Welcome to the next generation IT solutions with Sophos Synchronized Security

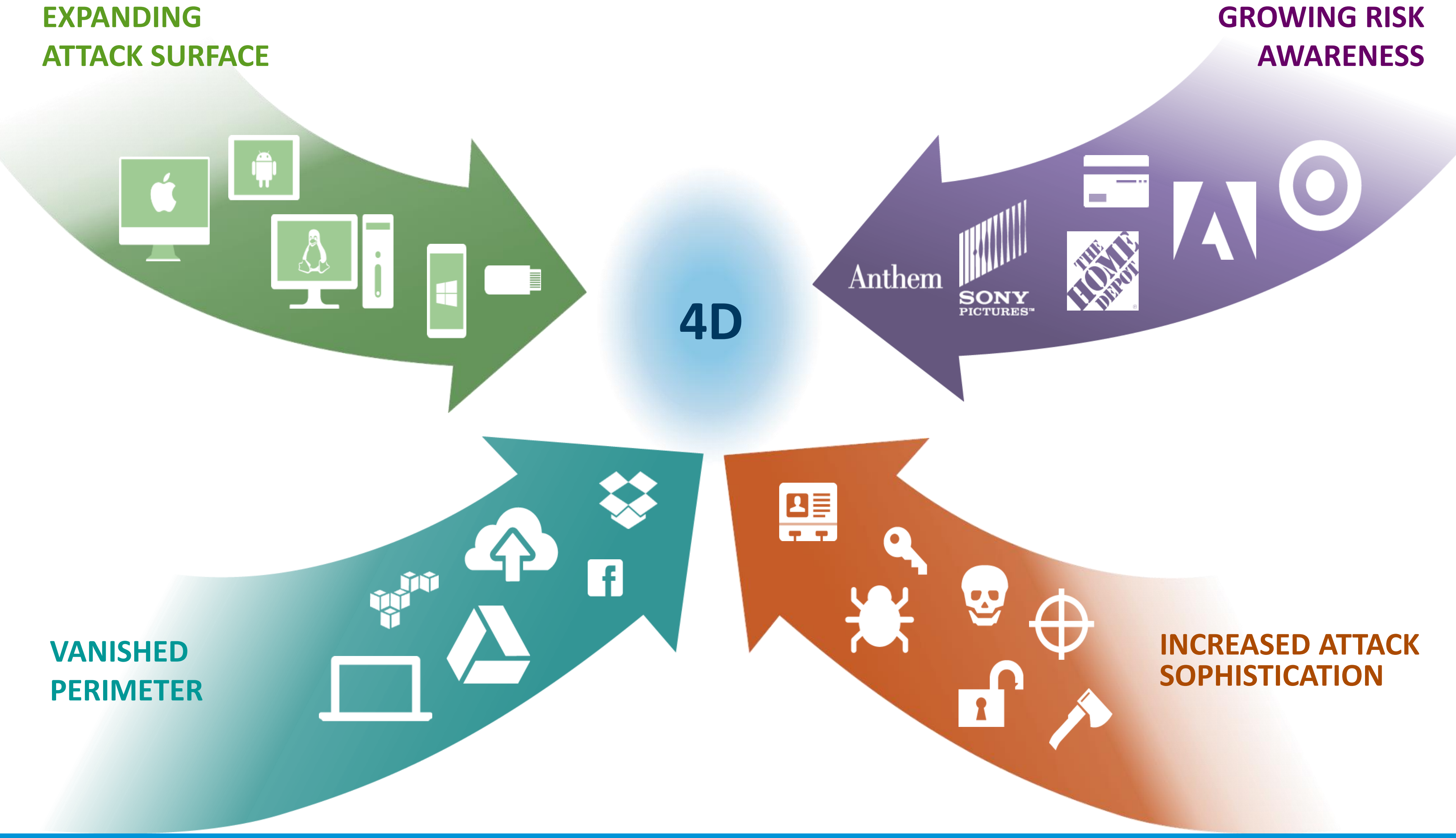
Joanna Wziątek

Sales Engineer, Sophos

SOPHOS

Security industry 2D view

Security dimensions



EXPANDING ATTACK SURFACE

GROWING RISK AWARENESS

4D

VANISHED PERIMETER

INCREASED ATTACK SOPHISTICATION

It’s time for a security revolution

Generations of security

Point Products

Anti-virus

IPS

Firewall

Sandbox

Layers

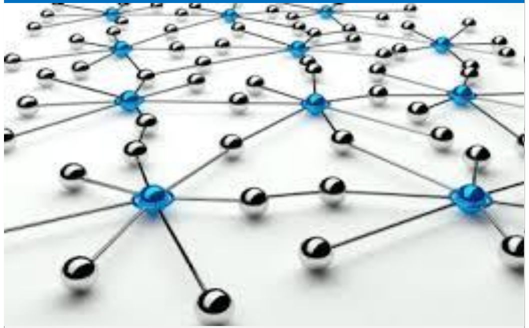
Bundles

Suites

UTM

