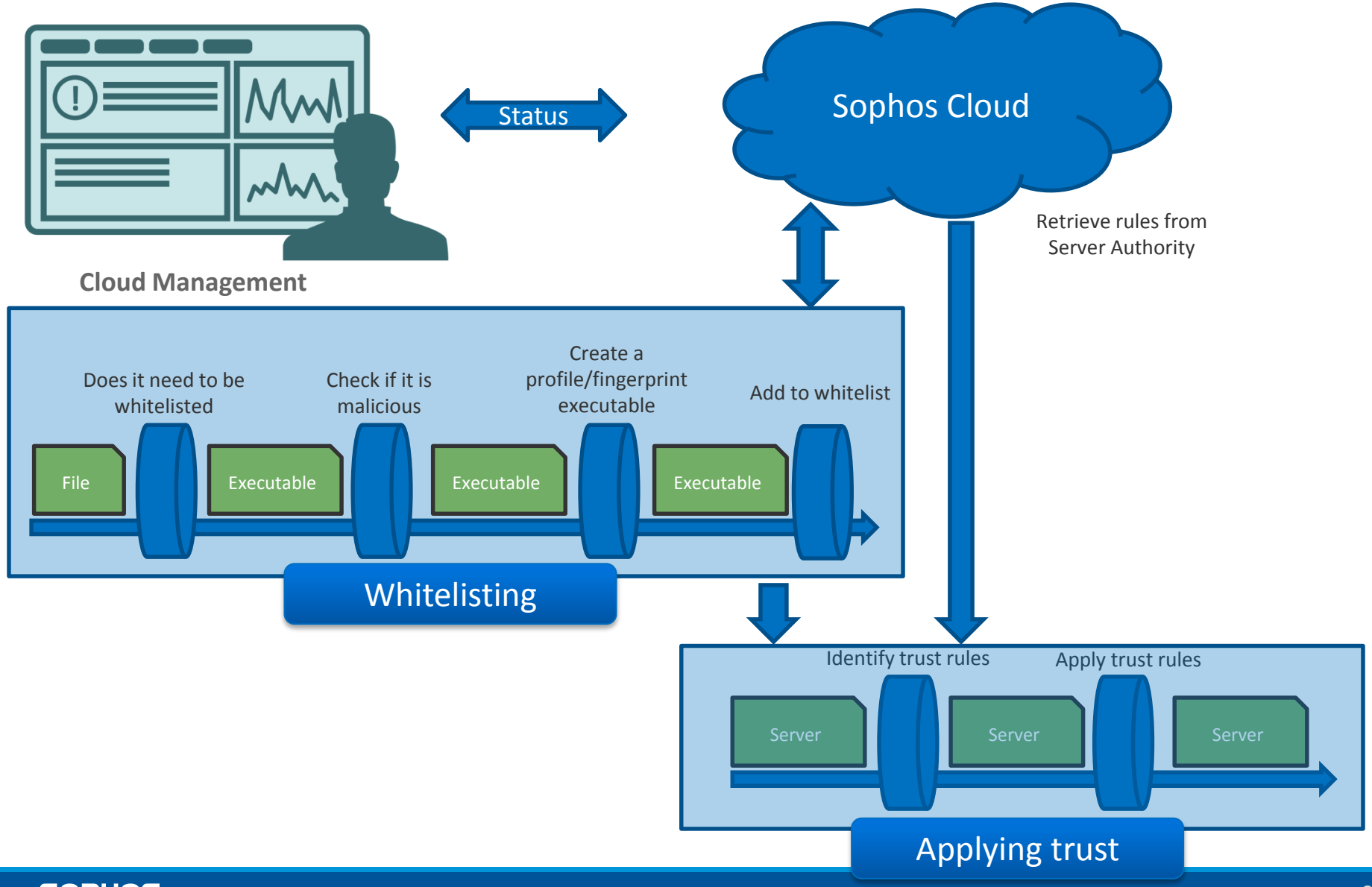
Sophos Cloud Server Protection

- Facile da configurare e gestire
- Regole di esclusione automatiche
- Ottime performance
- Protezione eccellente

