

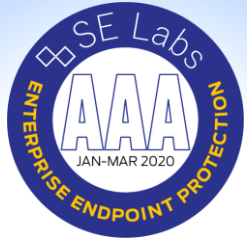
Sophos Central

Uroš Lolić

Security Technical Support Engineer



The World's Best Endpoint Protection



100% Total Accuracy

Enterprise
Protection



Winner

Best Endpoint
Security Solution

Gartner

Leader

Endpoint Protections
Platform Magic Quadrant



Perfect Score

Mac
Protection



#1

Malware
Protection



Winner

Best Small Business
Endpoint Protection



#1

Exploit
Protection

FORRESTER

Leader

Endpoint Security
Forrester Wave



Leader

Worldwide Mobile
Threat Management



**Editor's
Choice**

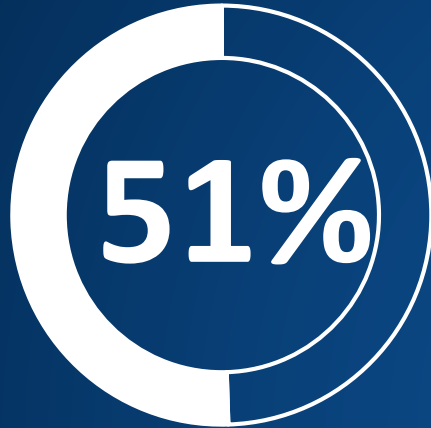
Prednost Cloud security rešenja i kako rasteretiti svoje resurse

- Rasterećenje postojećih resursa
- Automatizovan upgrade Administrativnih konzola, baza podataka i pratećih feature-a
- Uklonjena briga o održavanju neophodnih servera za rad On prem rešenja.
- Licenciranje servera, baza itd..

