Seeing the Future: Sophos Introduces Deep Learning into its Synchronized Security Portfolio

Malay Upadhyay
Senior Sales Engineer

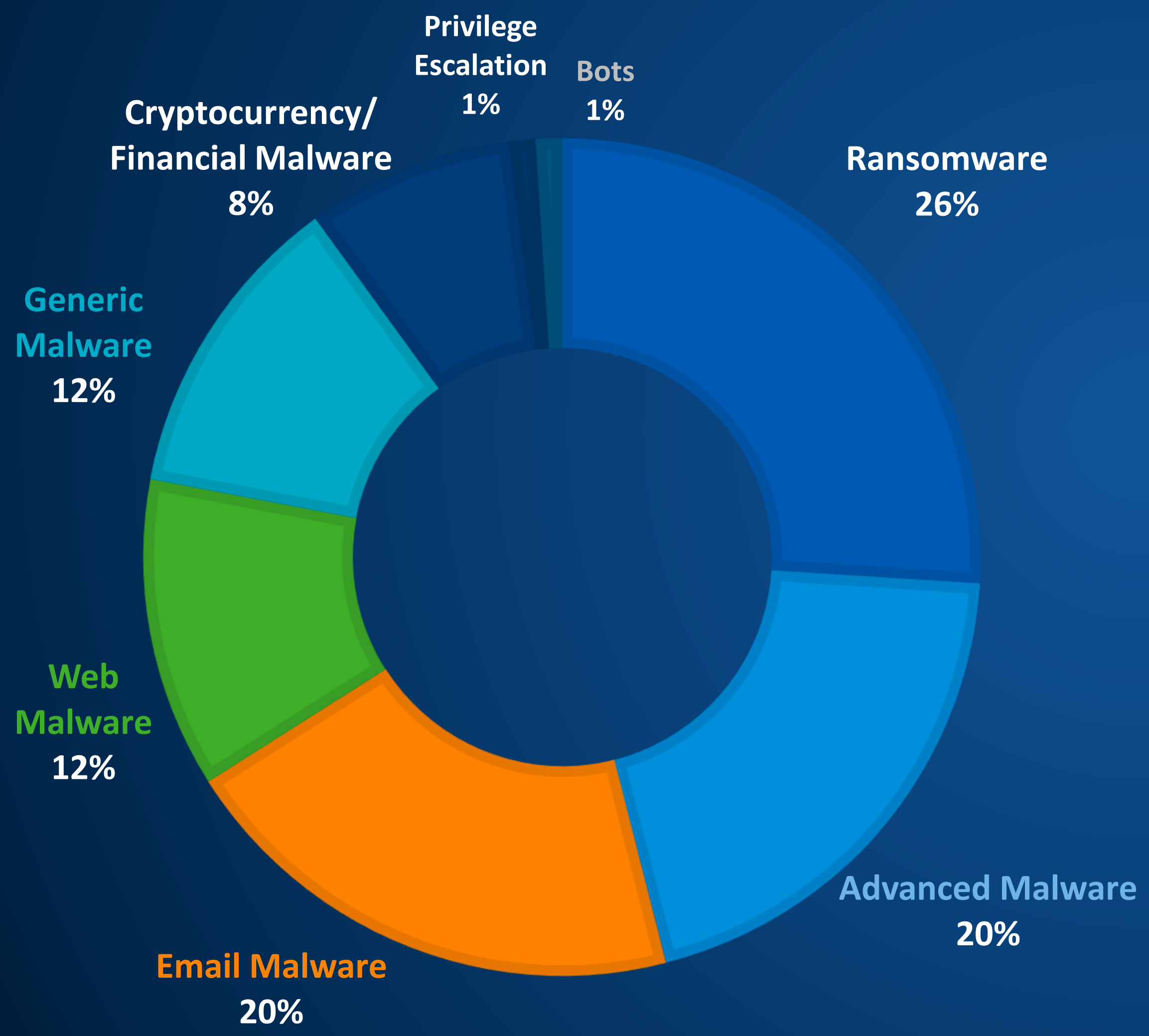
19/04/2018

SOPHOS

Threat Landscape

SOPHOS

The Threat Landscape Has Shifted



Source: SophosLabs

Ransomware

54% of organizations hit twice on average in 2017^

Advanced Threats

83% agree it has become more difficult to stop threats ^

Exploits

Most organizations have no exploit prevention^

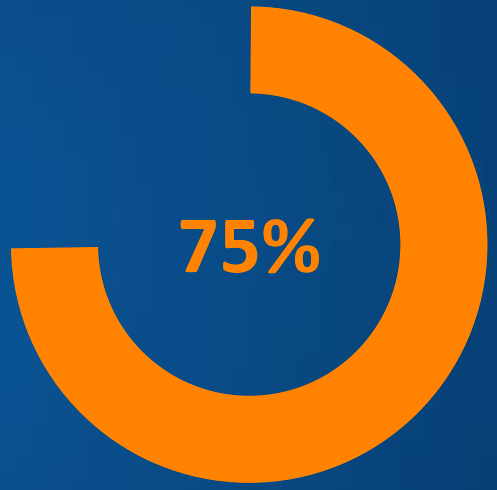
SOPHOS

^Source: The State of Endpoint Security Today Survey

Threats are unknown, making them harder to detect

400,000

SophosLabs receives and processes 400,000 previously unseen malware samples each day.



75% of the malicious files SophosLabs detects are found only within a single organization.

