Threat Landscape

Cybercrime Dynamics

TODAY

INTEGRATED BUSINESS MODEL (WannaCry, Locky, CryptoLocker)

INDUSTRIALIZATION (RIG Exploit Kit, Neutrino Exploit Kit)

AUTOMATION (Asprox botnet, Blackhole, Zeus)

EFFICIENT ECOSYSTEMS (Mpack, Conficker)

EARLY COMMERCIALIZATION (Loveletter, Pump & Dump email)

DIGITAL GRAFFITI (Melissa, CodeRed worm)

EVOLUTION OF CYBERCRIME OVER TIME >

COMPOUNDING FACTORS

LEVEL / SOURCES OF FUNDING	NUMBER OF THREATS	THREAT SOPHISTICATION	RANSOMWARE
NON-WINDOWS/ MOBILE	NUMBER & RANGE OF ACTORS	PROLIFERATION / NATION STATE	

SOPHOS

3

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
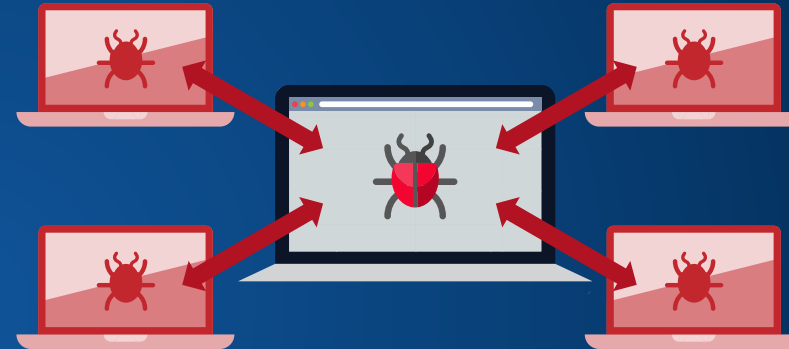*Network and endpoint integrated*

Synchronized Security

SOPHOS

Synchronized Security

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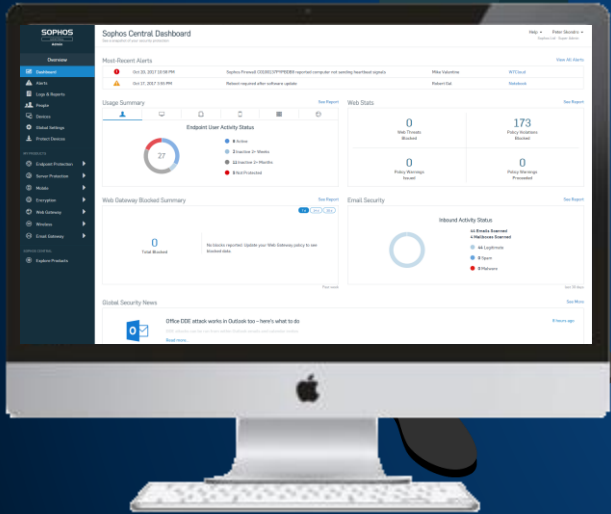
SOPHOS

