

# *Next-Gen Synchronized Security*

**George Kouimintzis**

Commercial Director NSS

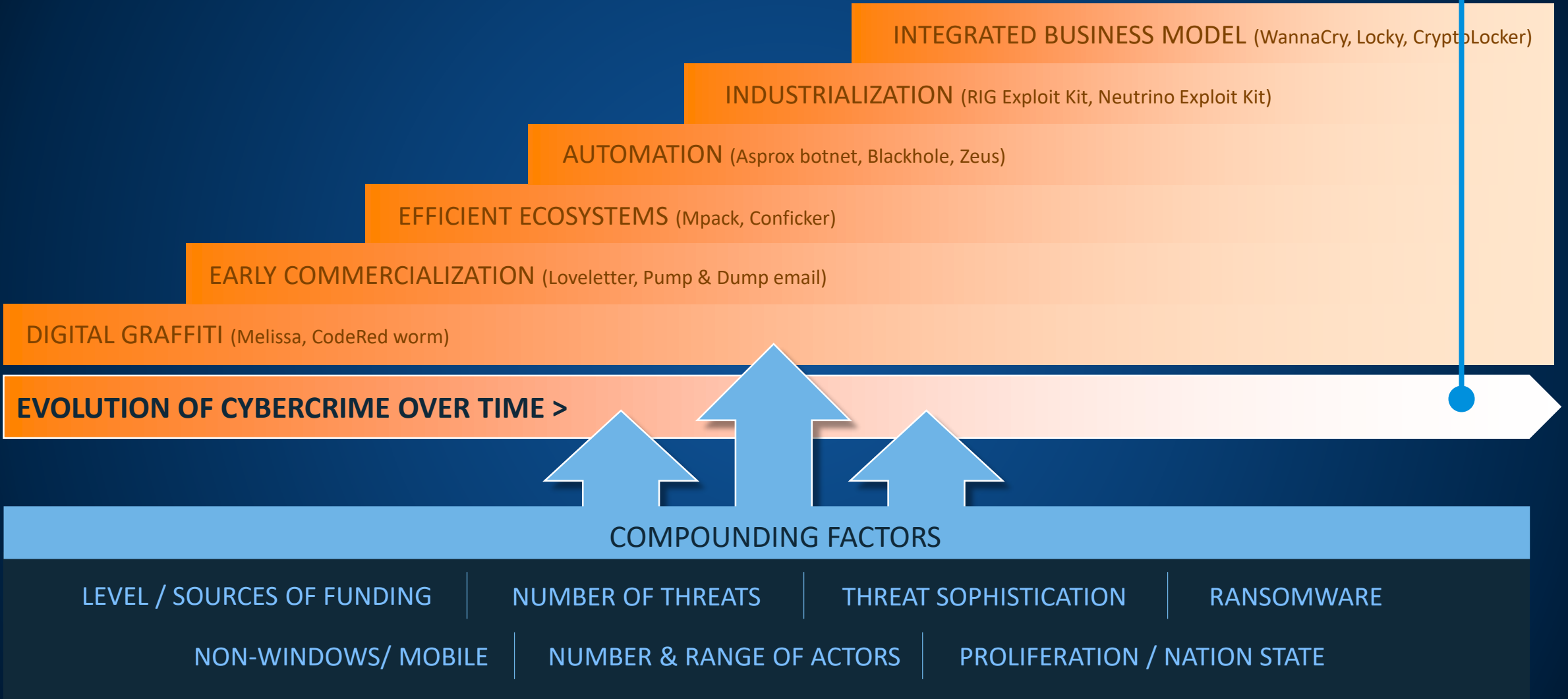
Sophos VAD for SE Europe

**SOPHOS**

# *Threat Landscape*

# Cybercrime Dynamics

TODAY

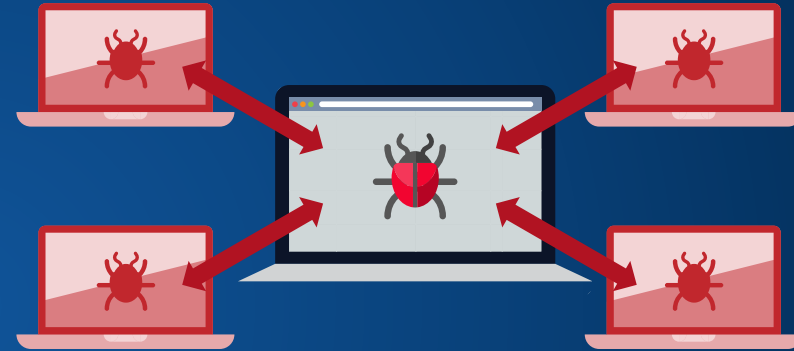


# Increasing attacks, increasing sophistication



## Attack surface exponentially larger

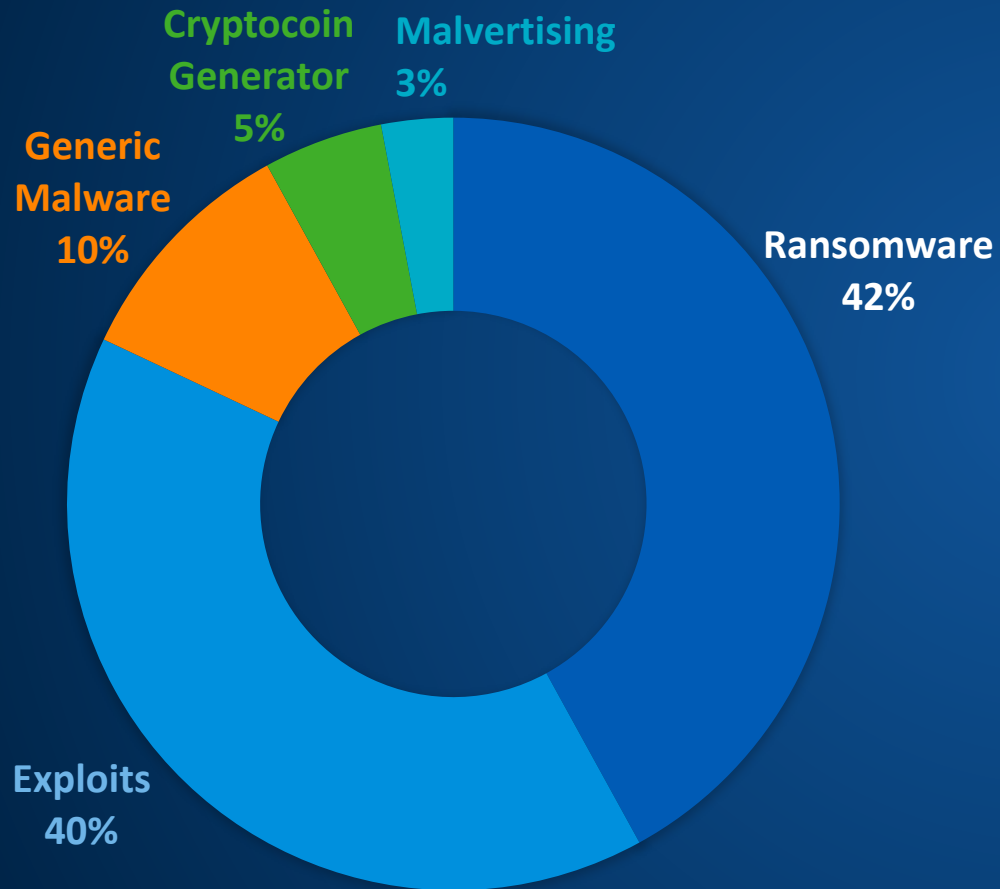
*Laptops/Desktops*  
*Phones/Tablets*  
*Virtual servers/desktops*  
*Cloud servers/storage*



## Attacks are more sophisticated than defenses

*Syndicated crime tools*  
*Zero day exploits*  
*Memory resident*  
*Polymorphic/metamorphic*  
*Network and endpoint integrated*

# Top Threats Worldwide



- **Exploits**

- Industrialized attacks
- Flash, Downloader, JS redirect, Malvertising

- **Ransomware**

- Dropper, Phish, Shortcut, Doc Macro
- Successful attacker can earn up to \$394,000 in a single month

- **Phishing**

- 93% of phishing emails have a ransomware payload (CSO Online)