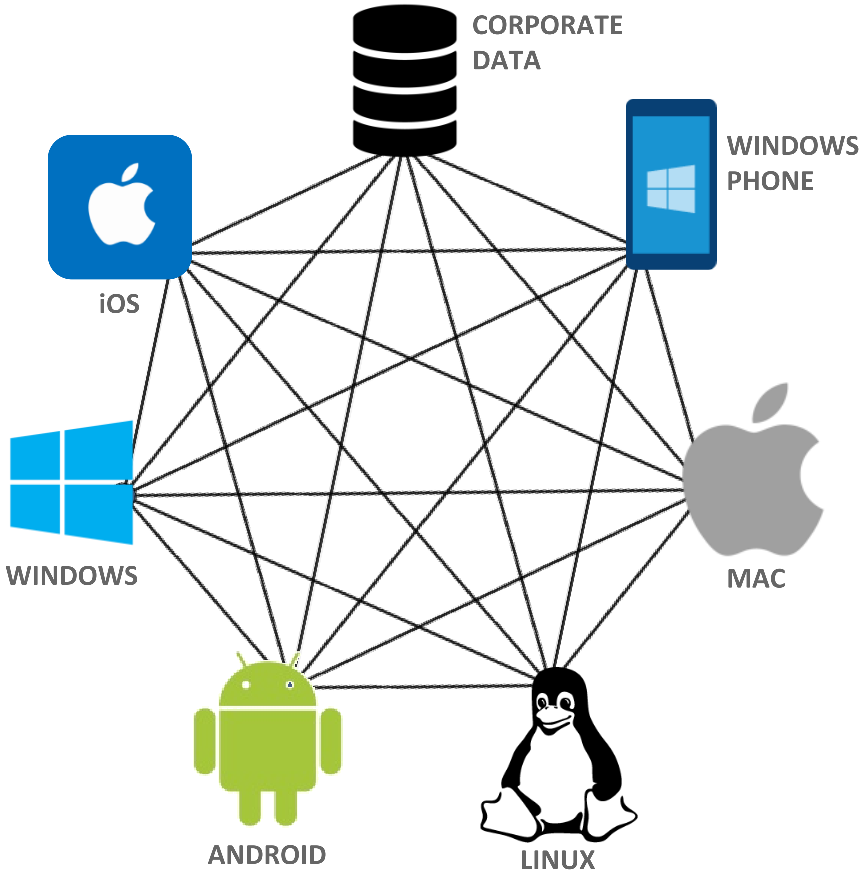
EMM

Synchronized Security



Security Heartbeat™

Synchronized Security

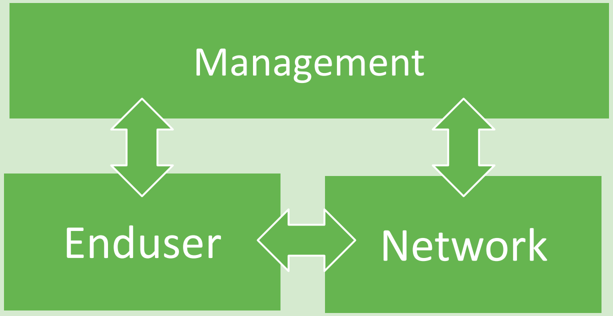


Comprehensive protection

- Prevent Malware
- Detect Compromises
- Remediate Threats
- Investigate Issues
- Encrypt Data

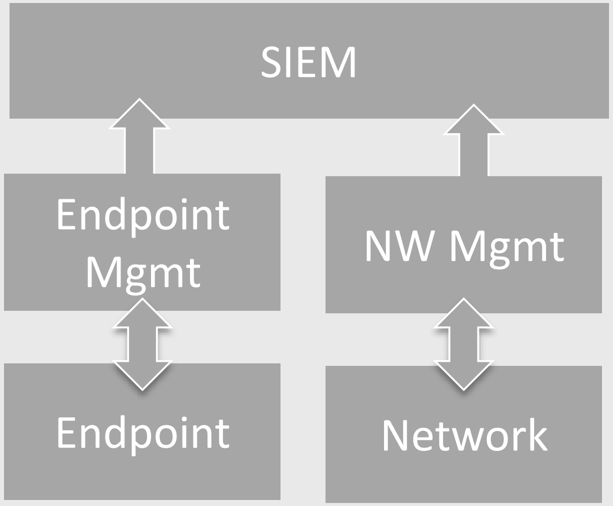
Integration at a different level

Synchronized Security



- System-level intelligence
- Automated correlation
- Faster decision-making
- Accelerated Threat Discovery
- Automated Incident Response
- Simple unified management