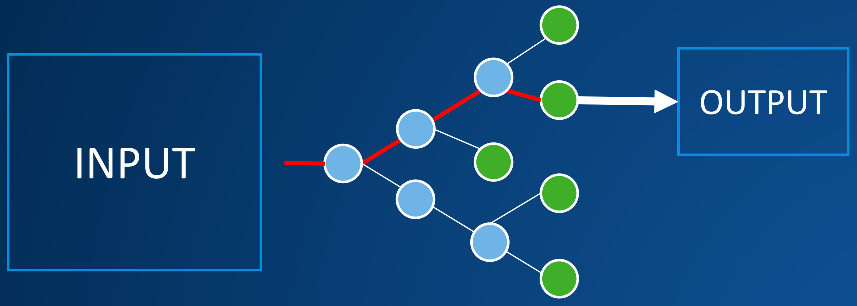
Source: SophosLabs

Predictive Security with Deep Learning

SOPHOS

Machine Learning Vs. Deep Learning

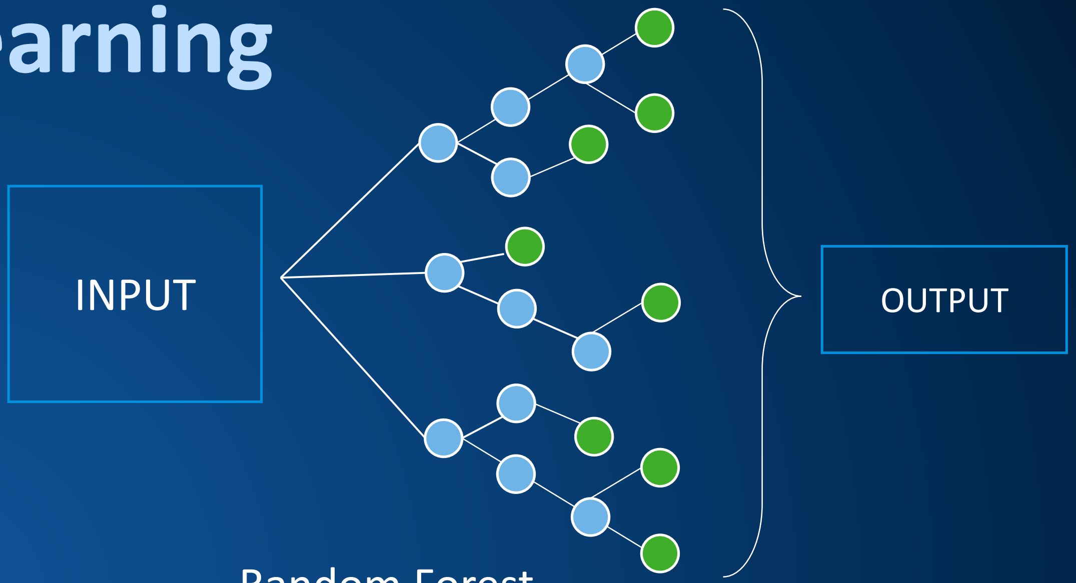
MACHINE LEARNING



INPUT

OUTPUT

Decision Tree

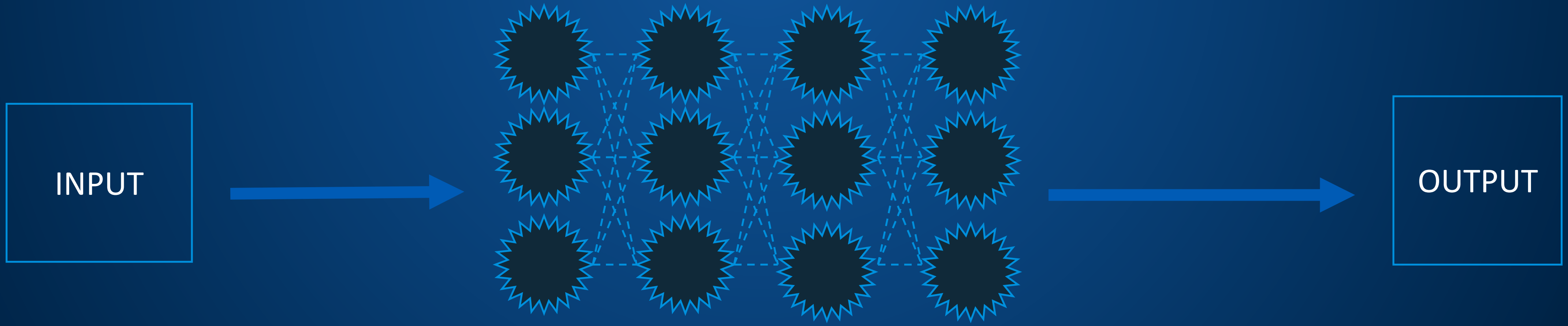


INPUT

OUTPUT

Random Forest

DEEP LEARNING



INPUT

OUTPUT

Interconnected Layers of Neurons, Each Identifying More Complex Features

Sophos Deep Learning

- Based on deep neural networks – comparable to the human brain
- Detects known and unknown threats without signatures
- Extremely fast – typical detection in < 20ms
- No internet connection needed – works offline
- Works out-of-the-box, no training on customer environment necessary
- Very reliable – lowest False Positive rate
- Profits from 30 years of experience and 100s of millions of samples
- Proven – very effective in independant tests!

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

VIRUS TOTAL

NSS LABS

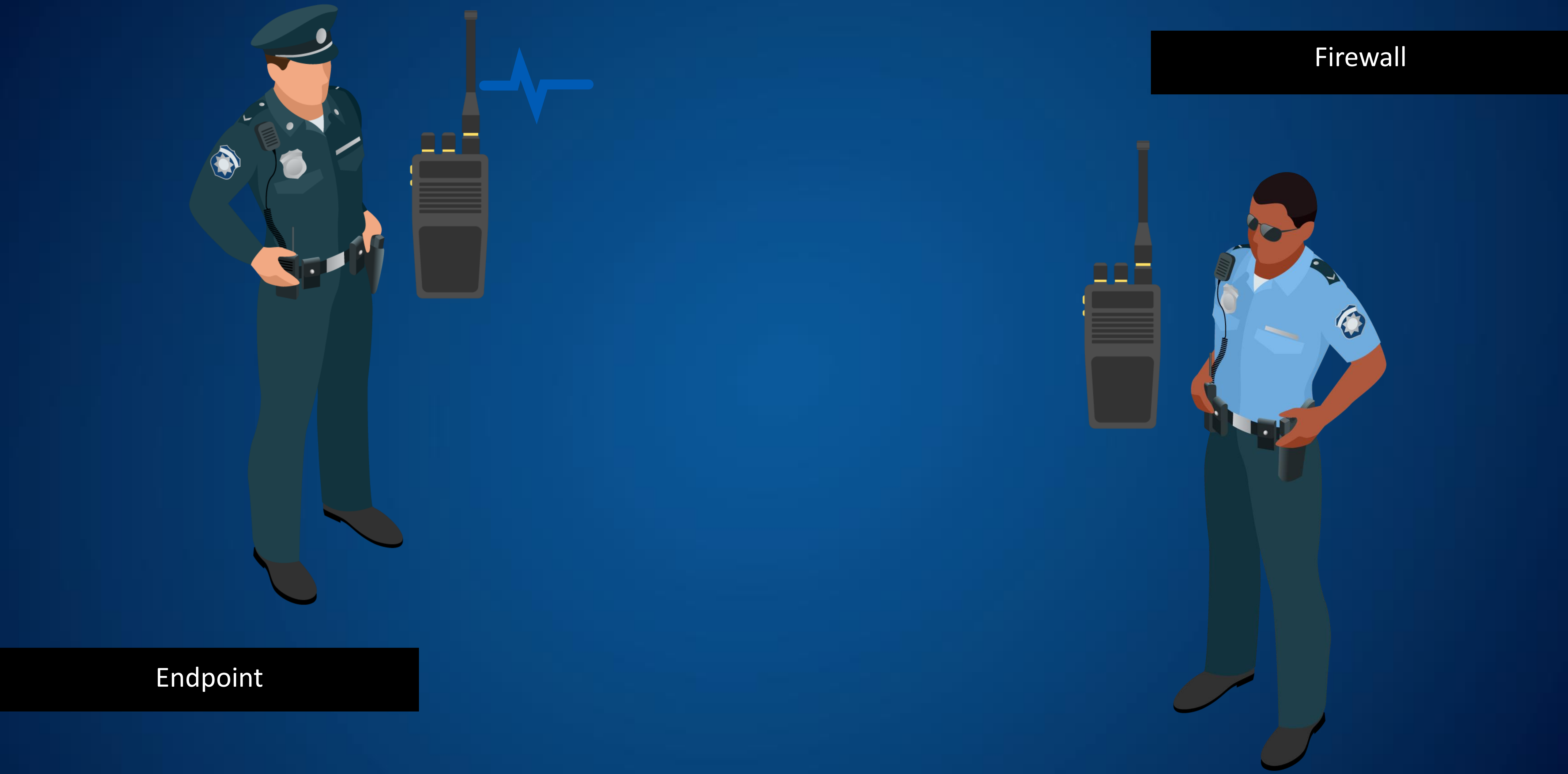
AV TEST av-test.org APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS

Synchronized Security

SOPHOS

Synchronized Security

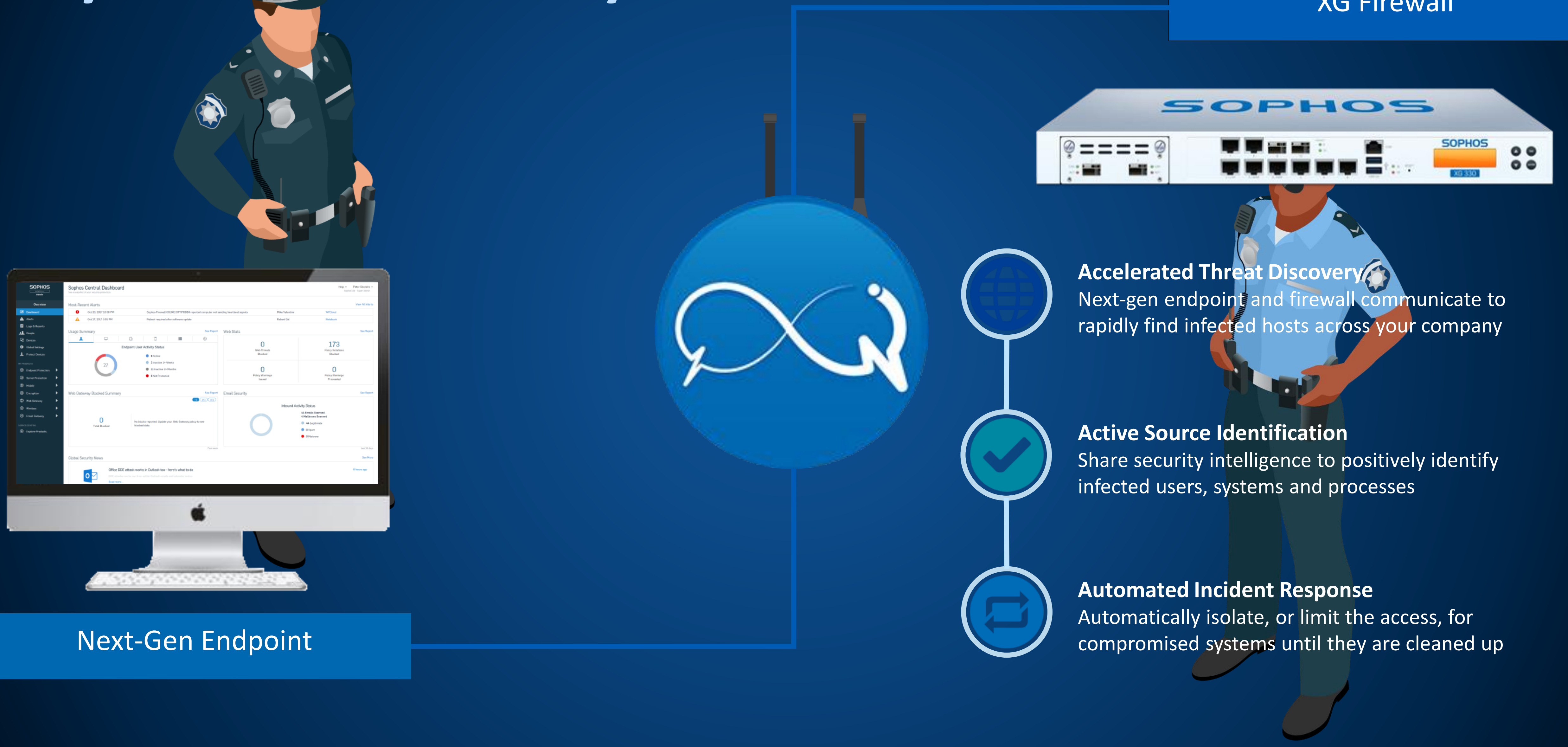
Linking Network and Endpoint security to deliver unparalleled protection by automating threat discovery, analysis, and response.



Endpoint

Firewall

Synchronized Security

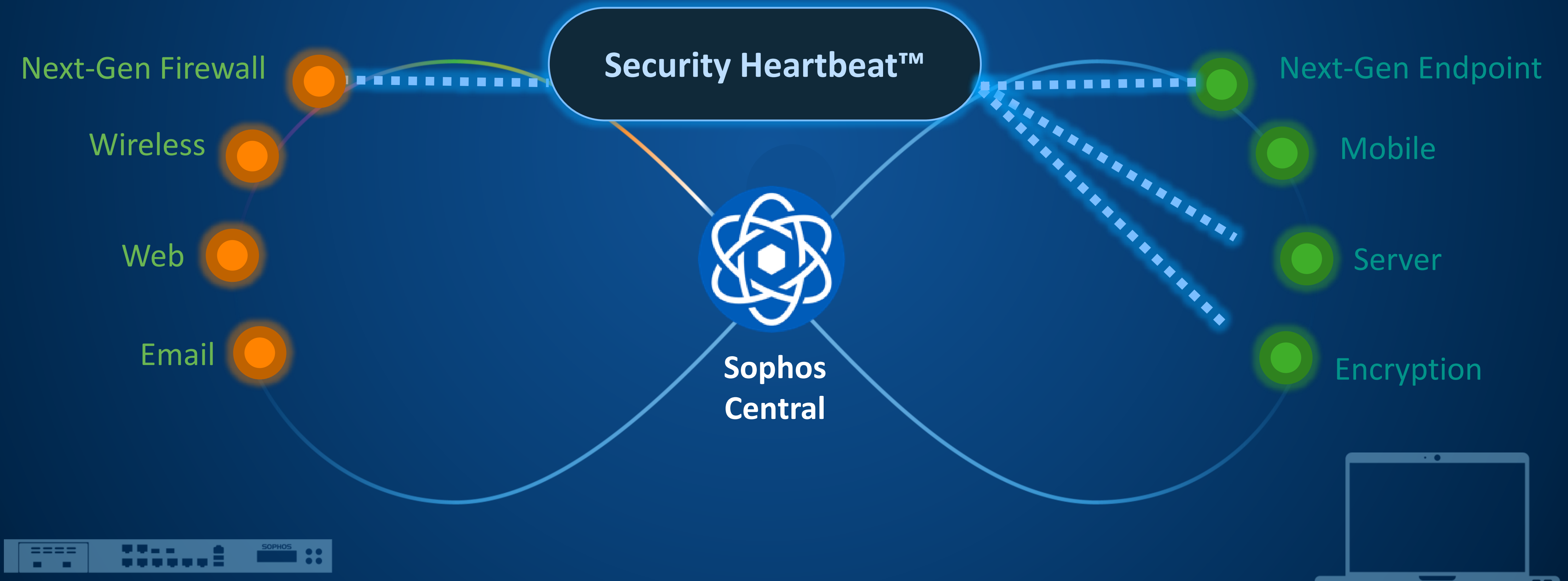


Accelerated Threat Discovery
Next-gen endpoint and firewall communicate to rapidly find infected hosts across your company