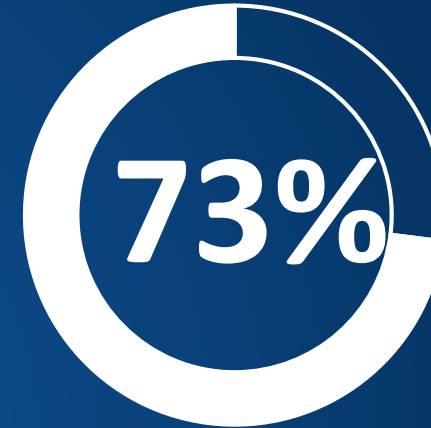
Intercept X *with EDR* III

Visibility

SOPHOS



of organizations were hit by ransomware
in the last year



of attack victims said the cybercriminal
succeeded in encrypting their data

The State of Ransomware 2020, Sophos

SOPHOS

The World's Best Endpoint Protection

Foundational



Known
Threats



Deep Learning



Unknown Executables



Anti-ransomware



Ransomware



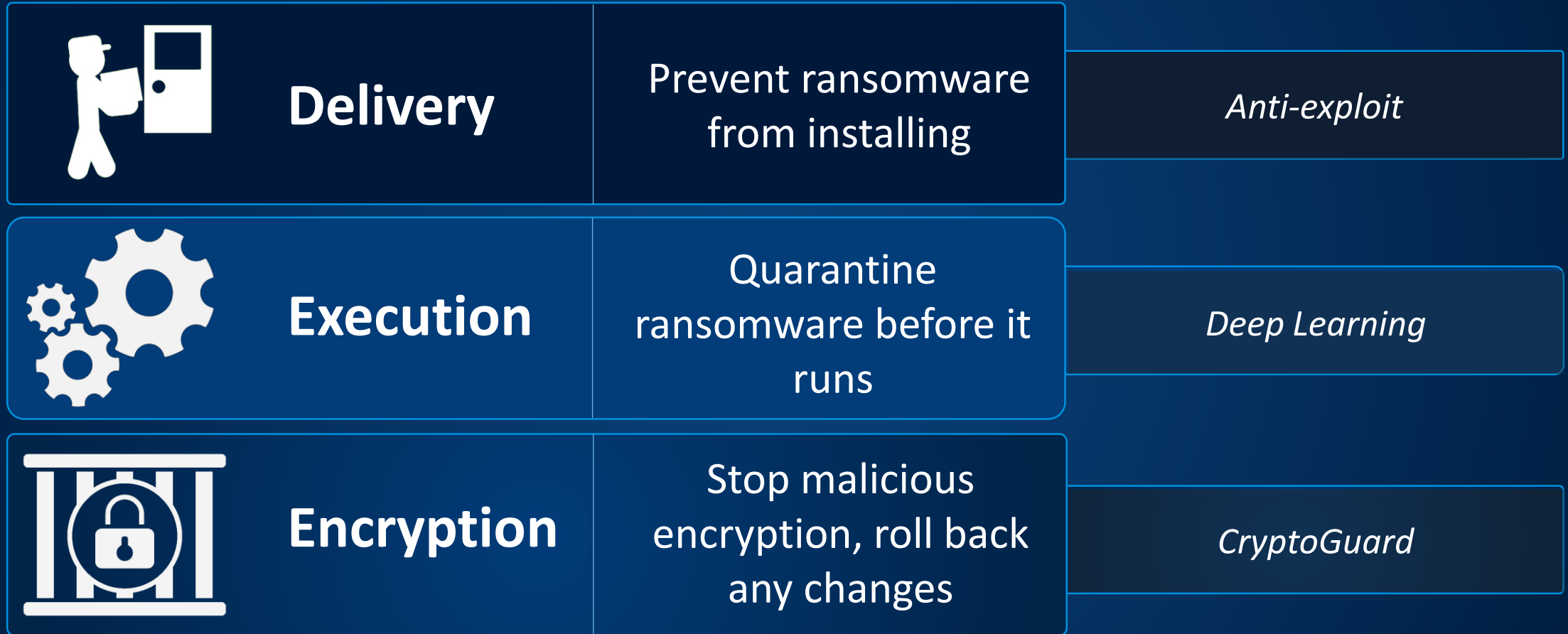
Anti-exploit



Exploits
File-less Attacks

Multiple Layers of Defense

Layers of Defense in Action



Get Detailed Threat Intelligence

- See where to start
- Apply context
 - Deep learning malware analysis
 - SophosLabs expert intelligence
- Take action with confidence

The screenshot displays the Sophos Threat Analysis Center interface. On the left is a navigation sidebar with 'Threat Indicators' selected. The main area shows a table of threat indicators with columns for 'First seen', 'File name', 'SHA-256', 'Suspicion', 'Devices affected', 'Executed', and 'Actions'. The table lists several files, including 'standardsetup1.exe', 'lister.exe', 'monitor util.exe', 'tweetcapture.exe', and 'installer.exe', all marked as 'High Suspicion' or 'Medium Suspicion'. A summary bar above the table shows 5 High, 7 Medium, and 4 Low suspicion items. A 'Clean and block' button is visible. An inset window shows 'Machine learning analysis' for 'fakedrop-cli.exe', indicating it is '84% Suspicious' based on analysis of 29 million good and 15 million bad items. Another inset shows 'File/path : 43% Suspicious' based on analysis of 1 million good and 23 million bad items, listing several file paths with their respective suspicion levels (High, Medium, or Low).

First seen	File name	SHA-256	Suspicion	Devices affected	Executed	Actions
Oct 23, 2019 8...	Threat Indicators Octobe...	32d14314d5d197ae0a40290fe8a...	High Suspicion	1	Yes	View details Generate threat ci
Oct 24, 2019 10...	standardsetup1.exe	8cec0fdc2ceaa8972c1def7c8e2c...	High Suspicion	1	Yes	View details Generate threat ci