Alternative



- Resource intensive
- Manual correlation
- Dependent upon human analysis
- Manual Threat/Incident response
- Extra products
- Endpoint/Network unaware of each other

Security Heartbeat

Green

Endpoints have full access to internal applications and data as well as internet

Yellow

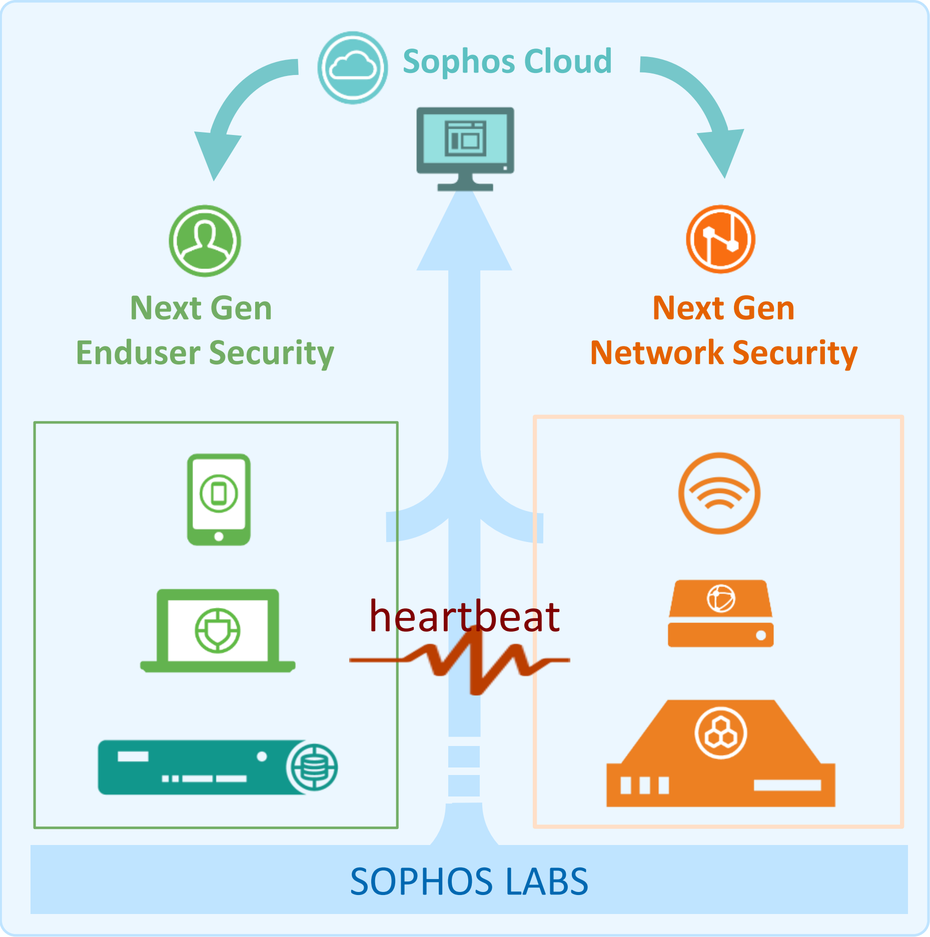
Affected endpoints can be isolated from internal/sensitive applications and data while maintaining access to internet

Red

Affected endpoints are isolated from the network and have no access to internal systems or external internet

Defaults and customization

There are no default policies based on health status so admins can customize responses as needed. We are developing a best practices guide to assist customers in recommended policy setup.