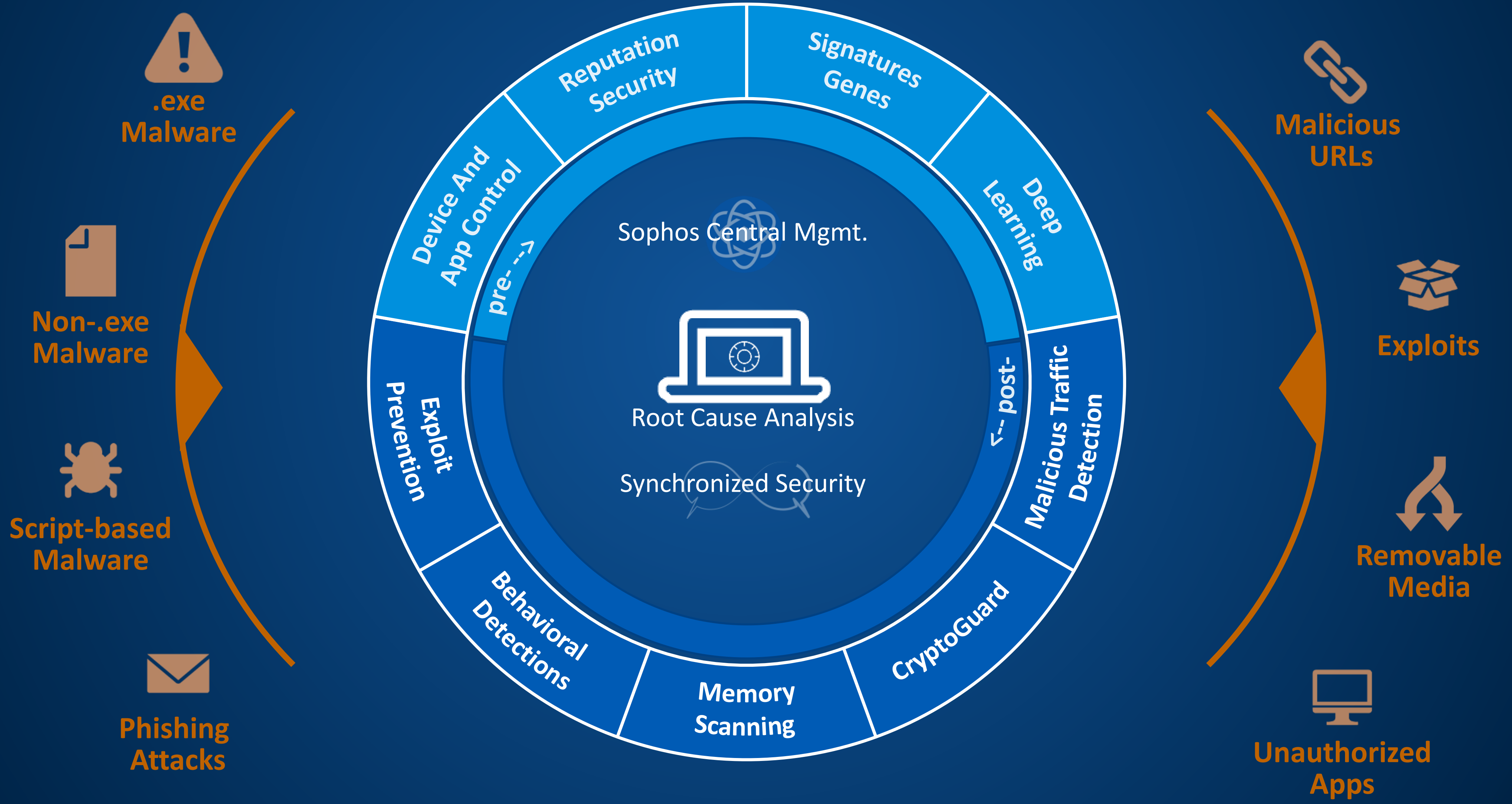
Active Source Identification
Share security intelligence to positively identify infected users, systems and processes

Automated Incident Response
Automatically isolate, or limit the access, for compromised systems until they are cleaned up