Oct 24, 2019 10...	lister.exe	3e3be76b75923824ca621c60e7a...	High Suspicion	1	No	View details Generate threat ci
Oct 24, 2019 10...	monitor util.exe	025ab8a0fad4957062734814803...	High Suspicion	1	No	View details Generate threat ci
Oct 24, 2019 10...	tweetcapture.exe	a593c719e13a92d6130d48520b7...	High Suspicion	1	No	View details Generate threat ci
Oct 23, 2019 8...	installer.exe	ab8a3eb042db0a7633f4a4d00db...	Medium Suspicion	1	No	View details Generate threat ci

Close Security Gaps

The screenshot shows the Sophos Central Admin interface. On the left is a sidebar with navigation options: Admin, Endpoint Protection, Back to Overview, ANALYZE (Dashboard, Logs & Reports), DETECTION AND REMEDIATION (Threat Cases, Threat Searches), MANAGE PROTECTION (People, Computers), CONFIGURE (Policies, Settings, Protect Devices), and SOPHOS CENTRAL. The main area is titled 'Analyze' and shows a process tree diagram for 'recipeadictstool.exe'. The diagram shows the process tree starting from 'dropper.exe' which spawned 'recipeadictstool.exe'. This process then spawned 'Explorer' and 'dropper.exe' again. It also shows connections to '39 IP Addresses', 'Files', and 'Registry Keys'. A green notification box at the top right says 'Threat case recipeadictstool.exe - DESKTOP-M33EE38 has been generated.' The right pane shows 'Process details : recipeadictstool.exe' with tabs for 'Process details', 'Report summary', 'Machine learning analysis', 'File properties', and 'File breakdown'. The reputation is 'Uncertain' with a red-to-green gradient bar. The detection status is 'Not detected at time case was created'. Below that is 'SOPHOSLABS Threat Intelligence' with a 'Request Latest Intelligence' button. At the bottom, technical details are listed: Path: c:\users\martynroberts\downloads\recipeadictstool new 25 09 2018\recipeadictstool.exe, Name: recipeadictstool.exe, Process ID: 592, and SHA-256: 5e147d105b93a01b0756f2af2f44a8a27914c42d948c0e3051a2db3657c453.