SOPHOS

How it works

System Initialization

Registration

NGEP & NGFW register with Sophos Cloud which sends certificate/sec info to both

Connection

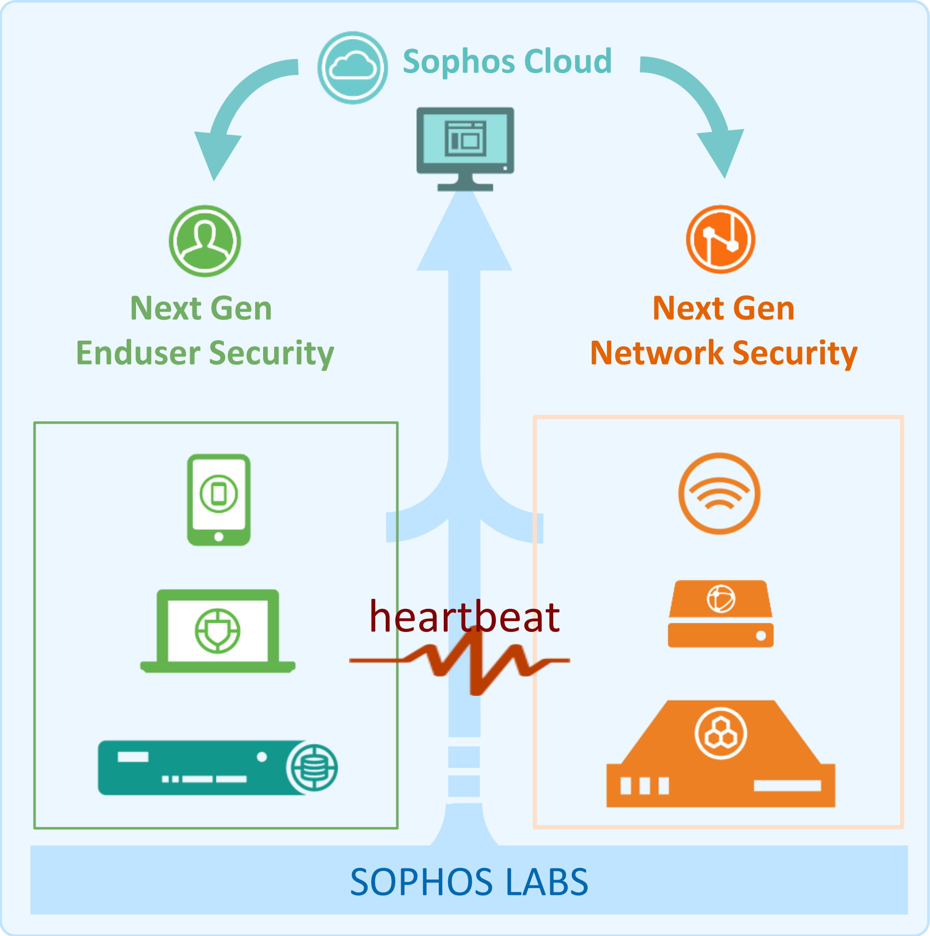
Endpoints initiate connection to the trusted Firewall

Validation

Firewall and Endpoints check sec info sent to them by Cloud to verify they are valid

Support of multiple locations

Endpoints can establish connection to Firewalls at any customer's location as the Sophos Cloud registry can be shared among all Galileo-enabled Firewalls



Accelerated Threat Discovery

Security Heartbeat

A few bytes of information are shared every 15 seconds from Endpoint to Network

Events

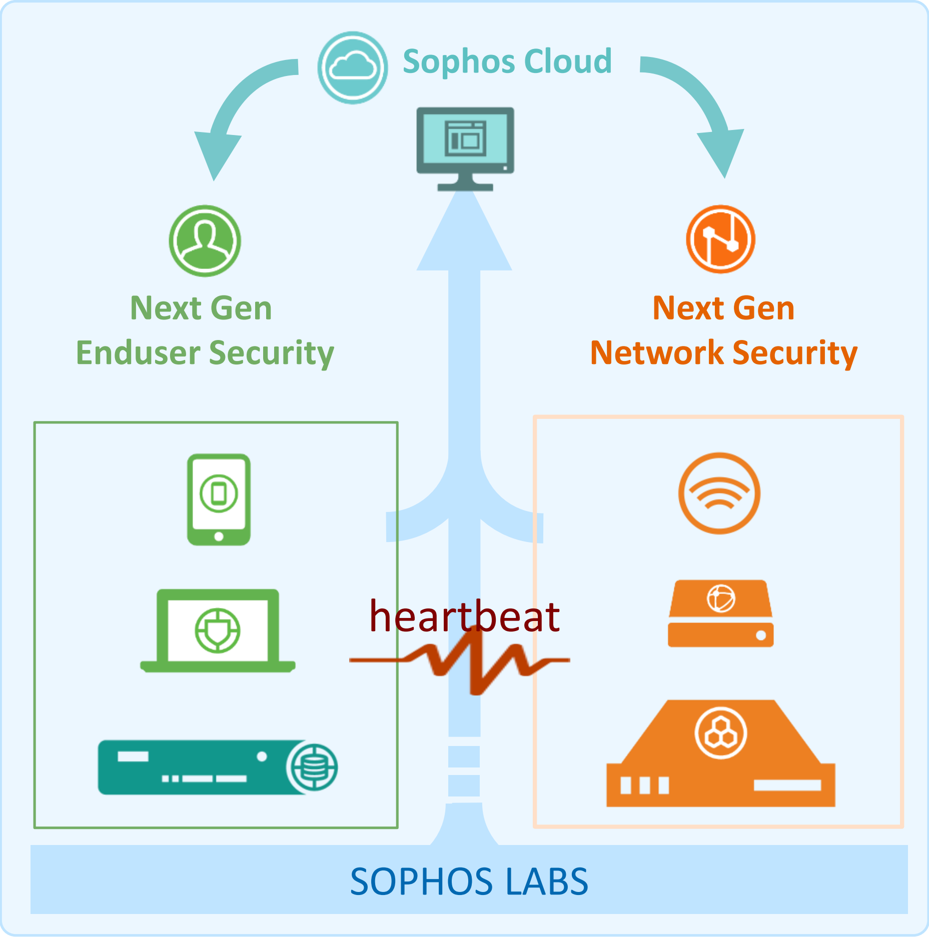
Upon discovery, security information like Malware, PUA is shared between Endpoints and Network