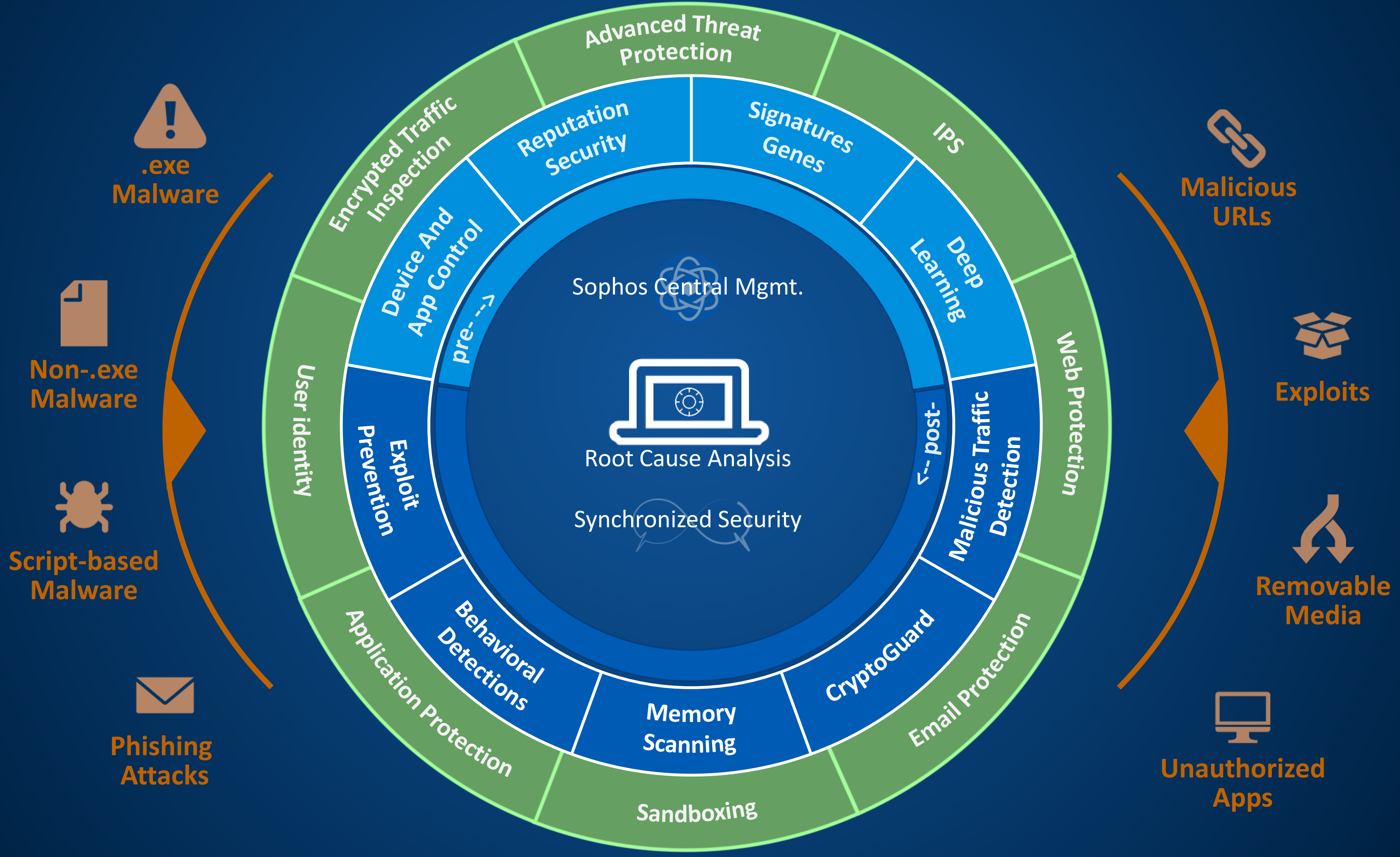
Sophos Synchronized Security



Next-Gen Endpoint



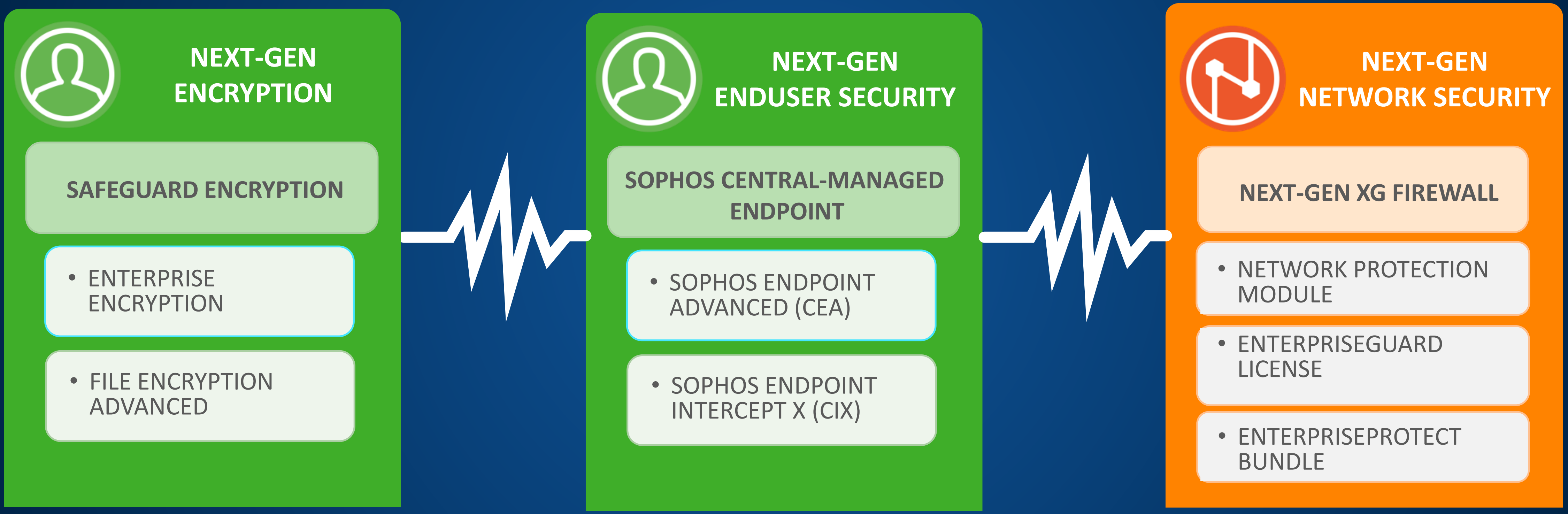
Next-Gen Endpoint + Network Protection



Synchronized Security Products

SOPHOS

Accessing Synchronized Security



NEXT-GEN ENCRYPTION

SAFEGUARD ENCRYPTION

- ENTERPRISE ENCRYPTION
- FILE ENCRYPTION ADVANCED

NEXT-GEN ENDUSER SECURITY

SOPHOS CENTRAL-MANAGED ENDPOINT

- SOPHOS ENDPOINT ADVANCED (CEA)
- SOPHOS ENDPOINT INTERCEPT X (CIX)

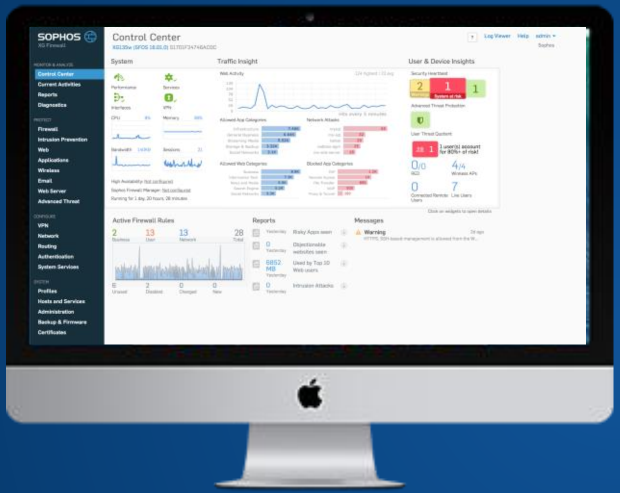
NEXT-GEN NETWORK SECURITY

NEXT-GEN XG FIREWALL

- NETWORK PROTECTION MODULE
- ENTERPRISEGUARD LICENSE
- ENTERPRISEPROTECT BUNDLE

Sophos XG Firewall

Solving today's top problems with existing Firewalls



Simpler to manage

- ✓ Streamlined workflows
- ✓ Unified policies
- ✓ Policy templates

Instant visibility

- ✓ New control center
- ✓ User & App Risk
- ✓ On-box reporting

Complete protection

- ✓ Firewall & Wireless
- ✓ Web, APT, Apps
- ✓ Email and WAF
- ✓ Sandboxing

Synchronized security

- ✓ Linking firewall & EP
- ✓ Security Heartbeat™
- ✓ Dynamic app ID

Top performance

- ✓ Industry-leading HW
- ✓ FastPath optimization
- ✓ High-performance proxy

Central Management

- ✓ Full-featured & consistent
- ✓ Cloud or on-premise
- ✓ Free for partners

Sophos INTERCEPT X

In addition to Endpoint Protection

Protection against Ransomware & Co

- **Deep Learning** detects unknown Malware
- **CryptoGuard** detects **Encryption** and restores the original files

Anti-Hacker

- **Signatureless Protection** against Zero-Day attacks
- **Exploit** Detection
- **Anti-Hacker** technologies
- **Credential Theft Protection**