- Determine root cause
- Identify scope of threat
- See where it was neutralized

Multi-Platform and OS Support



Sophos Endpoint
Intercept X



Sophos Server



Sophos Mobile



Windows



macOS



Windows



Linux



Android / iOS / Chromebook

Invest In a Security System

Sophos Central

SOPHOS CENTRAL Admin

Sophos Central Dashboard
See a snapshot of your security protection

Help ▾ chris mccormack ▾
sophos · Super Admin

Overview

- Dashboard
- Alerts
- Threat Analysis Center ▶
- Logs & Reports
- People
- Devices
- Global Settings
- Protect Devices

MY PRODUCTS

- Endpoint Protection ▶
- Server Protection ▶
- Mobile ▶
- Encryption ▶
- Wireless ▶
- Firewall Management ▶
- Phish Threat ▶

Most Recent Alerts [View All Alerts](#)

⚠	Dec 16, 2019 12:59 PM	An attempt to communicate with a botnet or command and control s...
!	Dec 16, 2019 12:54 PM	Sophos Firewall detected malicious connections: 'C2/Generic-C' at '/...' Mac-Server\Chris Mac-Server
!	Dec 16, 2019 12:54 PM	Malicious connection detected: 'C2/Generic-A' at '/Users/Chris/Deskt...' Mac-Server\Chris Mac-Server
!	Dec 16, 2019 12:54 PM	Sophos Firewall detected malicious connections: 'C2/Generic-C' at '/...' Mac-Server\Chris Mac-Server
!	Dec 16, 2019 12:54 PM	Malicious connection detected: 'C2/Generic-A' at '/Users/Chris/Deskt...' Mac-Server\Chris Mac-Server

Devices and users: summary [See Report](#)

Endpoint Computer Activity Status

- 5 Active
- 0 Inactive 2+ Weeks
- 0 Inactive 2+ Months
- 0 Not Protected

Endpoint and server web control [See Reports](#)

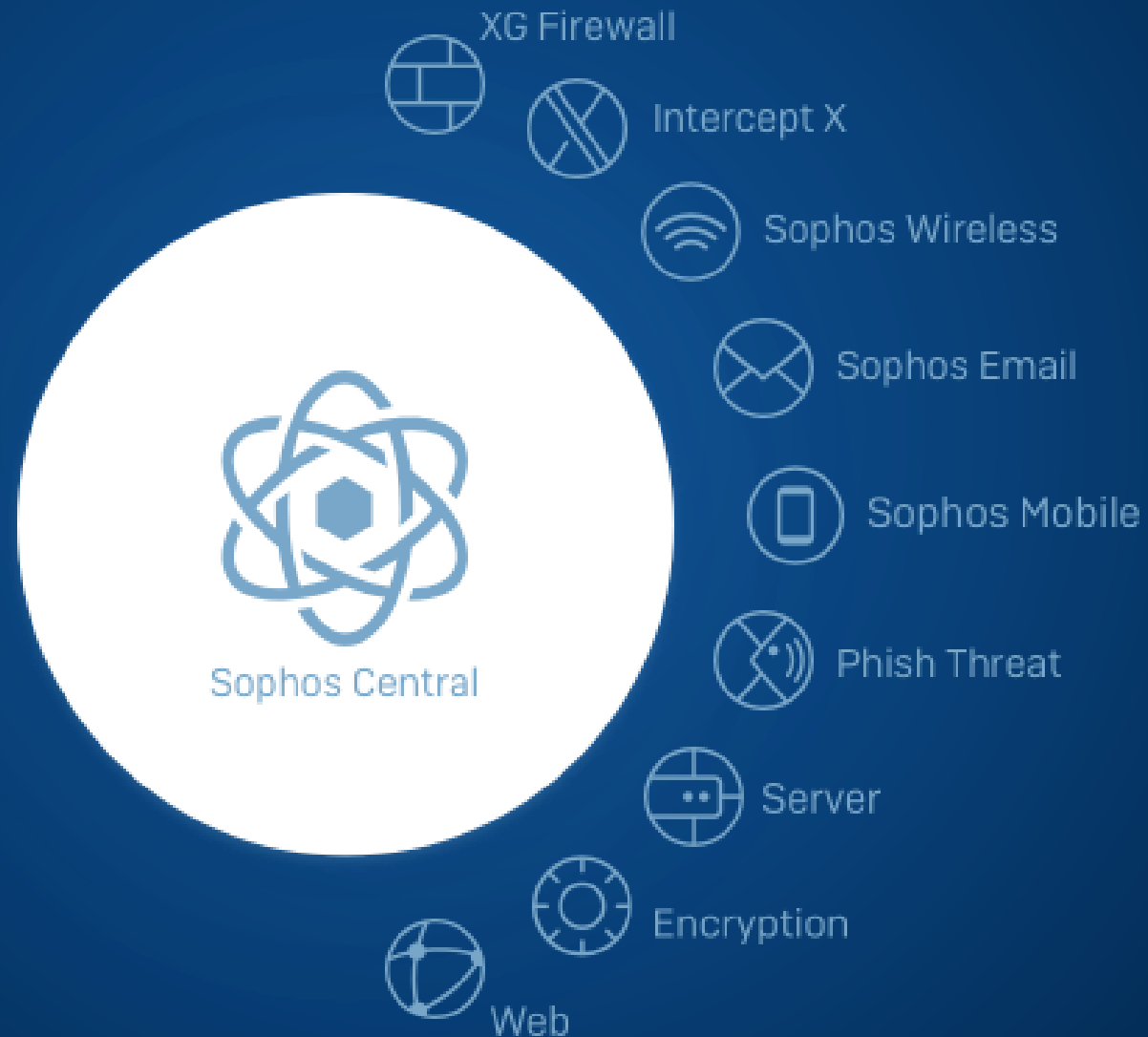
No pages blocked or warned about in the last 30 days.