# *Synchronized Security*

**SOPHOS**

# Synchronized Security

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

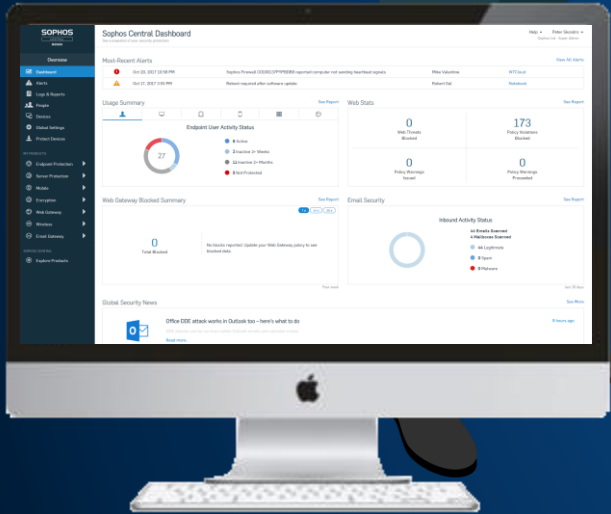


Endpoint



Firewall

# Synchronized Security



Next-Gen Endpoint

XG Firewall



## Accelerated Threat Discovery

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

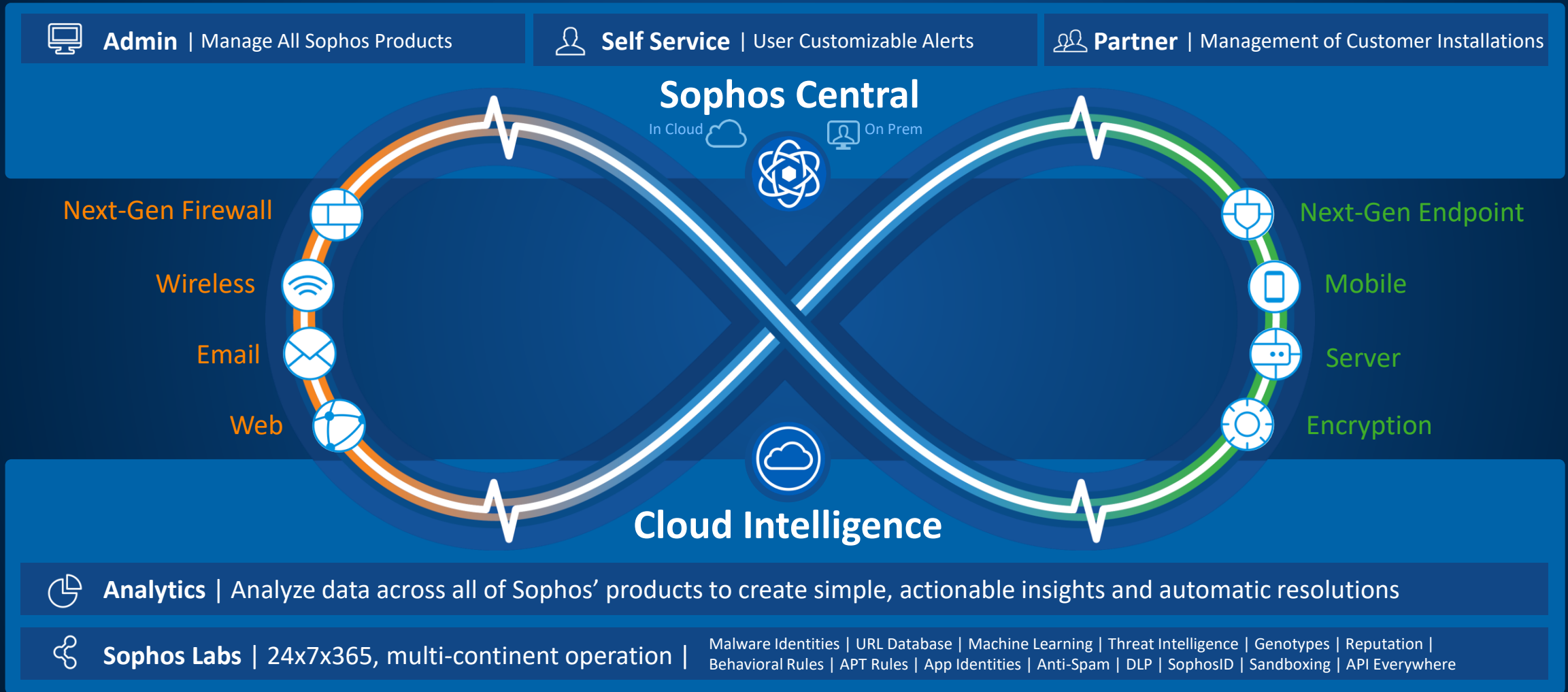
## Active Source Identification

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