Synchronized Security

XG Firewall

Next-Gen Endpoint

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

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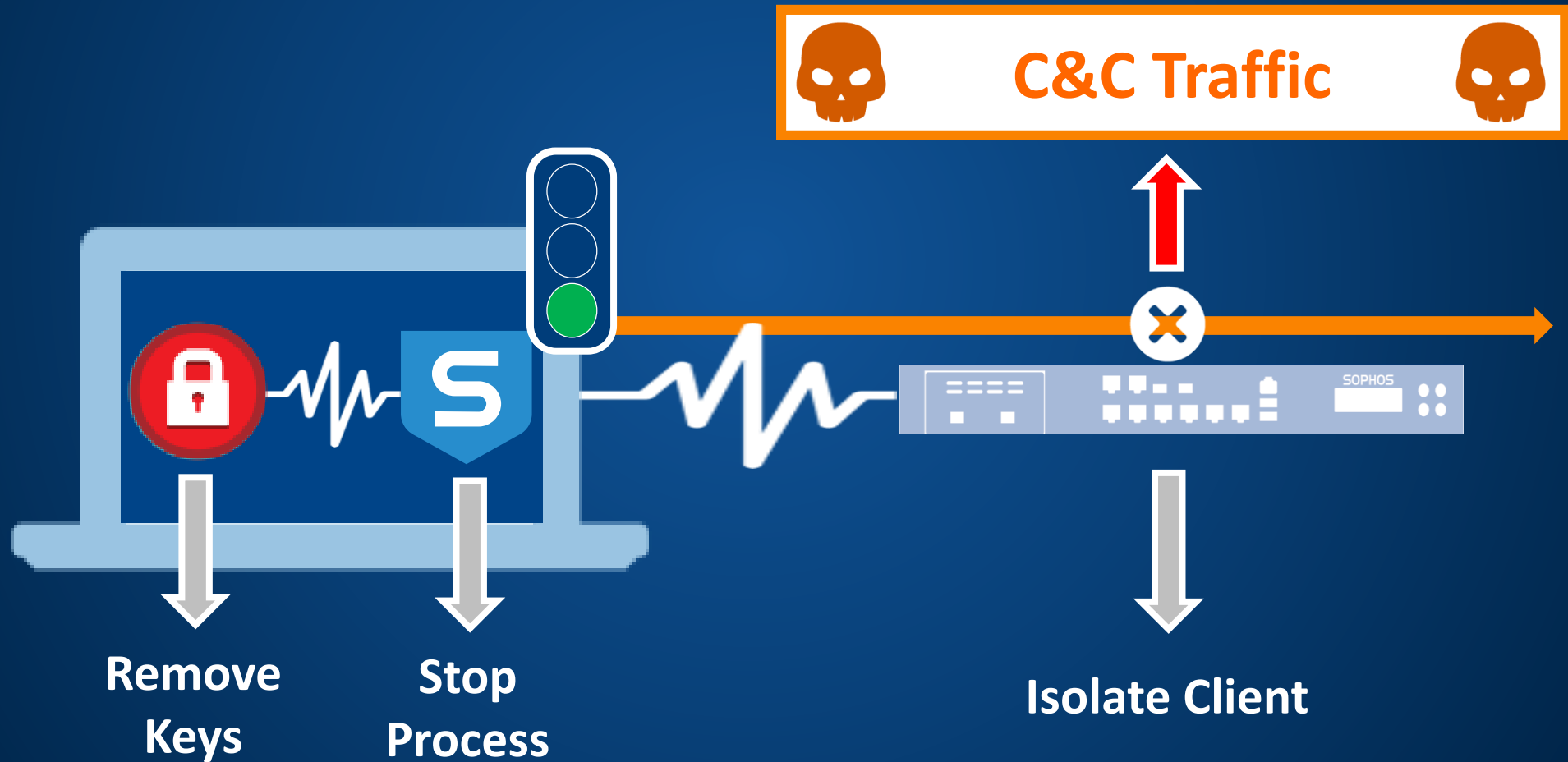Share security intelligence to positively identify infected users, systems and processes

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

SOPHOS

Security Heartbeat – Malware Detection

Malware

Remove Keys

Isolate Client

SOPHOS
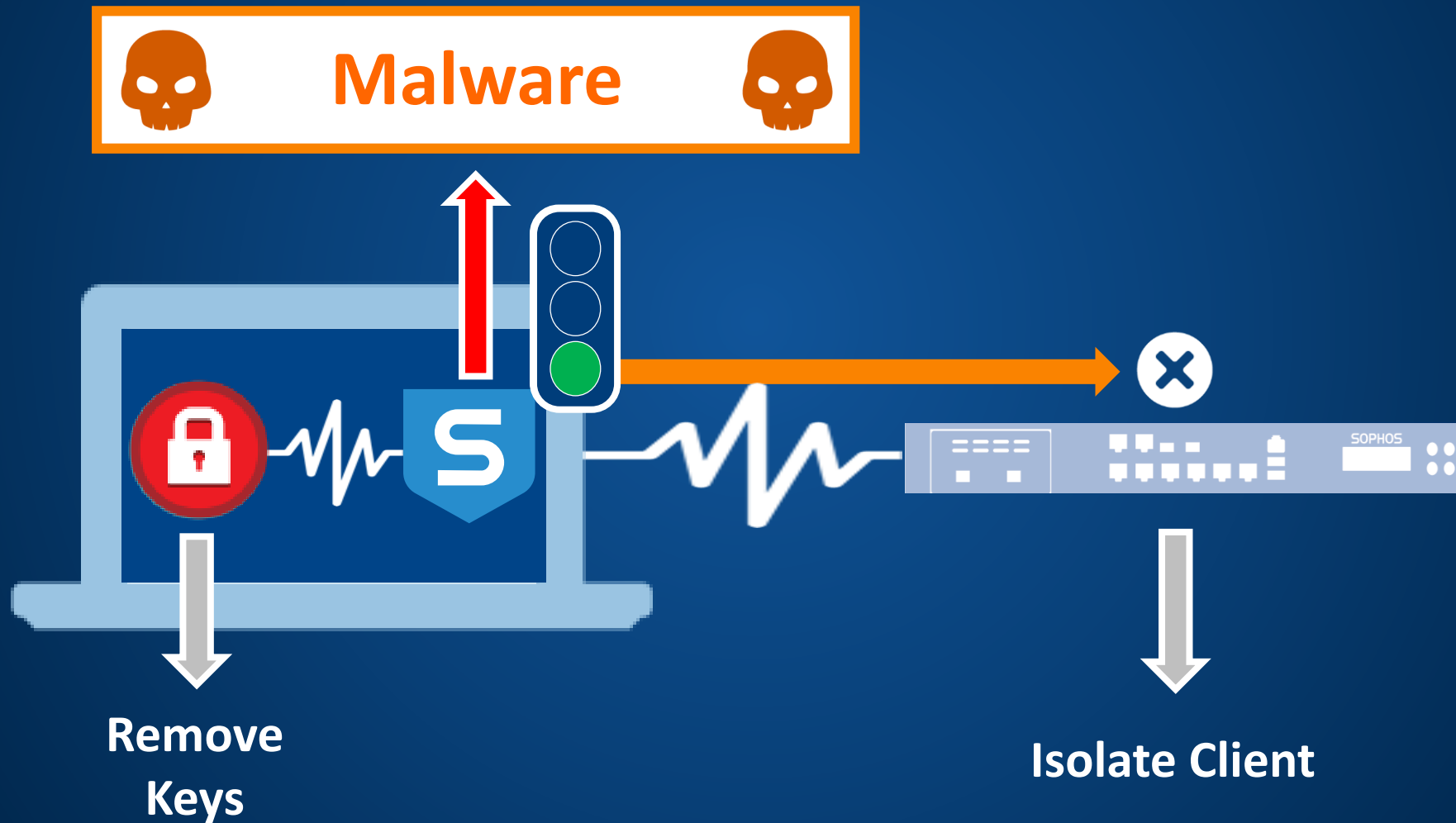
Security Heartbeat – Botnet C&C-Traffic Detection