Anti-malware

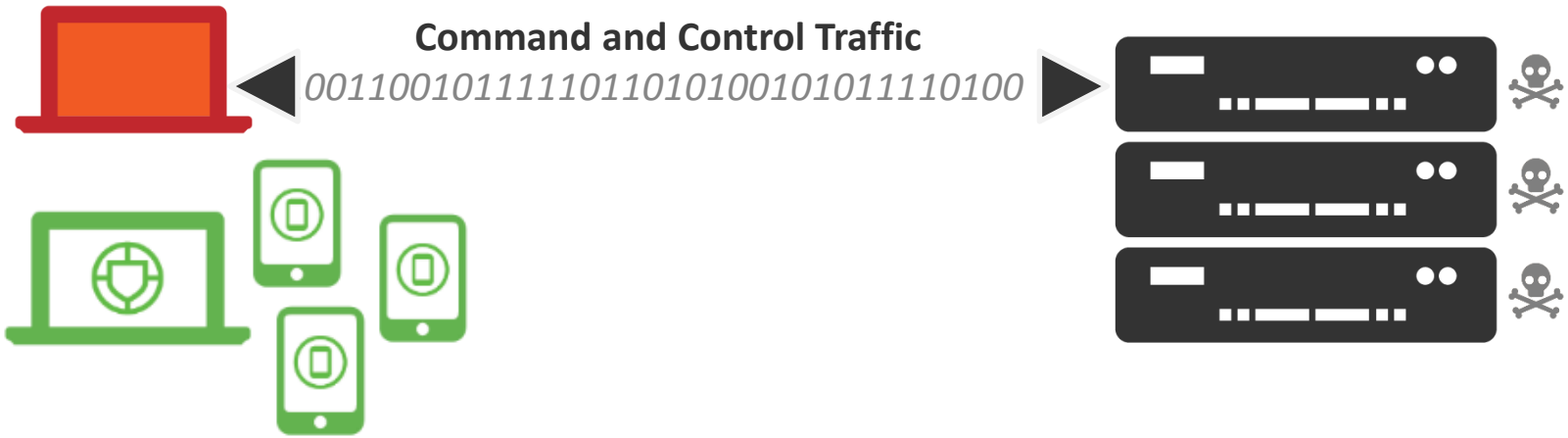
Server-specific policy

Cosa succede quando