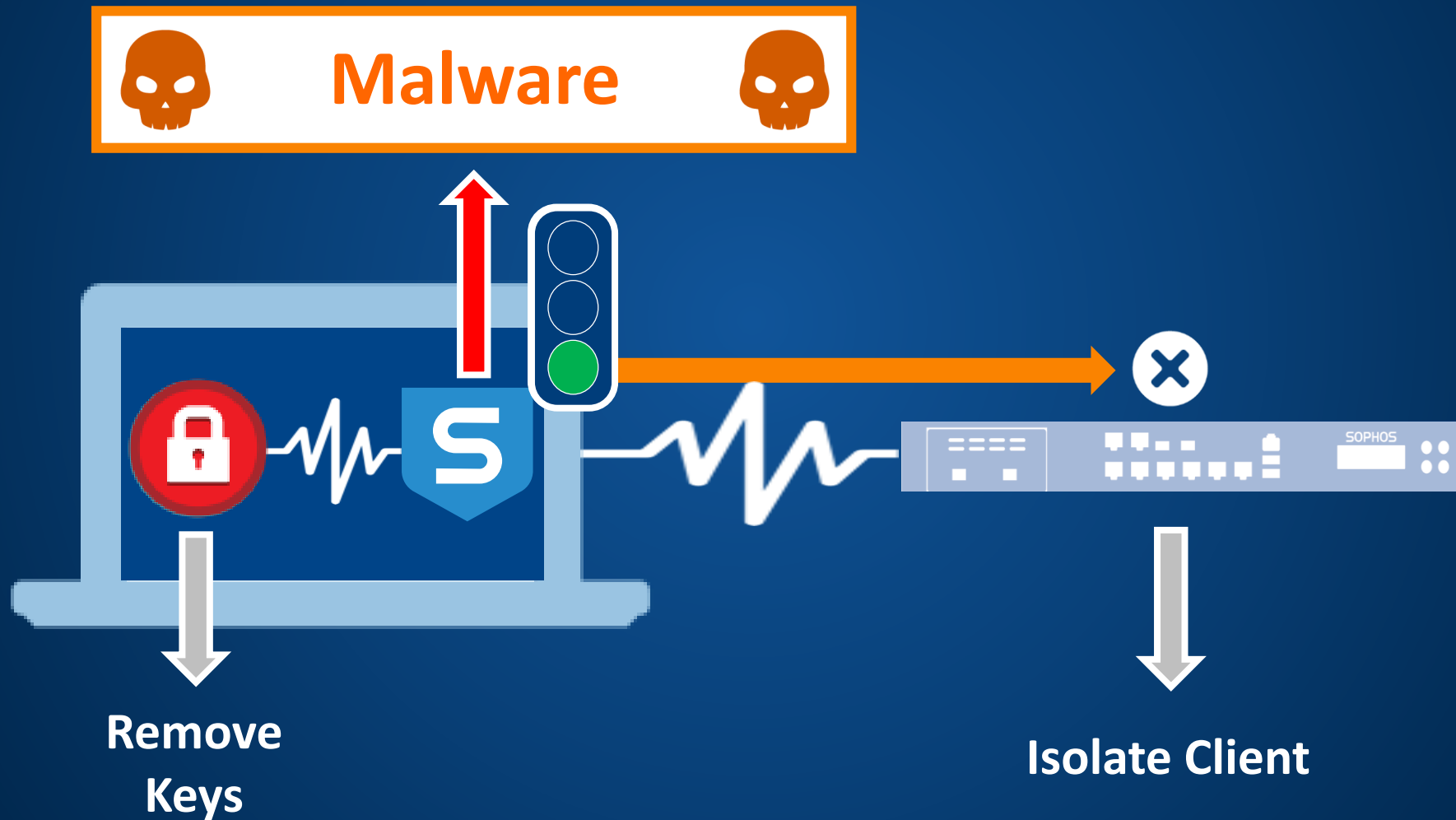
## Automated Incident Response

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

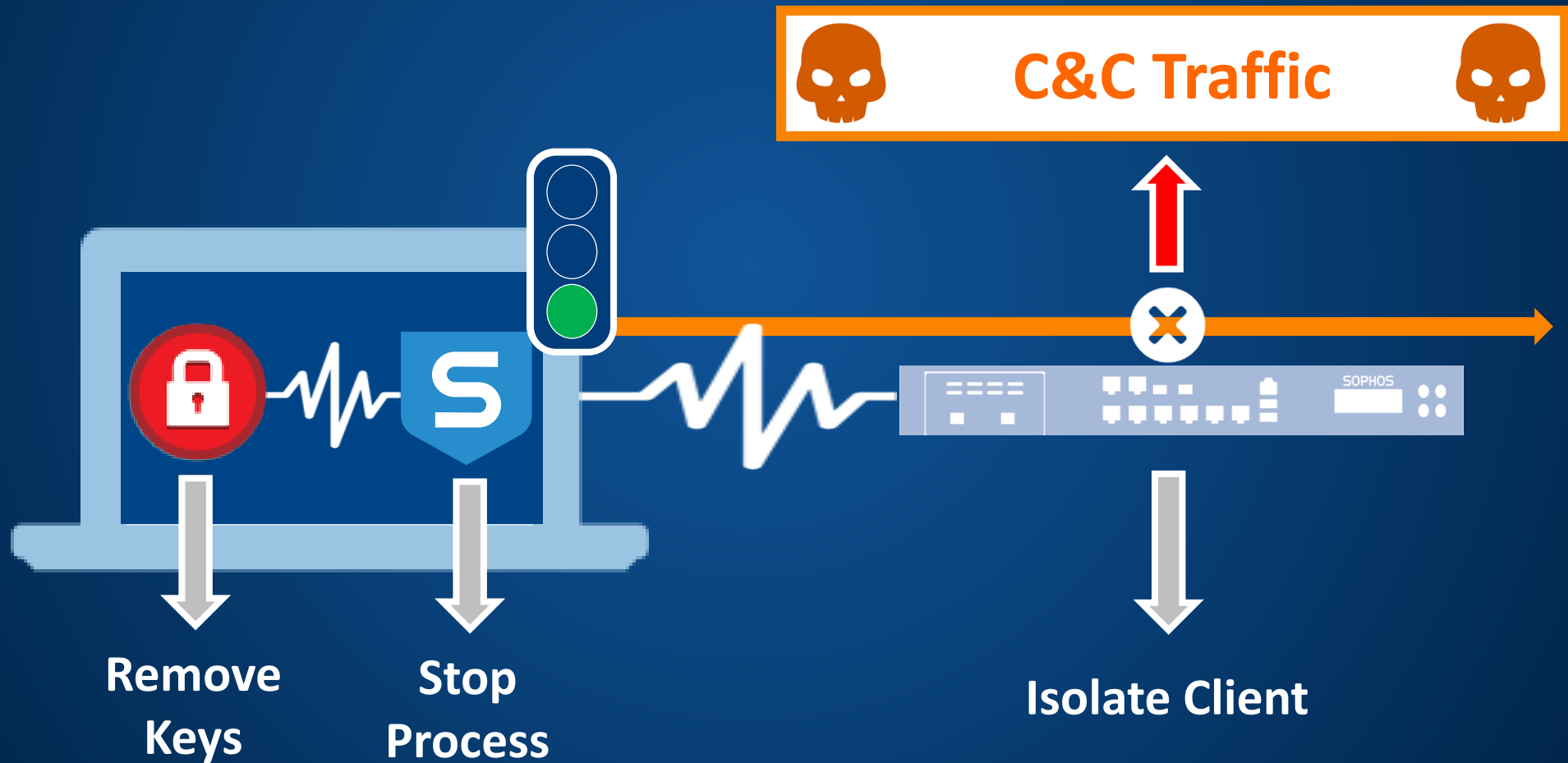
# Synchronized Security Platform and Strategy