Health

Endpoint sends Red, Yellow, Green health status to Network

VPN support

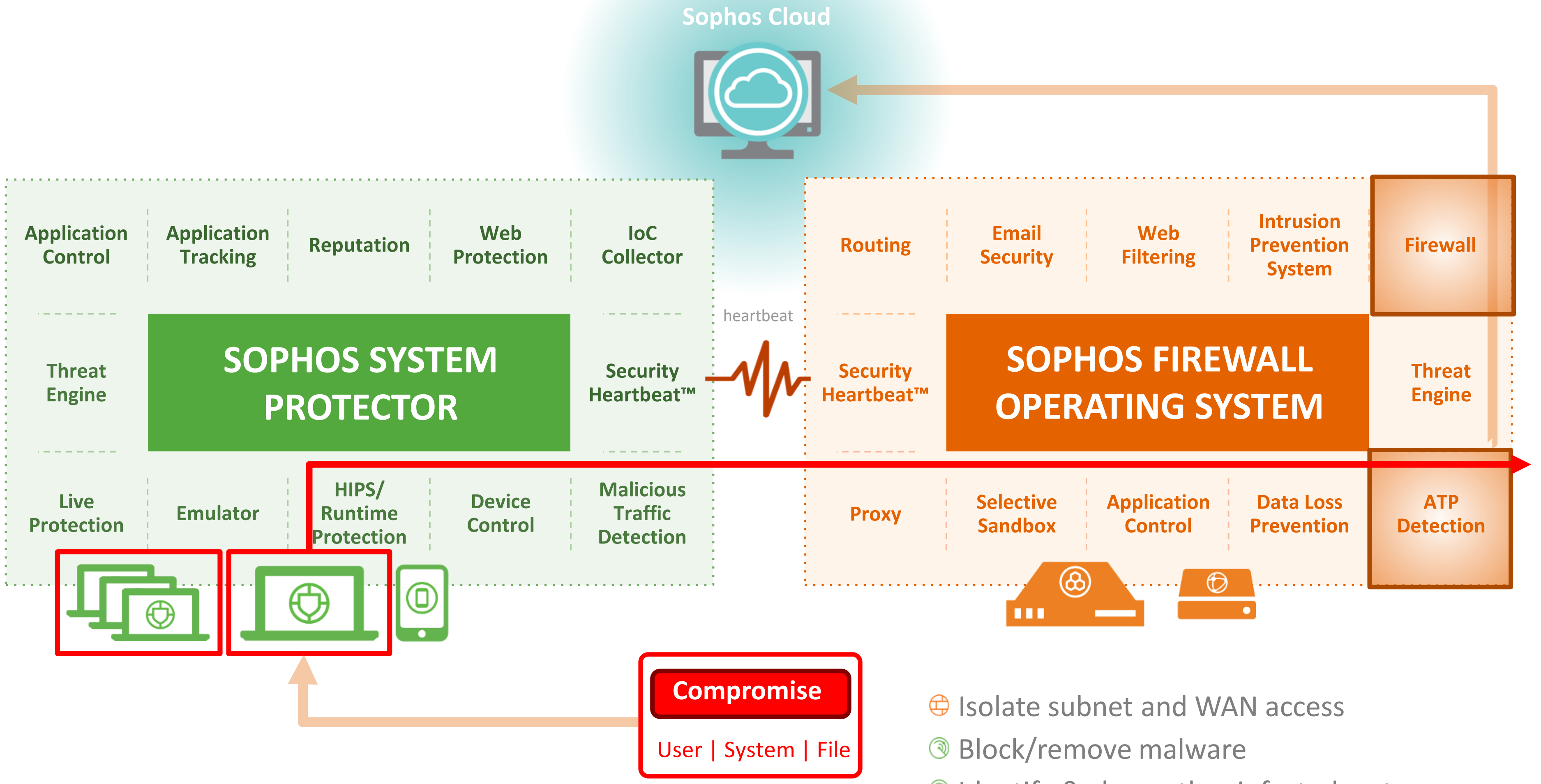
Galileo supports endpoints connected within the local network as well as those connected via VPN as long as they are connecting to the Firewall.