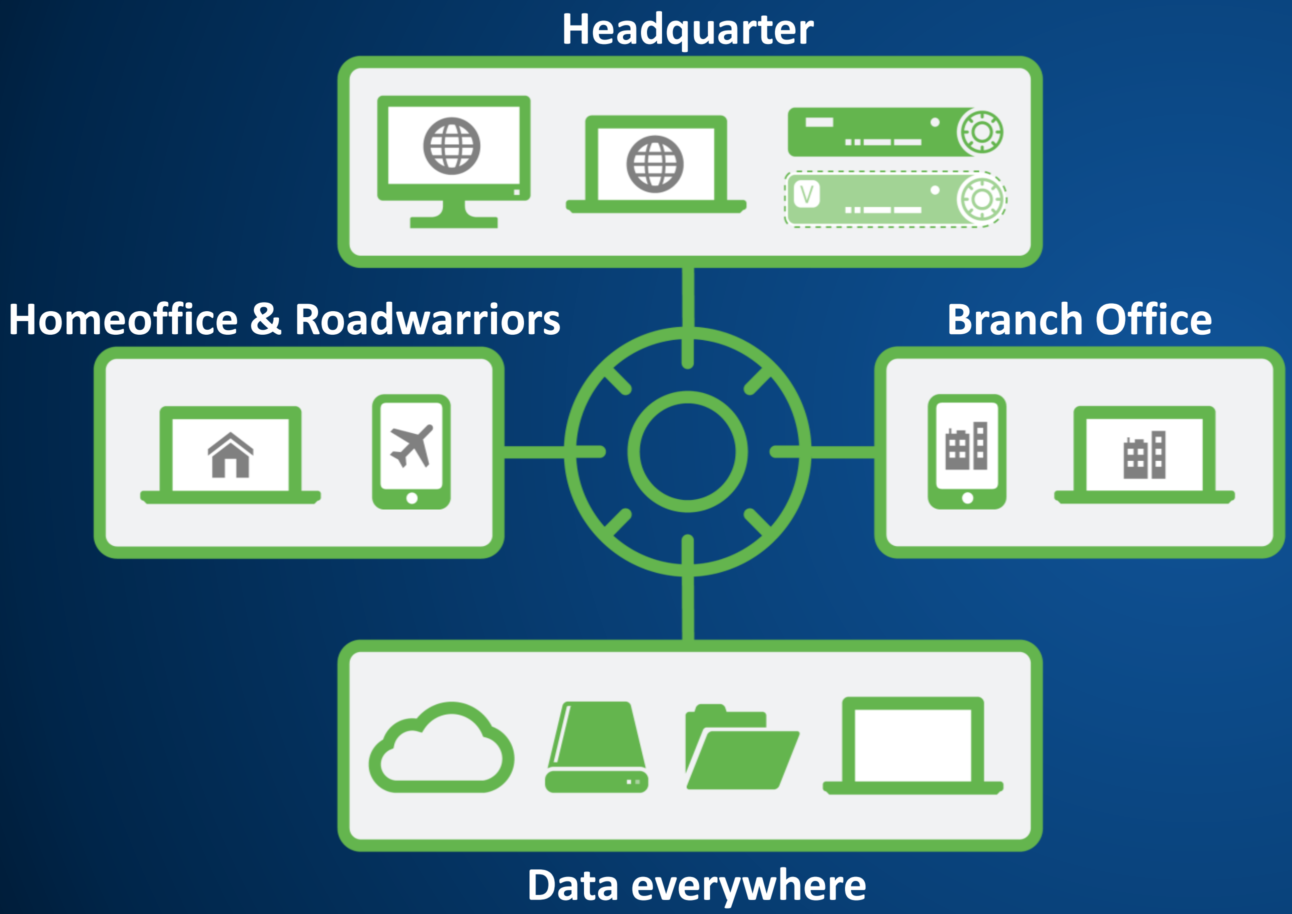
Extended Cleanup

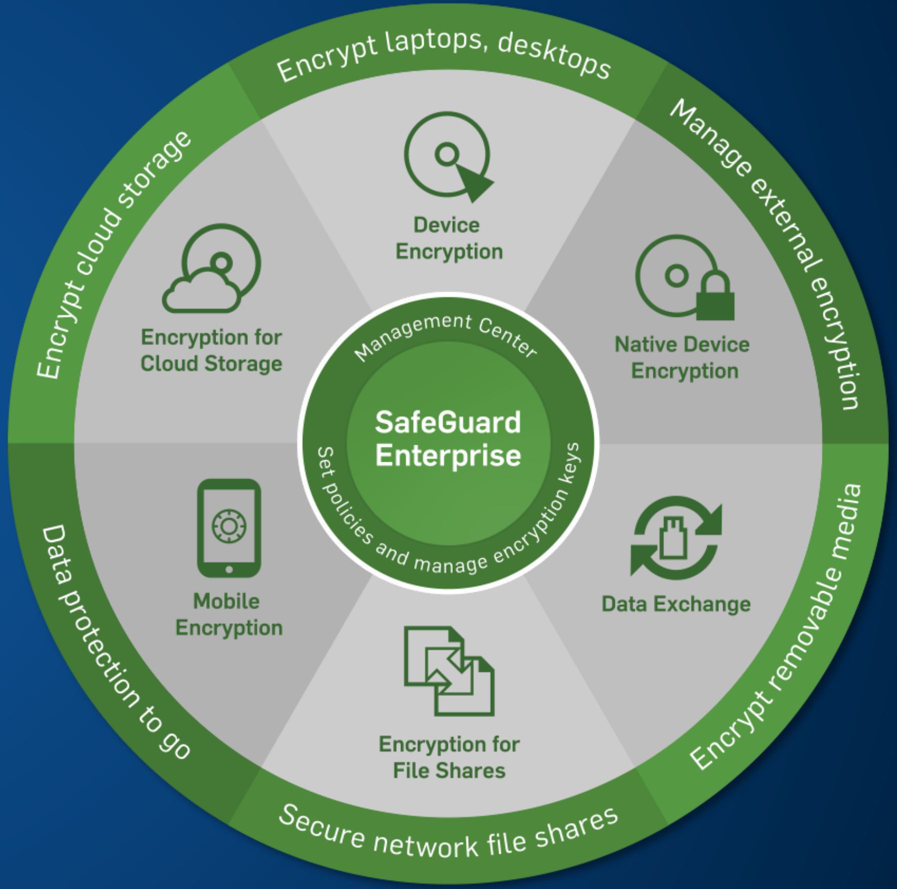
- **Signatureless Removal** unknown Malware
- Restores **original files**

Root Cause Analysis

- **Graphical analysis** of malware infection and propagation
- What has **happened**?
- What is **affected**?
- How do I **prevent** this in the **future**?