# Security Heartbeat – Malware Detection



# Security Heartbeat – Botnet C&C-Traffic Detection



# 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.

SOPHOS

XG Firewall

MONITOR & ANALYZE

Control Center

Current Activities

Reports

Logs

Diagnostics

APPLY FILTERS

Firewall

Device Provision

Web

Applications

Wireless

Email

Web Server

Advanced Threat

Synchronized Security

CONFIGURE

VPN

Network

Routing

Authentication

System Services

SETTINGS

Profiles

Hosts and Services

Administration

Log Viewer

Help

Admin

Sophos

Applications

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

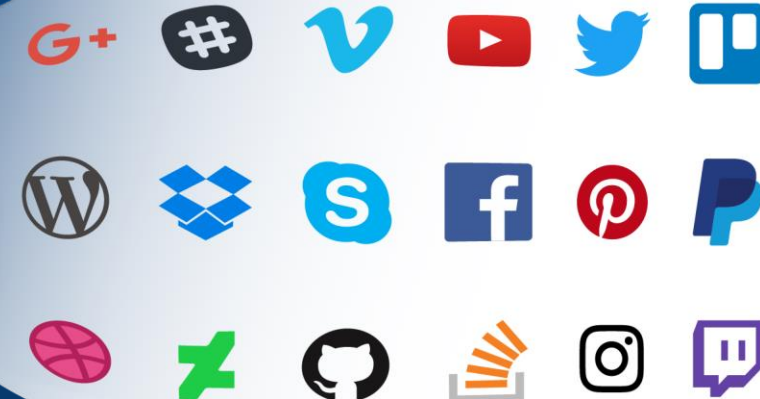
New Applications

APPLICATION *	AUTO-ASSIGNED	ENDPOINTS *	OCCURRENCES *	LAST OCCURRENCE *	MANAGE
 Pipemon		Found on 12 Endpoints	12	2018-10-27T16:44	Modify
 Dropbox Desktop		Found on 6 Endpoints	34	2018-10-27T16:42	Modify
		thar.corp	2	2018-10-27T16:42	
		heindall.corp	8	2018-10-27T16:39	
		freya.corp	10	2018-10-27T14:20	
		hodor.corp	10	2018-10-27T14:15	
		luki.corp	2	2018-10-27T12:20	
		frigg.corp	2	2018-10-27T09:30	
 Evernote Desktop		Found on 3 Endpoints	17	2018-10-27T16:36	Modify