SOPHOS

Synchronized Security 2015

Next Generation Threat Detection



Sophos Cloud

Application Control

Application Tracking

Reputation

Web Protection

IoC Collector

Threat Engine

SOPHOS SYSTEM PROTECTOR

Security Heartbeat™

Live Protection

Emulator

HIPS/ Runtime Protection

Device Control

Malicious Traffic Detection

heartbeat

Routing

Email Security

Web Filtering

Intrusion Prevention System

Firewall

Security Heartbeat™

SOPHOS FIREWALL OPERATING SYSTEM

Threat Engine

Proxy

Selective Sandbox

Application Control

Data Loss Prevention

ATP Detection

Compromise

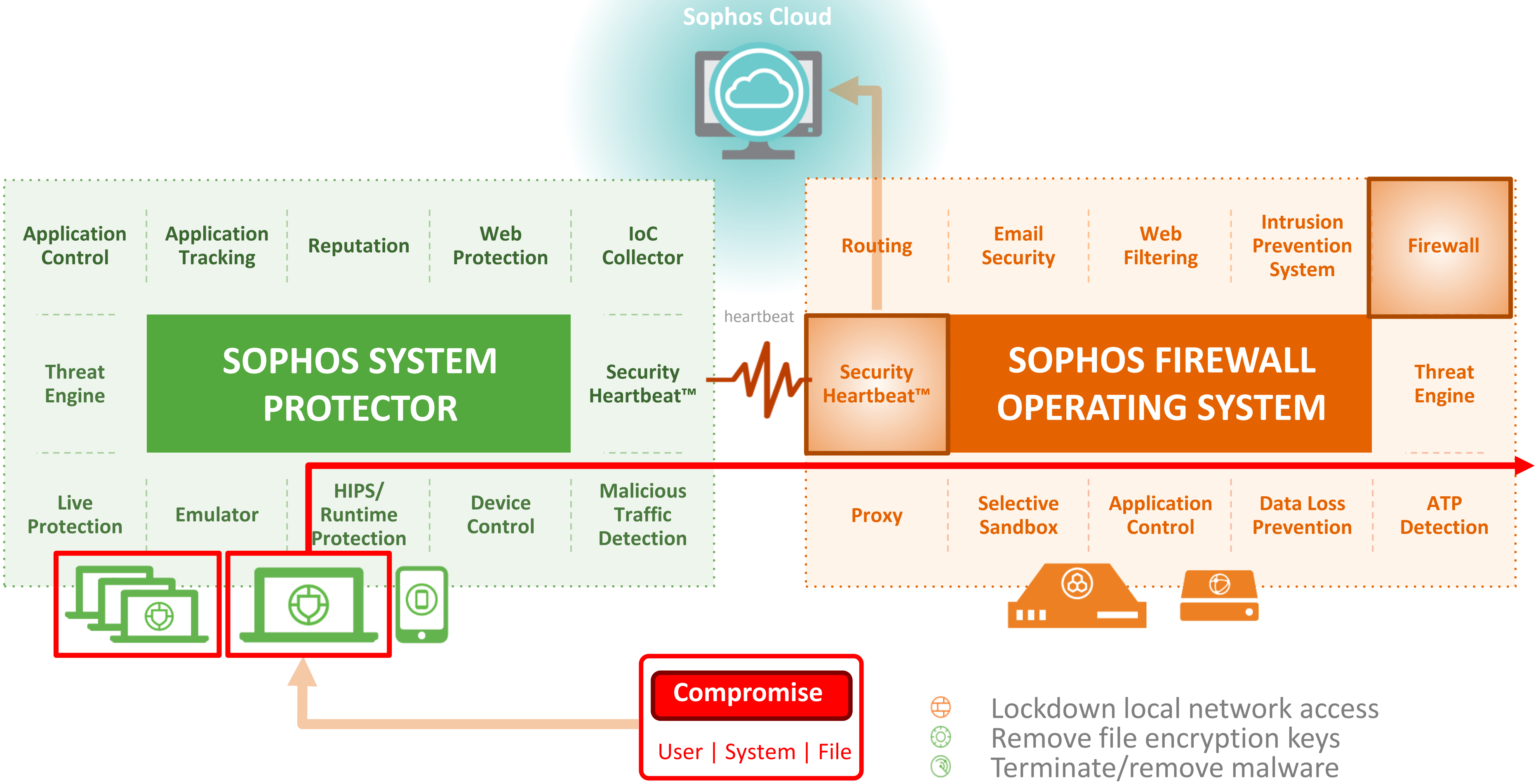
User | System | File

- Isolate subnet and WAN access
- Block/remove malware
- Identify & clean other infected systems