C&C Traffic

Remove Keys

Stop Process

Isolate Client

SOPHOS

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.
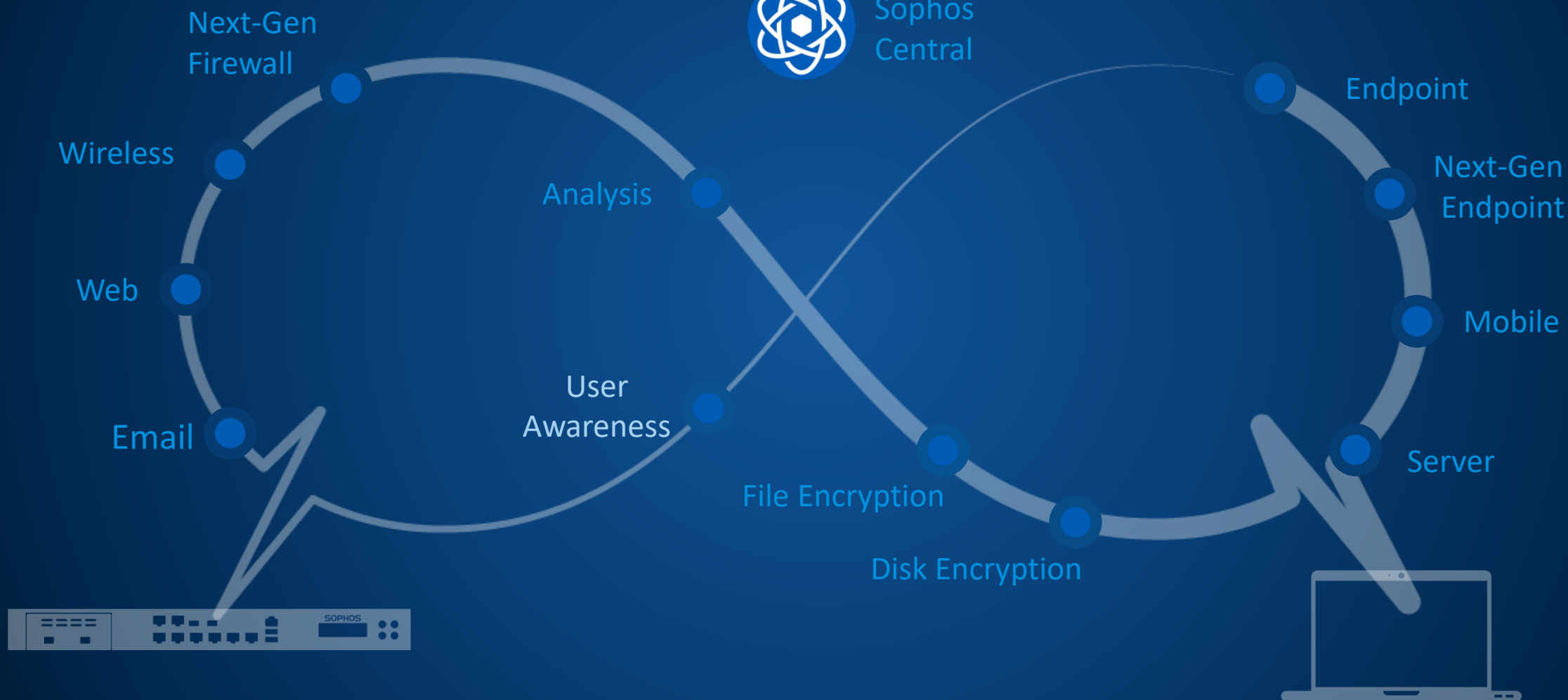
Automated Incident Response

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.

SOPHOS

Free Tools

SOPHOS

Free Tools

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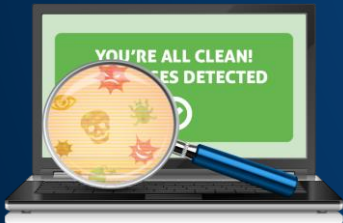
Sophos Home

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