YOUR NETWORK



**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

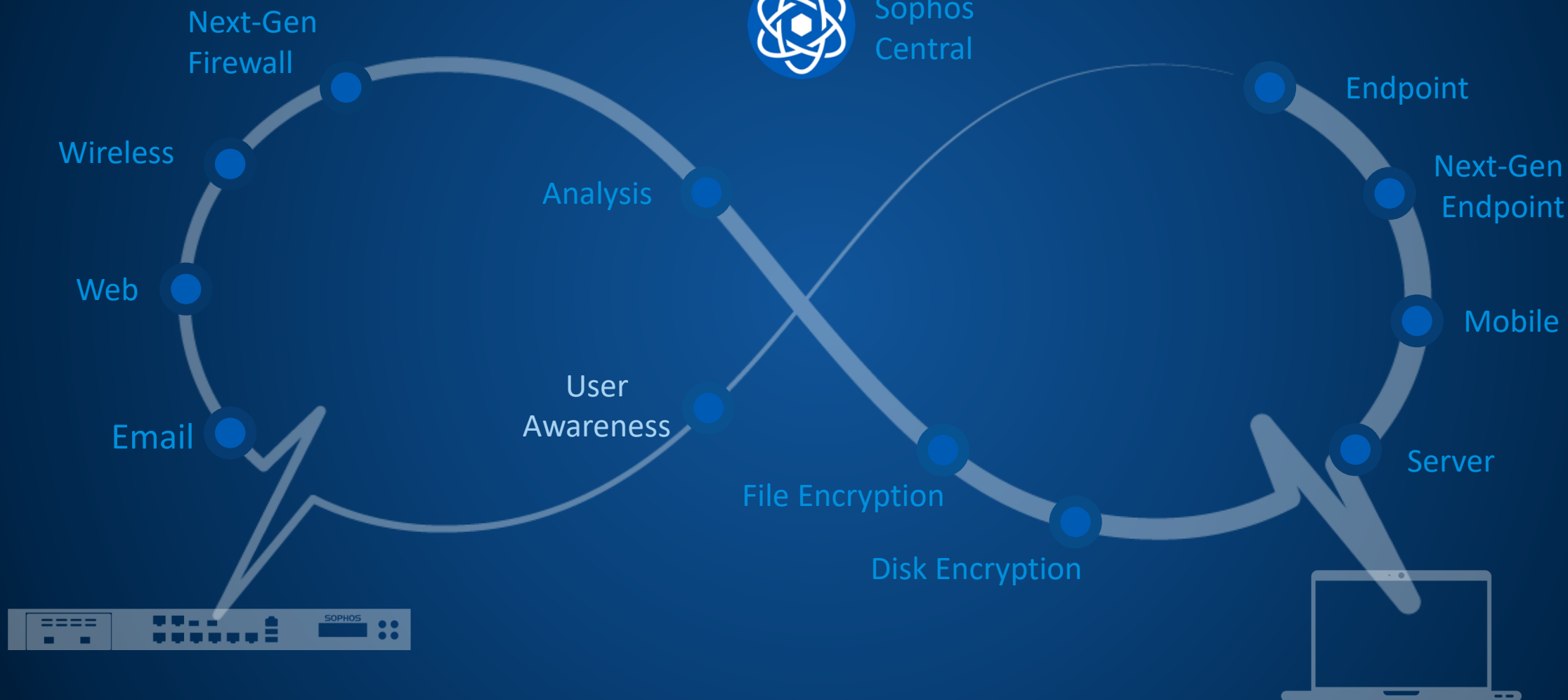
Security information is shared and acted on automatically across the system, isolating infected endpoints before the threat can spread and slashing incident response time by 99.9%.



## Real-time Insight and Control

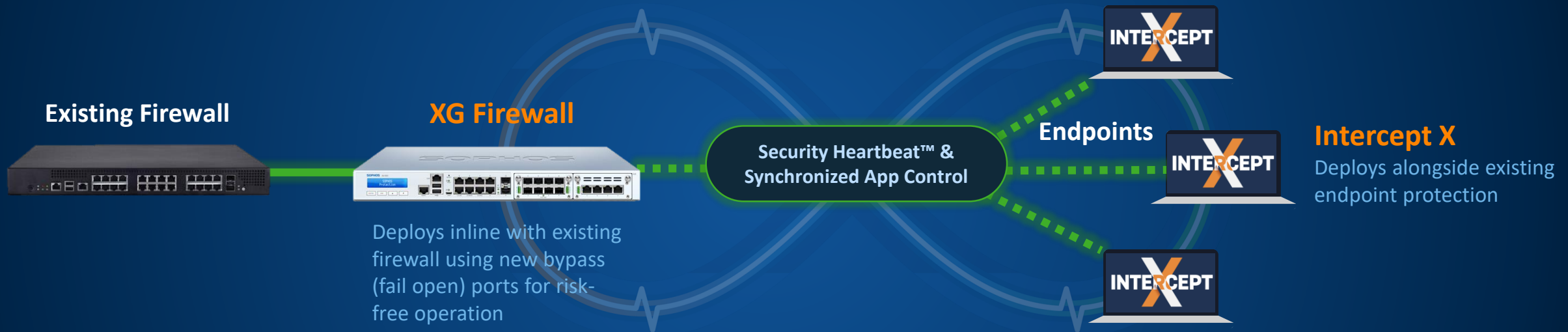
See - and control - what's happening in real-time for simpler, better IT security management.

# Synchronized Security – Teampay replaces Best-of-Breed



# Inline Deployment

*Enable Synchronized Security Without any Disruption*



# *Free Tools*

# 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.