SOPHOS

Synchronized Security 2016

Improved Threat Detection

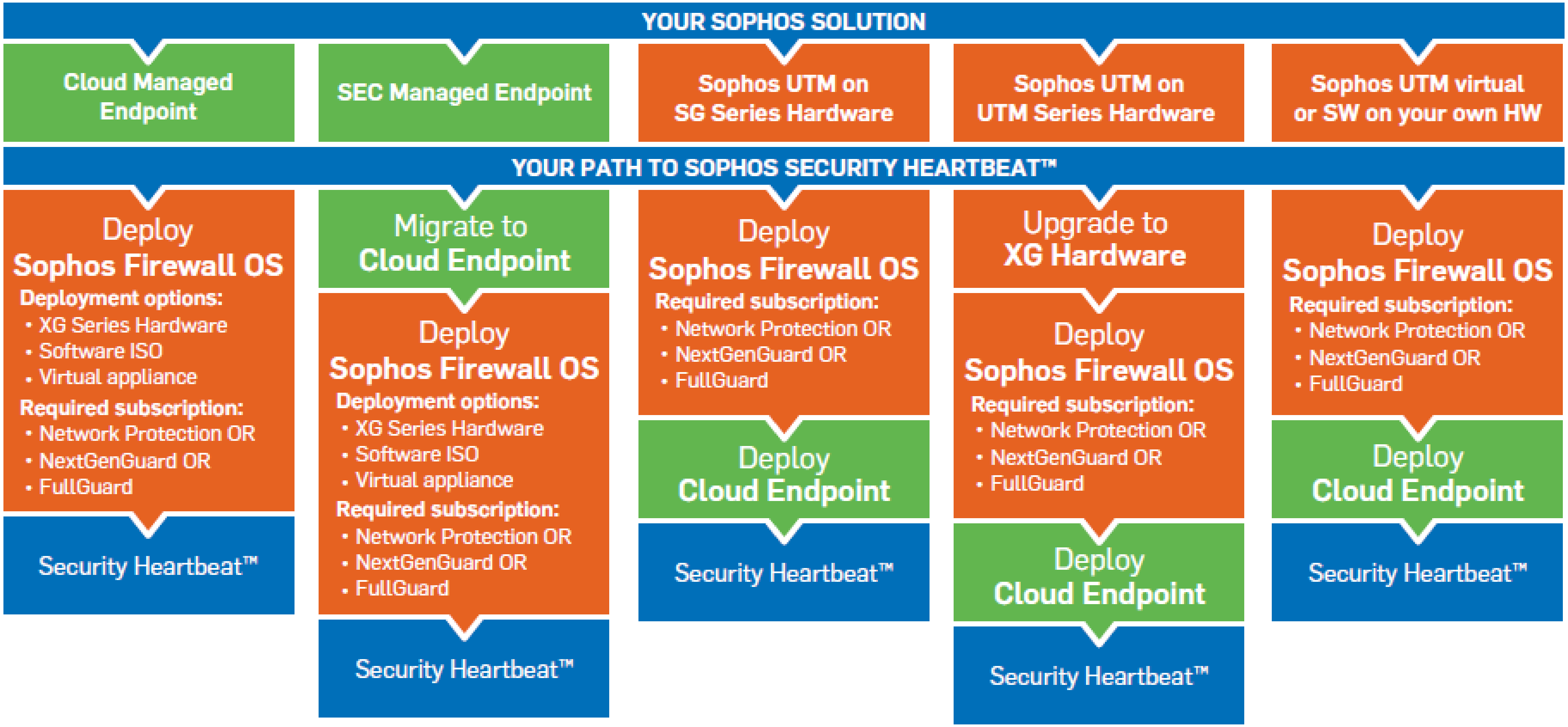


- Lockdown local network access
- Remove file encryption keys
- Terminate/remove malware
- Identify & clean other infected systems

SOPHOS

Your path to Synchronized Security

Already using Sophos



YOUR SOPHOS SOLUTION

YOUR PATH TO SOPHOS SECURITY HEARTBEAT™

Cloud Managed Endpoint

Deploy
Sophos Firewall OS

Deployment options:

- XG Series Hardware
- Software ISO
- Virtual appliance

Required subscription:

- Network Protection OR
- NextGenGuard OR
- FullGuard

Security Heartbeat™

SEC Managed Endpoint

Migrate to
Cloud Endpoint

Deploy
Sophos Firewall OS

Deployment options:

- XG Series Hardware
- Software ISO
- Virtual appliance

Required subscription:

- Network Protection OR
- NextGenGuard OR
- FullGuard

Security Heartbeat™

Sophos UTM on SG Series Hardware

Deploy
Sophos Firewall OS

Required subscription:

- Network Protection OR
- NextGenGuard OR
- FullGuard

Deploy
Cloud Endpoint

Security Heartbeat™

Sophos UTM on UTM Series Hardware

Upgrade to
XG Hardware

Deploy
Sophos Firewall OS

Required subscription:

- Network Protection OR
- NextGenGuard OR
- FullGuard

Deploy
Cloud Endpoint

Security Heartbeat™

Sophos UTM virtual or SW on your own HW

Deploy
Sophos Firewall OS

Required subscription:

- Network Protection OR
- NextGenGuard OR
- FullGuard

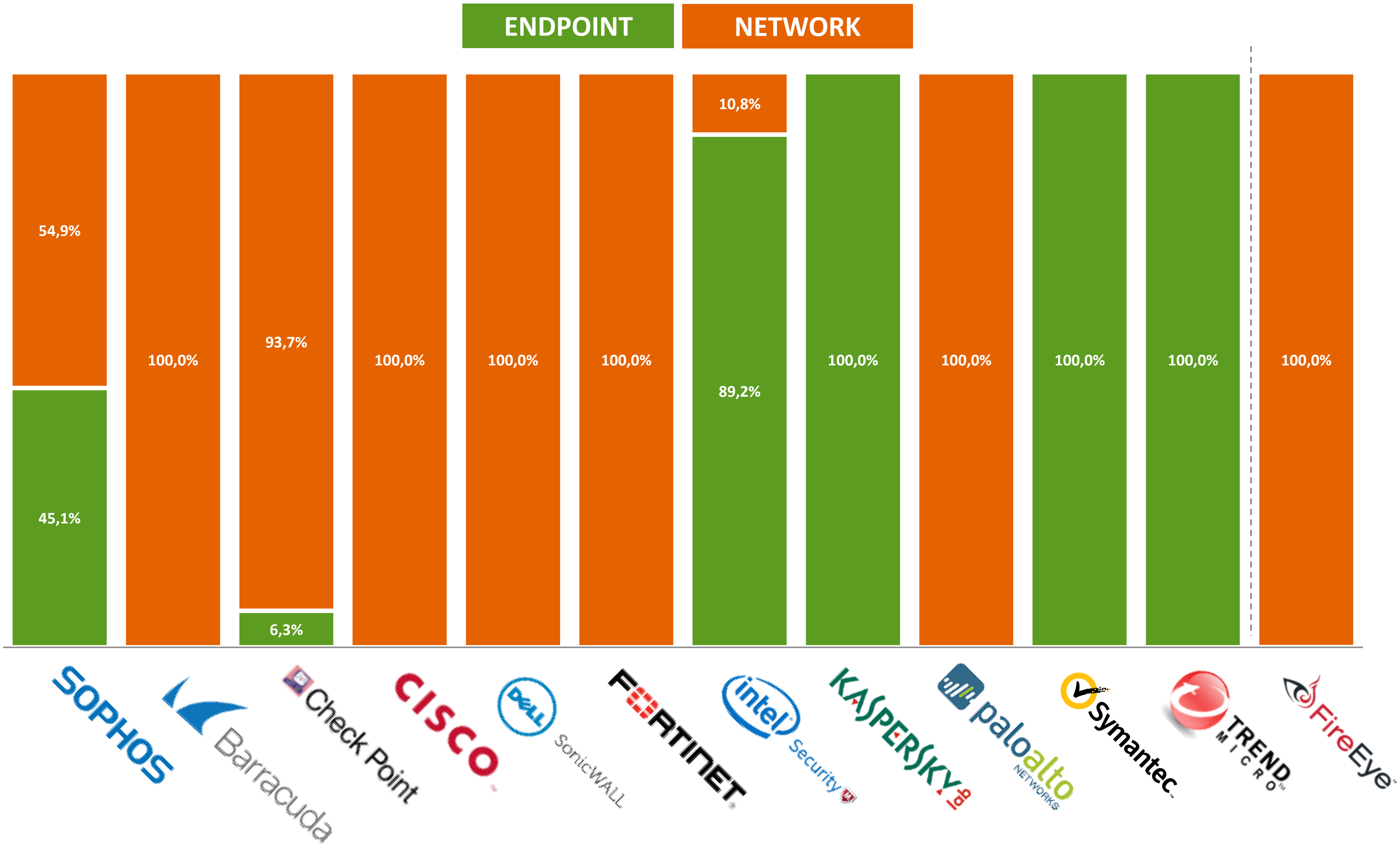
Deploy
Cloud Endpoint

Security Heartbeat™

* Cloud Endpoint requires Sophos Cloud Endpoint Protection Advanced or Sophos Cloud Enduser Protection subscriptions

Conclusion

Unique balance between Endpoint and Network



SOPHOS