cliccate lockdown

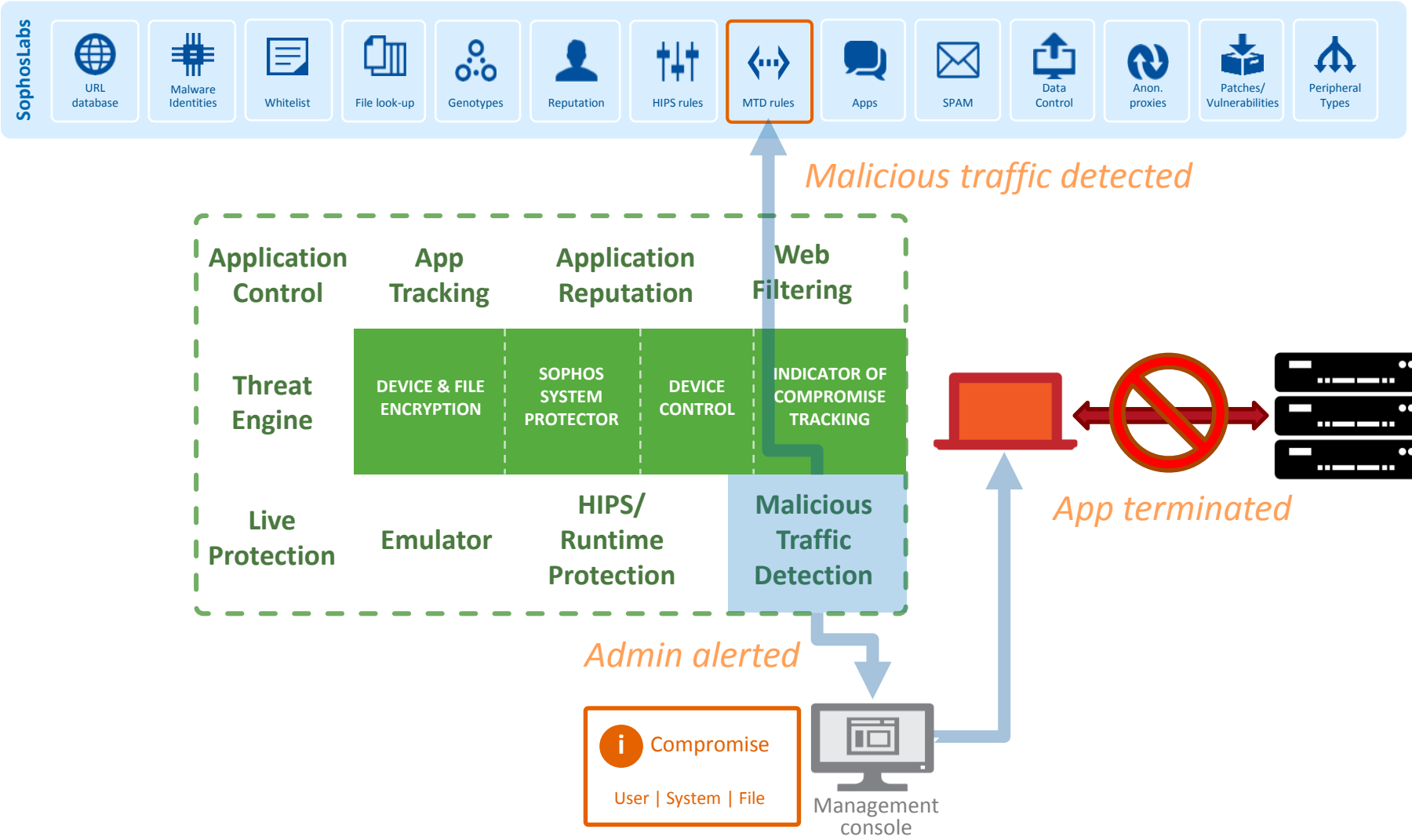


Perché rilevare il traffico “Malicious”?