last 30 days

Unified Endpoint Management [Go to product dashboard](#)

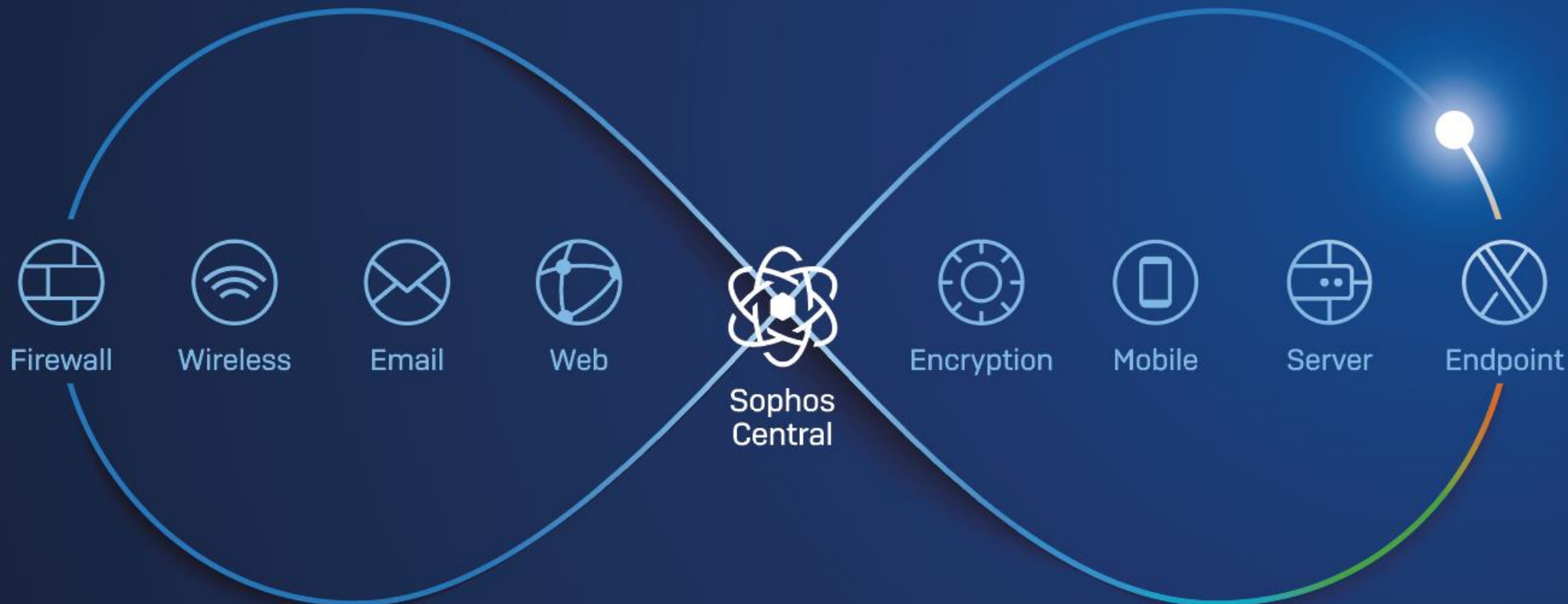
Unique: A Complete Cybersecurity Ecosystem Managed from One Console