SafeGuard Enterprise – Encryption everywhere

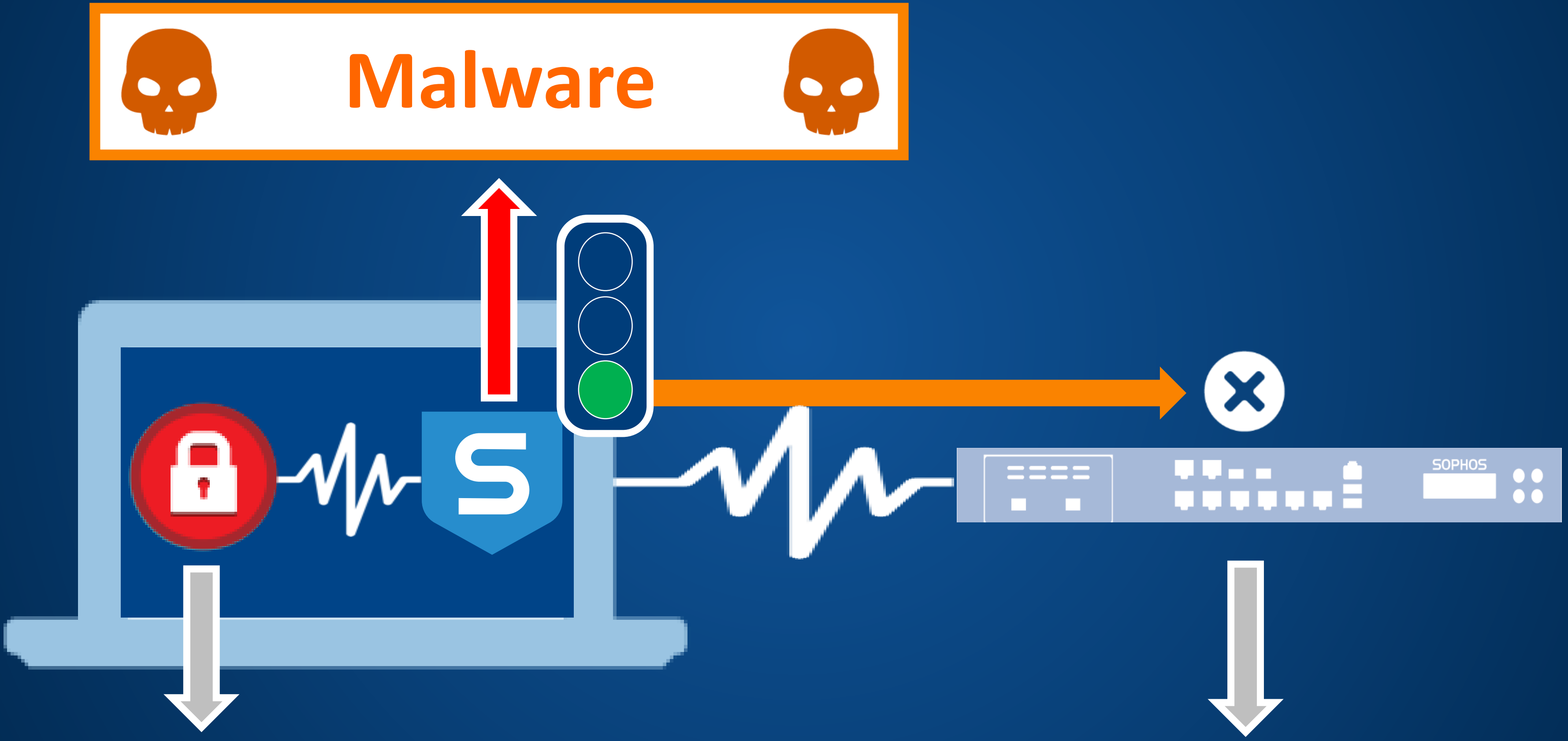




Synchronized Security Scenarios

SOPHOS

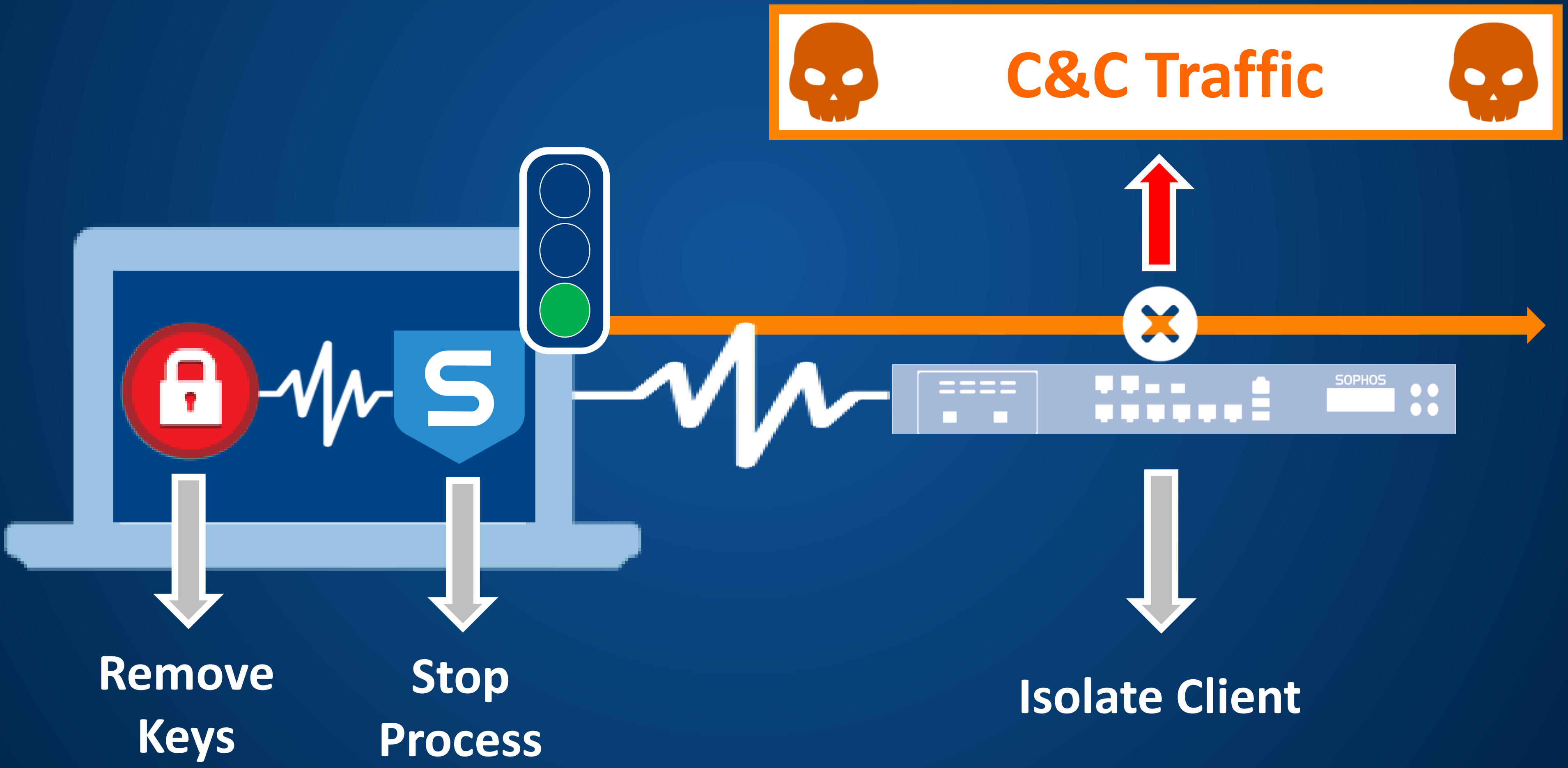
Security Heartbeat – Malware Detection



Remove Keys

Isolate Client

Security Heartbeat – Botnet C&C-Traffic Detection



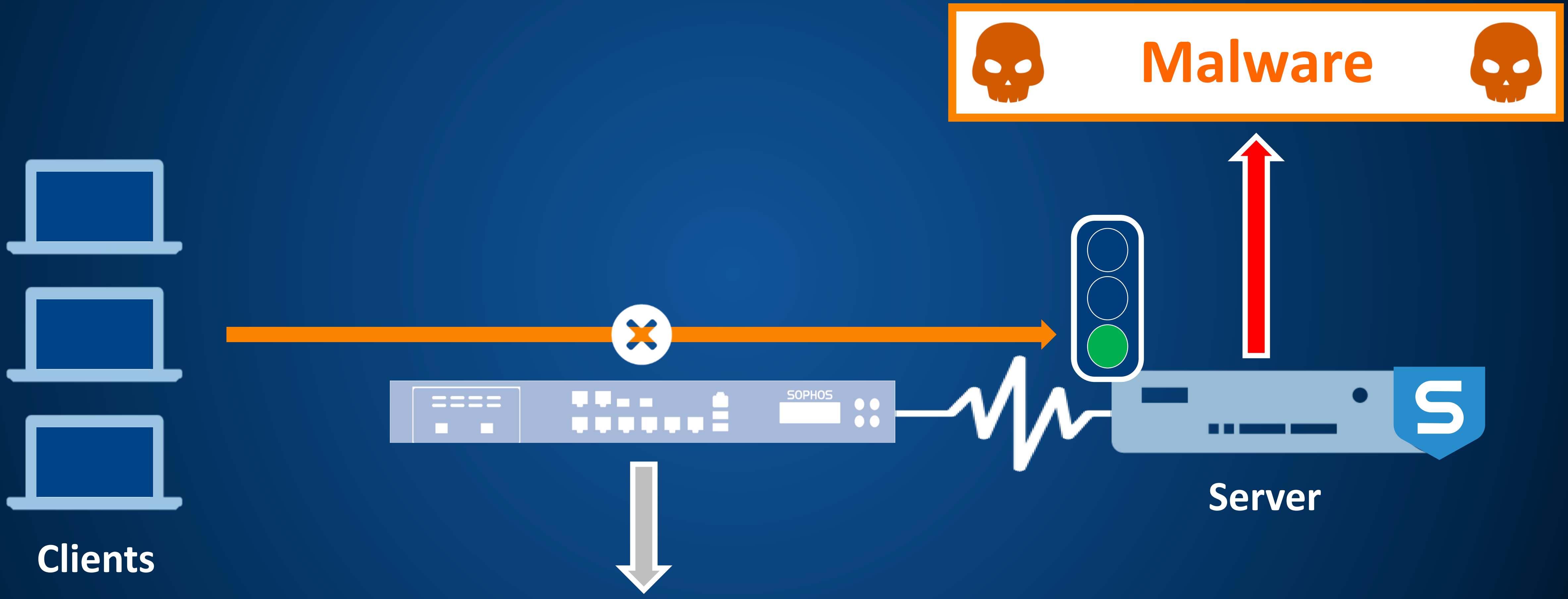
C&C Traffic

Remove Keys

Stop Process

Isolate Client

Security Heartbeat – Server Heartbeat



Synchronized App Control

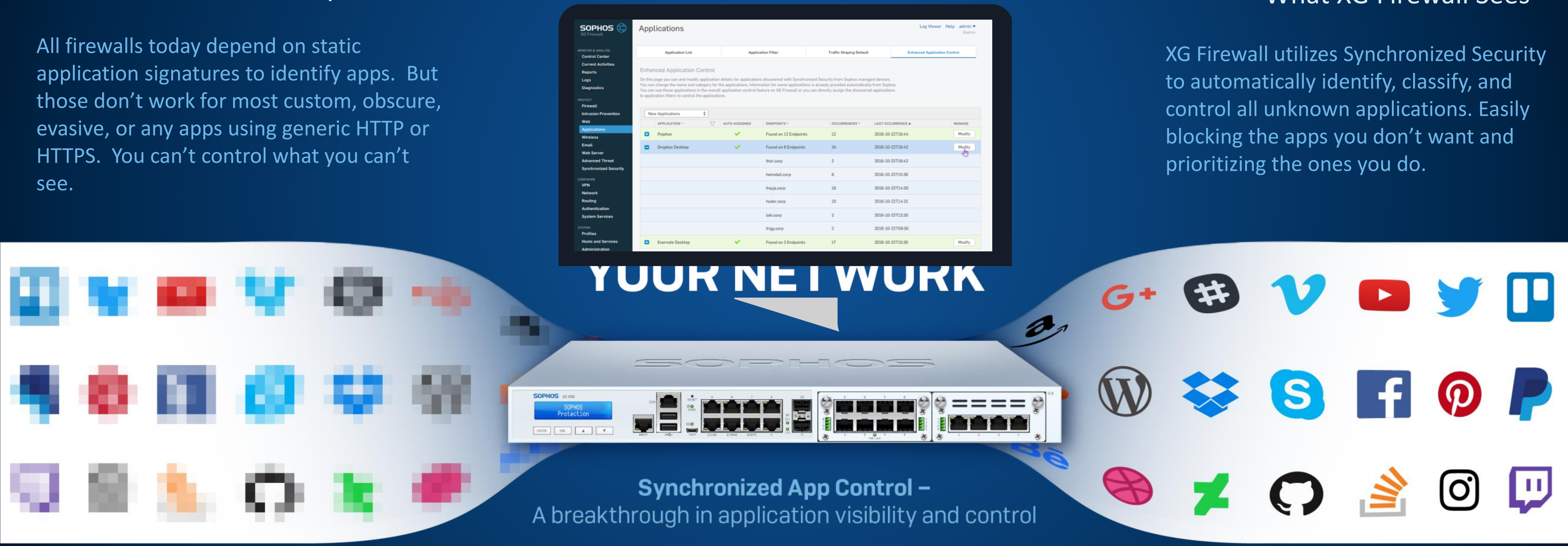
A breakthrough in network visibility and control

What Firewalls See Today

All firewalls today depend on static application signatures to identify apps. But those don't work for most custom, obscure, evasive, or any apps using generic HTTP or HTTPS. You can't control what you can't see.

What XG Firewall Sees

XG Firewall utilizes Synchronized Security to automatically identify, classify, and control all unknown applications. Easily blocking the apps you don't want and prioritizing the ones you do.



Applications

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 XG Firewall or you can directly assign the discovered applications to application filters to control the applications.

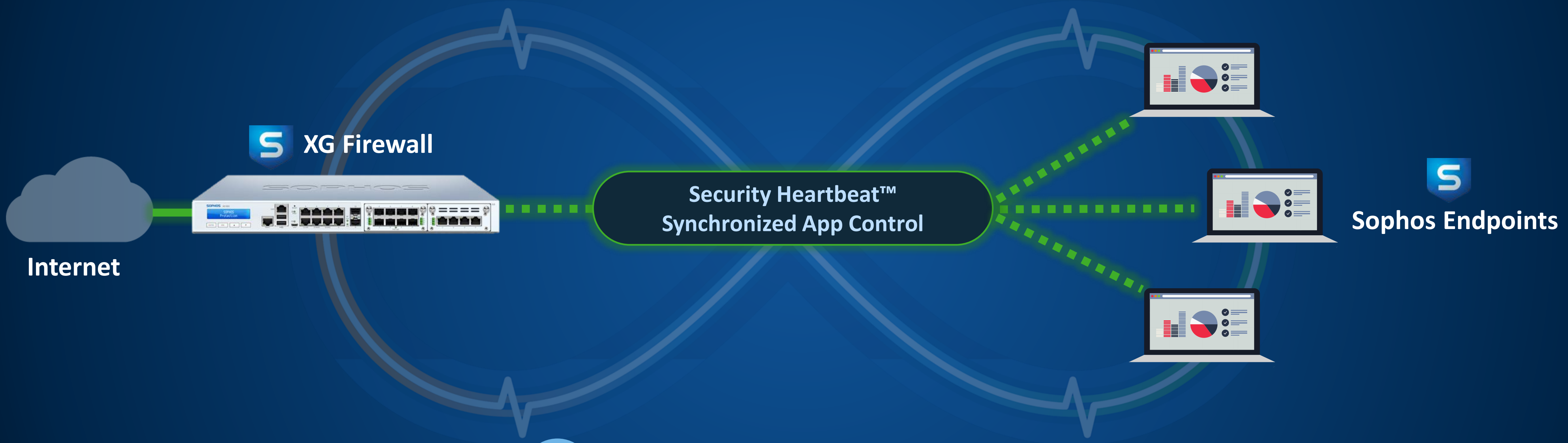
	APPLICATION	AUTO-ASSIGNED	ENDPOINTS	OCCURRENCES	LAST OCCURRENCE ▲	MANAGE
+	Psiphon	✓	Found on 12 Endpoints	12	2016-10-22T16:44	Modify
−	Dropbox Desktop	✓	Found on 6 Endpoints	34	2016-10-22T16:42	Modify
			thor.corp	2	2016-10-22T16:42	
			heimdall.corp	8	2016-10-22T15:30	
			freyja.corp	10	2016-10-22T14:20	