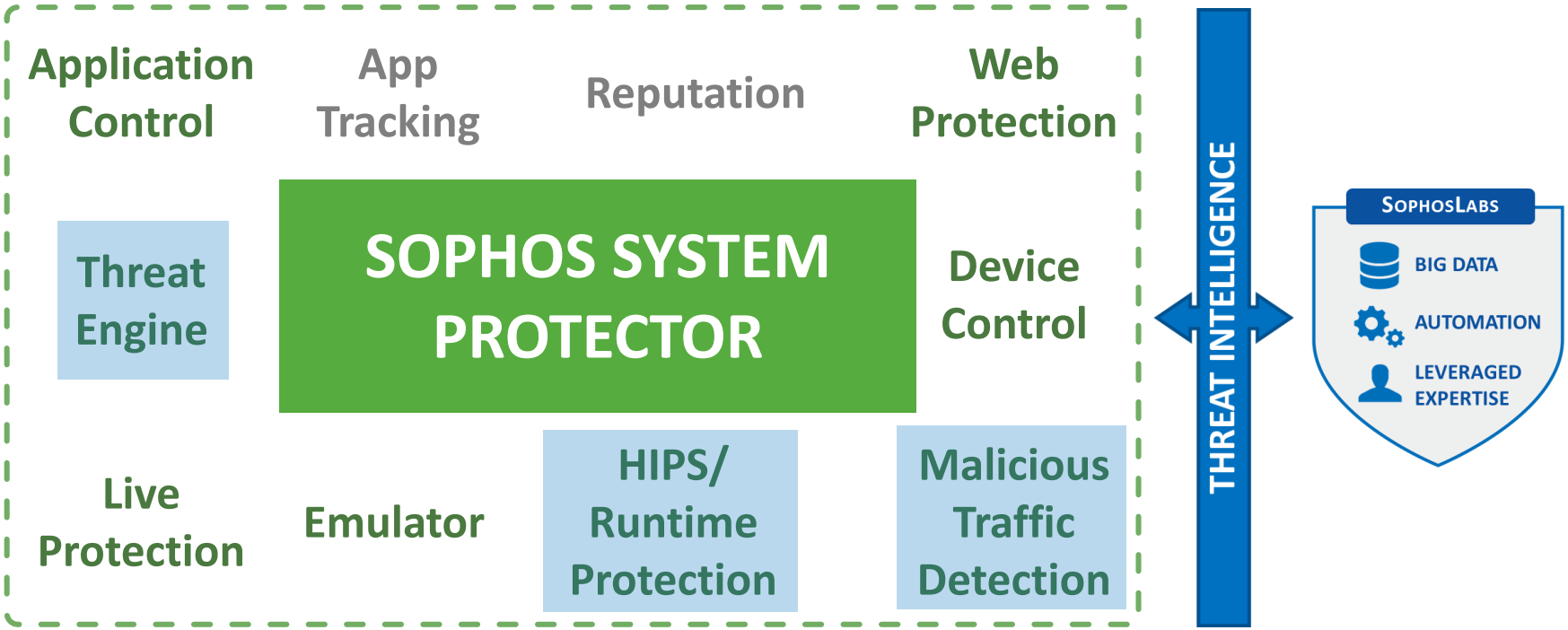
Vi piacerebbe sapere se uno dei vostri computer è stato compromesso e sta comunicando con i server degli attacker?



Come funziona la Malicious Traffic Detection



Esempio: nuova variante di Cryptowall



1. Uno user lancia qualche cosa che non dovrebbe. Viene inserita una nuova applicazione nella startup folder.
2. L'applicazione parte e inserisce se stessa in explorer.exe.
3. Explorer.exe tenta do scaricare le chiavi di cifratura da C&C.
4. Minaccia rimossa, admin avvisato.
5. Malware e indicatori della minaccia condivisi con SophosLabs.

Features, Packaging

	Sophos Cloud Endpoint Protection Standard	Sophos Cloud Endpoint Protection Advanced	Sophos Cloud Mobile Control	Sophos Cloud Enduser Protection	Sophos Cloud Server Protection Standard	Sophos Cloud Server Advanced
Anti-malware	✓	✓		✓	✓	
Web Security	✓	✓		✓	✓	
HIPS	✓	✓		✓	✓	
Live protection	✓	✓		✓	✓	
MTD		✓		✓		
Device Control		✓		✓		
Application Control		✓		✓		
Web Control		✓		✓		
Galileo Ready		✓		✓		
AD Sync		✓	✓	✓		
MDM			✓	✓		
Lockdown						✓
Policy type	User-based	User-based	User-based	User-based	Server-based	Server-based
Platform	Windows, Mac	Windows, Mac	iOS, Android	Windows, Mac, iOS, Android	Windows Server	Windows Server