The Most Comprehensive Cloud Platform



Synchronized Security

Cybersecurity as a System





XG

Firewall

Xstream

XG Firewall's Winning Advantages

The world's best visibility, protection, and response

Flexible Networking

- ✓ Flexible, Fast, Reliable XG Series Hardware
- ✓ Simple Remote User and Site Connectivity
- ✓ SD-WAN Evolved

The Best Visibility, Protection, Response

- ✓ Expose hidden risks
- ✓ Xstream DPI Engine, TLS, AI Protection
- ✓ Security Heartbeat Threat Isolation

Easy Management

- ✓ Sophos Central - One Console to Manage it All
- ✓ The Ultimate Experience
- ✓ Built-in Expertise

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

Hosts and services

Administration

Backup & firmware

Certificates

Control center

XG230 [SFOS 17.5.0 Beta-1] C240773Y2QQXTCA

How-to guides Log viewer Help admin
Sophos

System

Performance

Interfaces

Services

VPN

0/0
RED

0
Connected remote users

CPU
Bandwidth

3/3
Wireless APs

11
Live users

Memory
Sessions

High availability: **Not configured**

Sophos Firewall Manager: **Not configured**

Running for 12 day(s), 23 hour(s), 46 minute(s)

Active firewall rules
2 Unused

6
Business

5
User

13
Network

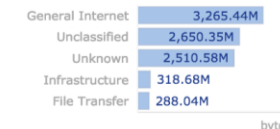
13
Total

Traffic insight

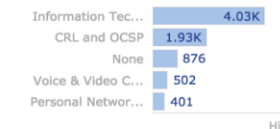
Web activity 621 max | 150 avg



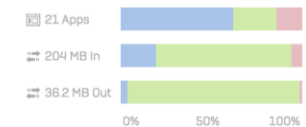
Allowed app categories



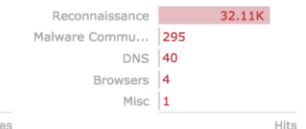
Allowed web categories



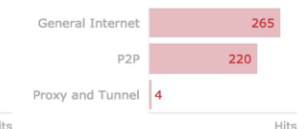
Cloud applications



Network attacks



Blocked app categories



User & device insights

Security Heartbeat®



Synchronized Application Control™



Sandstorm



ATP UTQ



Click on widgets to open details

Reports

15
Yesterday

192
Yesterday

7821
MB

Messages

Warning
HTTPS-based management is allowed from the WAN ...

1w ago



XG Firewall's Winning Network Advantages

Industry leading connectivity, simplicity, and performance

1. XG Series - Flexible, Fast, Reliable

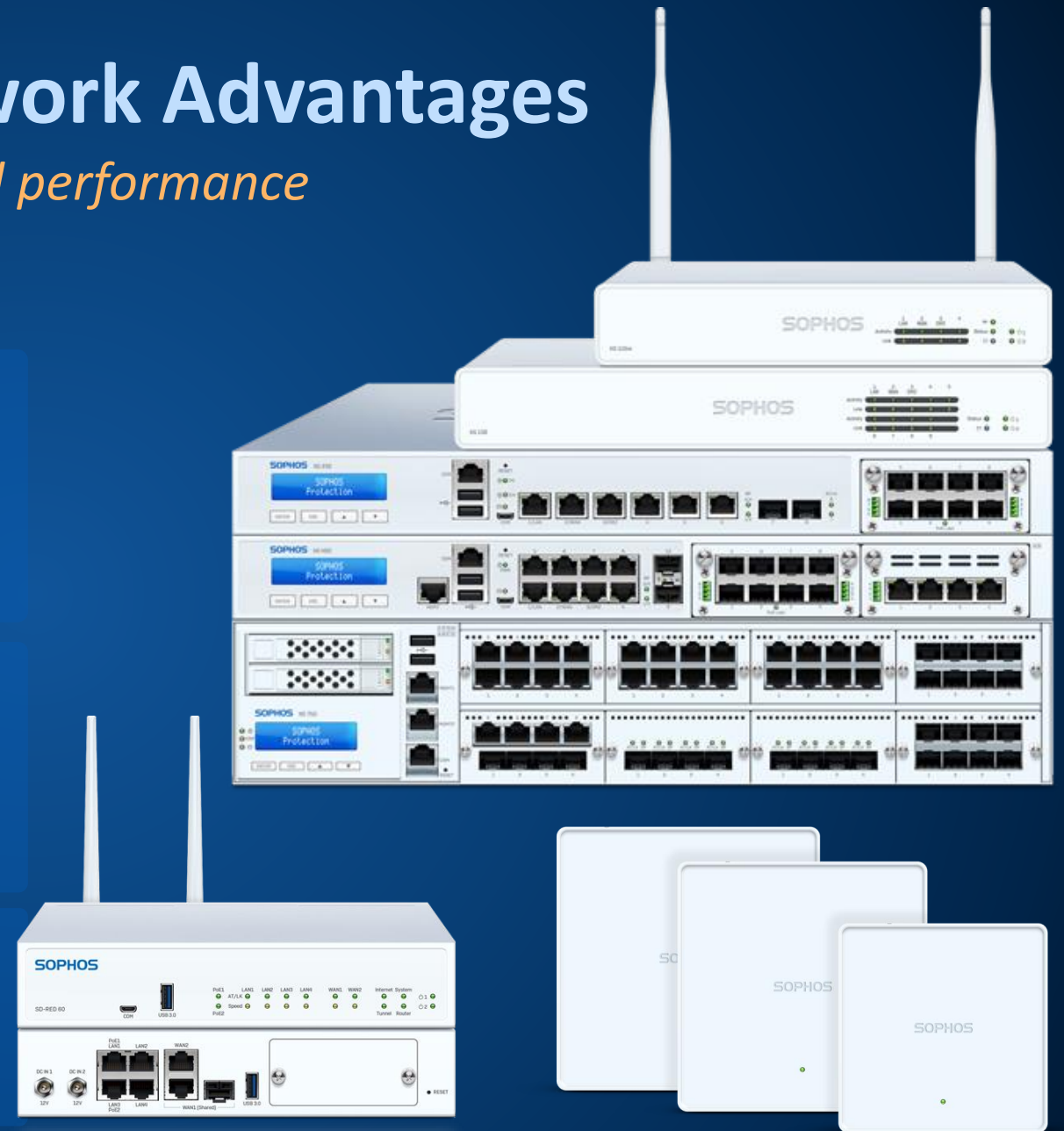
- ✓ Excellent price-performance
- ✓ Modular connectivity for copper, fiber, or LTE
- ✓ Plug-and-play HA and redundant power supply options