			hodor.corp	10	2016-10-22T14:15	
			loki.corp	2	2016-10-22T12:20	
			frigg.corp	2	2016-10-22T09:30	
+	Evernote Desktop	✓	Found on 2 Endpoints	17	2016-10-22T15:35	Modify

Synchronized App Control –
A breakthrough in application visibility and control

Synchronized App Control in Action

1 **Unknown Application**
XG Firewall sees app traffic that does not match a signature

2 **Endpoint Shares App Info**
Sophos Endpoint passes app name, path and even category to XG Firewall for classification



3 **Application is Classified & Controlled**
Automatically categorize and control where possible or admin can manually set category or policy to apply.

Synchronized Security Benefits

Unparalleled Protection

Best-of-breed products packed with next-gen technology actively work together to detect and prevent advanced attacks like ransomware and botnets.

Automated Incident Response

Security information is shared and acted on automatically across the system, isolating infected endpoints before the threat can spread and slashing incident response time by 99.9%.

Real-time Insight and Control

See - and control - what's happening in real-time for simpler, better IT security management.

Free Tools

SOPHOS

Free Tools

Sophos gives out free tools that check for security risk, remove viruses and protect home networks

Sophos Home

Mobile Security for iOS

XG Firewall Home Edition

Antivirus for Linux

Free 30-day trial of HitmanPro and HitmanPro.Alert

Mobile Security for Android

UTM Home Edition

SOPHOS

Security made simple.