Sophos Network Security Strategy

Grow Existing Businesses

Accelerate NGFW/UTM
Combine the strengths of Sophos and Cyberoam

Grow Secure Web Gateway
Revitalize technology and launch a hybrid offering

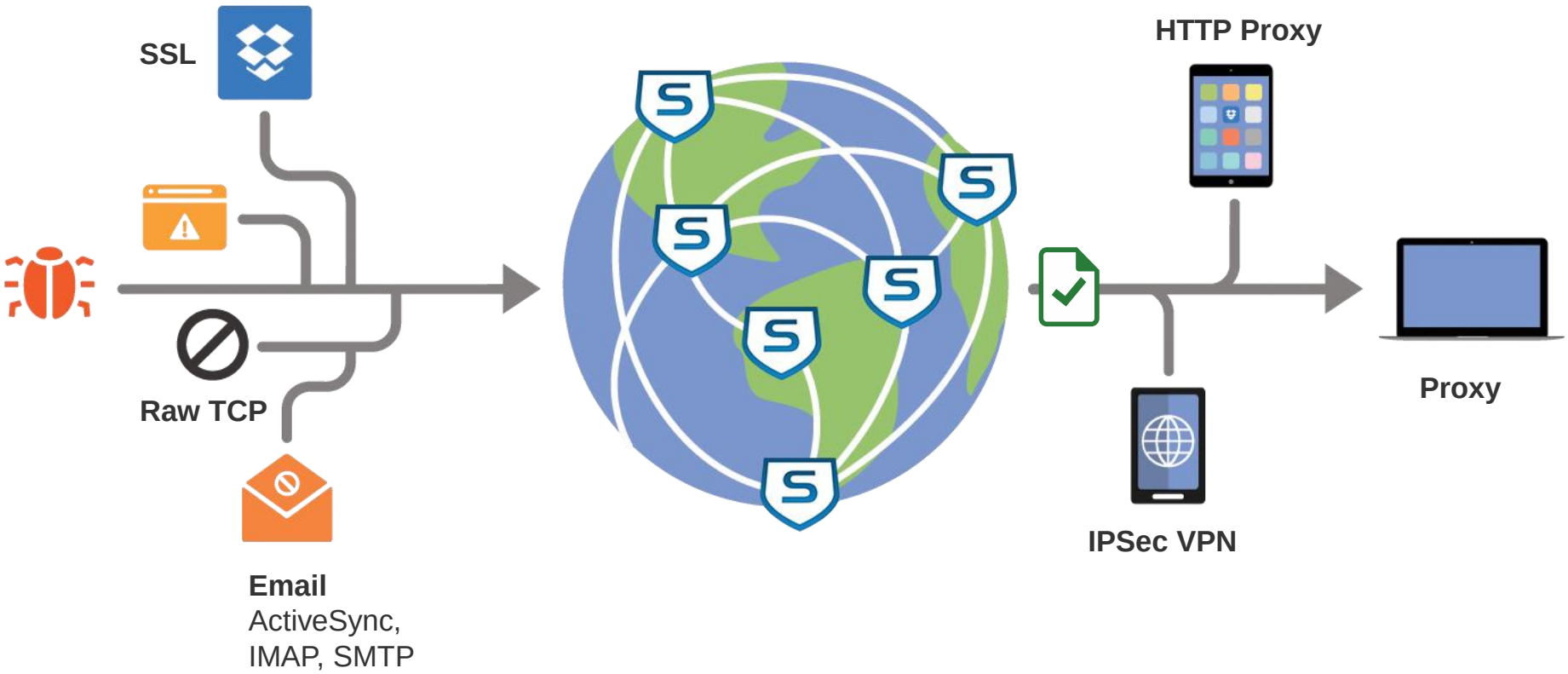
Grow Secure Email Gateway
Revitalize technology and launch a cloud offering