2. Simple Remote User and Site Connectivity

- ✓ SD-RED - affordable, simple branch office devices
- ✓ Easy VPN orchestration tools
- ✓ Free IPsec and SSL VPN client remote access

3. SD-WAN Evolved

- ✓ Multiple WAN options (copper, fiber, cellular)
- ✓ WAN Link monitoring and fail-over, fail-back
- ✓ Synchronized SD-WAN for optimized app routing



Flexible Deployment Options



XG Series
Appliance



Software or Virtual
Appliance



Public Cloud
(AWS/Azure)

XG Series Next-Gen Firewall Appliances

SMB & Branch Office Desktop

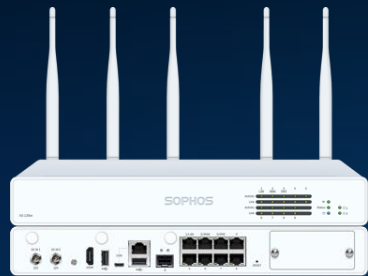


XG 86(w)



XG 106(w)

XG 115(w)



XG 125(w)

XG 135(w)

Distributed Edge 1U Rackmount



XG 210

XG 230



XG 310

XG 330



XG 430

XG 450

Performance 2U Rackmount



XG 550



XG 650


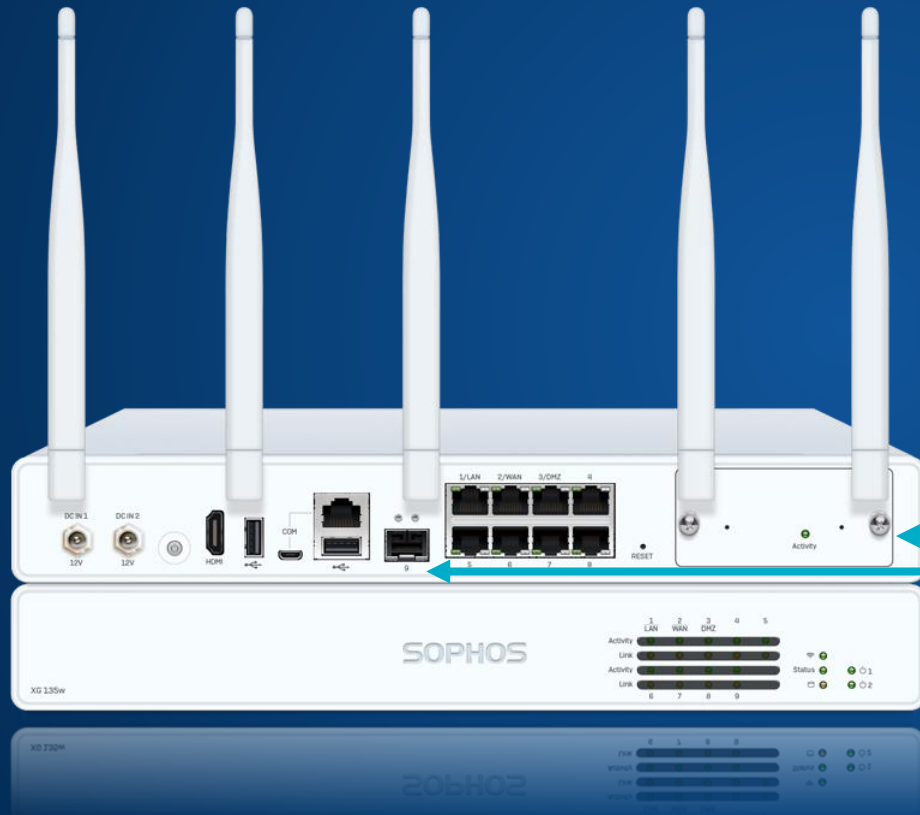
Data Center 2U Rackmount



XG 750

XG Series Desktop Models

Flexibility to fit any network – Multiple WAN options for SD-WAN



Connectivity
WiFi, Cellular, Copper, Fiber, and DSL Modem options

Multiple WAN options















Nobody can match this in a single appliance

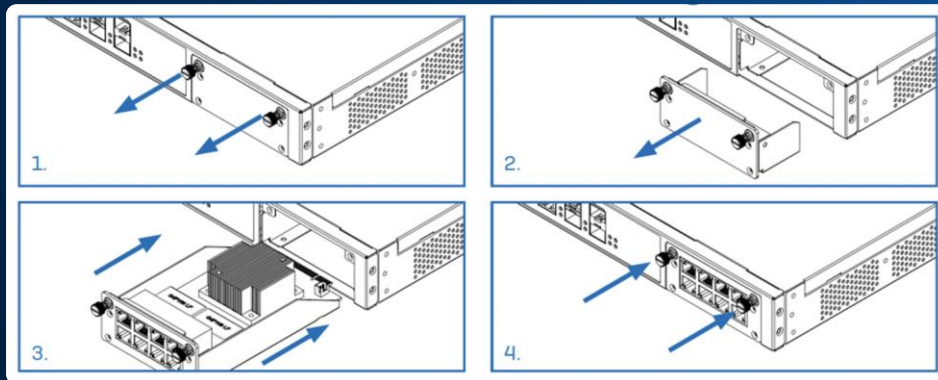
Unique: XG 125(w)/135(w) Flexible Connectivity Options

Flexible Connectivity for Any Network

Extensive line of Flexi Port Modules for 1U and 2U models

- Add more ports
- Add fiber connectivity: SFP (1 GE), SFP+ (10 GE), QSFP+ (40 GE)
- Add (more) bypass ports for fail-open deployment
- Add PoE to connect external devices (1U only)

Flexi Port Modules for 1U	Flexi Port Modules for 2U
 <p>8 port GbE copper Flexi Port module (for SG/XG 2xx/3xx/4xx only)</p>	 <p>8 port GbE copper Flexi Port module (for XG 750 and SG/XG 550/650 Rev.2 only)</p>
 <p>8 port GbE SFP Flexi Port module (for SG/XG 2xx/3xx/4xx only)</p>	 <p>8 port GbE SFP Flexi Port module (for XG 750 and SG/XG 550/650 Rev.2 only)</p>
 <p>2 port 10 GbE SFP+ Flexi Port module (for SG/XG 2xx/3xx/4xx only)</p>	 <p>2 port 10 GbE SFP+ Flexi Port module (for XG 750 and SG/XG 550/650 Rev.2 only)</p>
 <p>4 port 10 GbE SFP+ Flexi Port module (for SG/XG 2xx/3xx/4xx only)</p>	 <p>4 port 10 GbE SFP+ Flexi Port module (for XG 750 and SG/XG 550/650 Rev.2 only)</p>
 <p>4 port GbE copper LAN bypass Flexi Port module (for XG 2xx/3xx/4xx only)</p>	 <p>4 port GbE SFP plus 4 port GbE copper LAN bypass Flexi port module (for XG 750 and XG 550/650 Rev.2 only)</p>
 <p>2 port 40 GbE QSFP+ Flexi Port module (for SG/XG 210 Rev.3 and SG/XG 230, 3xx and 4xx Rev.2 only)</p>	 <p>2 port 40 GbE QSFP+ Flexi Port module (for XG 750 and SG/XG 550/650 Rev.2 only)</p>
 <p>4 port GbE copper PoE Flexi Port module (for SG/XG 210 Rev.3 and SG/XG 230, 3xx and 4xx Rev.2 only)</p>	
 <p>8 port GbE copper PoE Flexi Port module (for SG/XG 210 Rev.3 and SG/XG 230, 3xx and 4xx Rev.2 only)</p>	



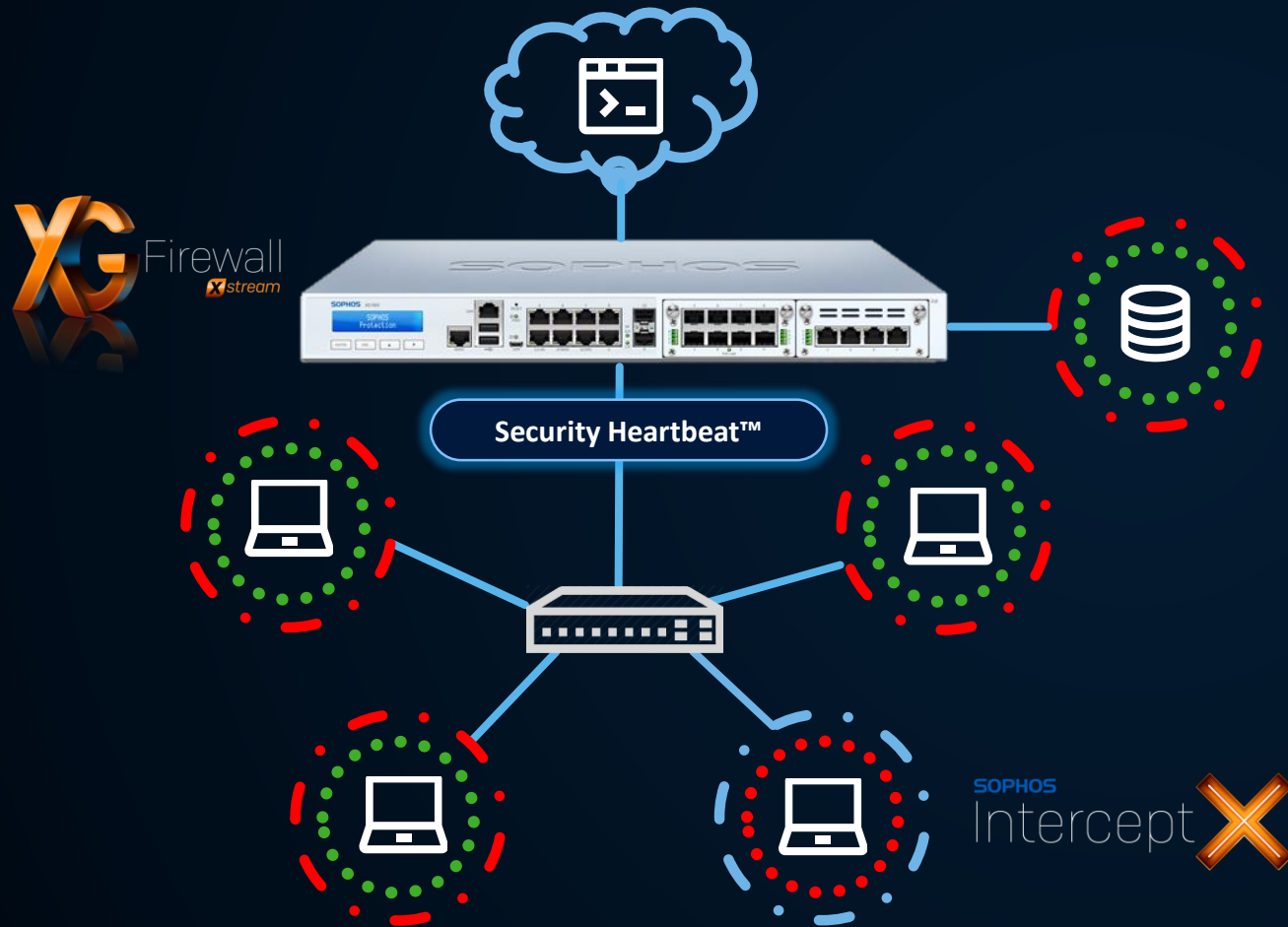
Synchronized Security



Unique: Synchronized Security Integration of Cybersecurity Products

Synchronized Security Heartbeat

Automatic Response to Threats and Breaches



1

Threat Identified

XG Firewall identifies the presence of a threat or a change in the health via Security Heartbeat

Security Heartbeat®

1	0	1	2
At risk	Missing	Warnings	Connected

2

Lateral Movement Protection

Firewall communicates via Security Heartbeat with other Endpoints to advise them of the compromised host to prevent spread

Wireless - APX Wave 2 Access Points

Faster, Better, Plug-and-Play Wi-Fi



Faster Connectivity – up to 2.3Gbps

High density – high capacity

Dual Radios – multiple SSIDs

APX 740

Flagship 4x4:4

APX 530

High performance 3x3:3

APX 320

2x2:2 Medium performance

APX 120

2x2:2 Affordable performance

SOPHOS

Regionalni distributer i Partner za Srbiju

Smart d.o.o.

office@smart.rs

+381 65 47 28 200