Cloud Web Gateway
Cloud management, enforcement, and reporting

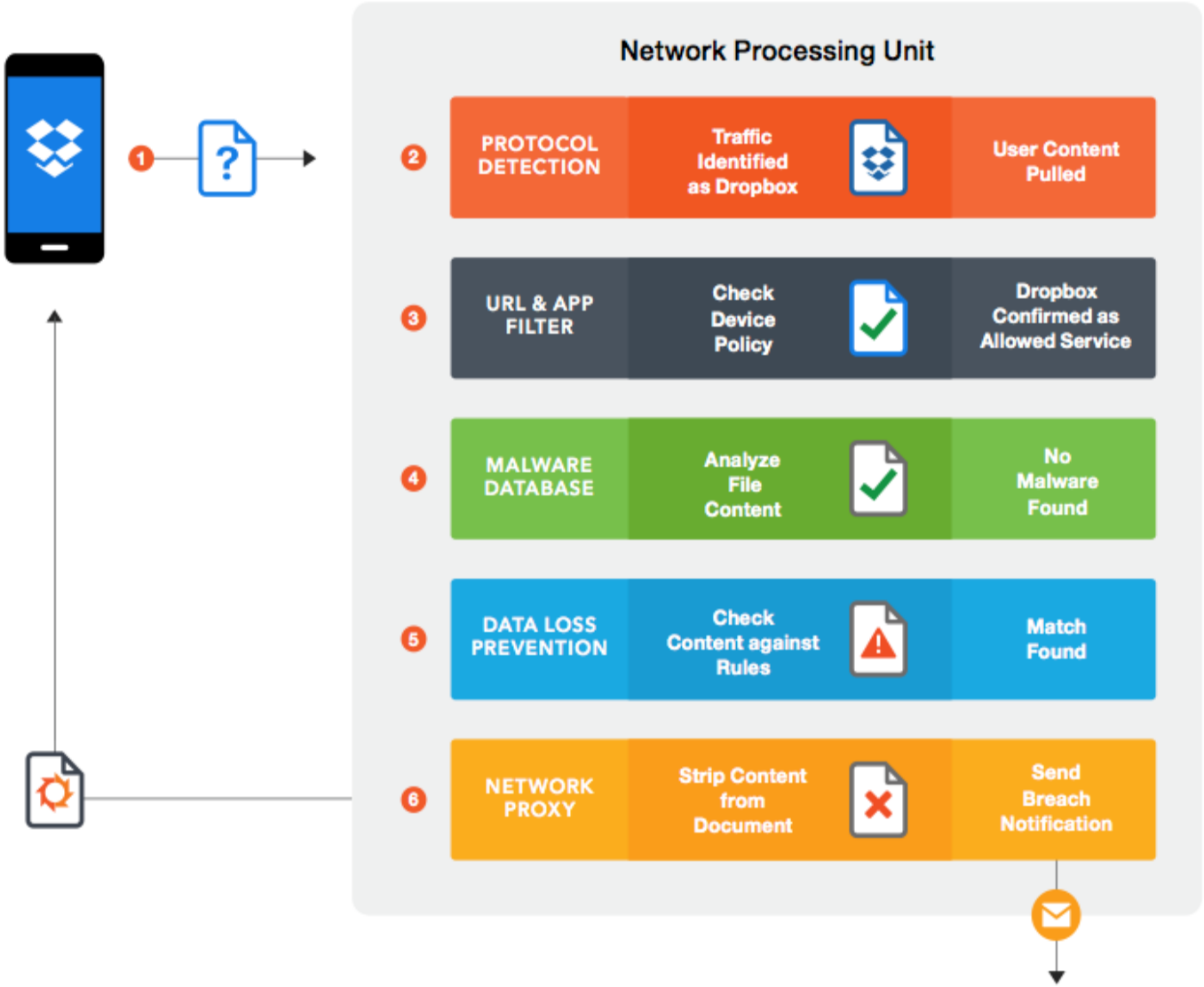
Sophos Web Appliance
New and improved!

Next-Gen SWG
Intelligent hybrid enforcement

Global Network Optimized for Mobile Workforce



Every Packet is Examined in Multistep Process



Supported Platforms

Mac & Windows Available Now, Android & iOS Available in Next 1-2 Months

Mac OS X 10.8.5+

Android 4.0+

Windows 7+

iOS 5.0+

SOPHOS

© Sophos Ltd. All rights reserved.