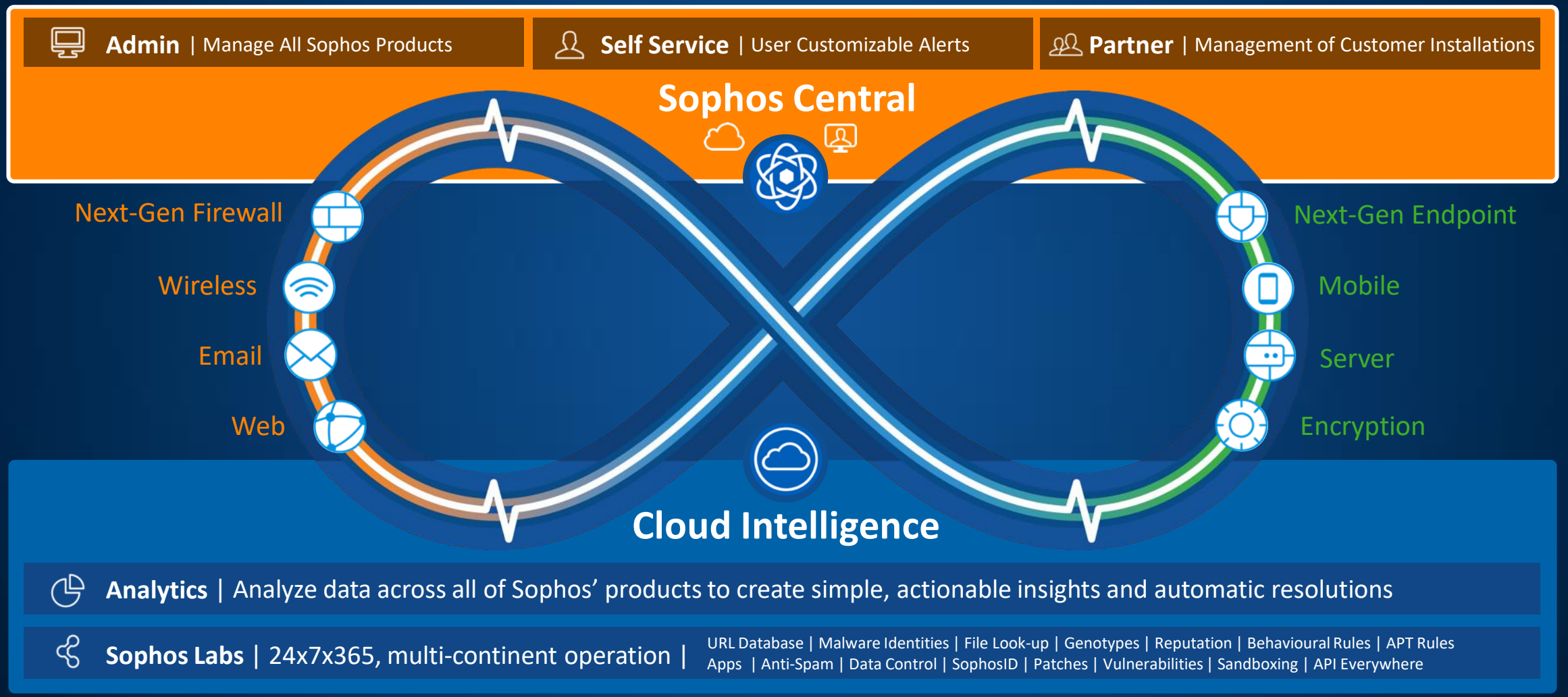
Sophos Synchronized Security
Bezpečnost jako systém

Michal Hebeda
Sales Engineer

SOPHOS

Platforma Synchronized Security a Strategie



SOPHOS

Synchronized Security - Koncept

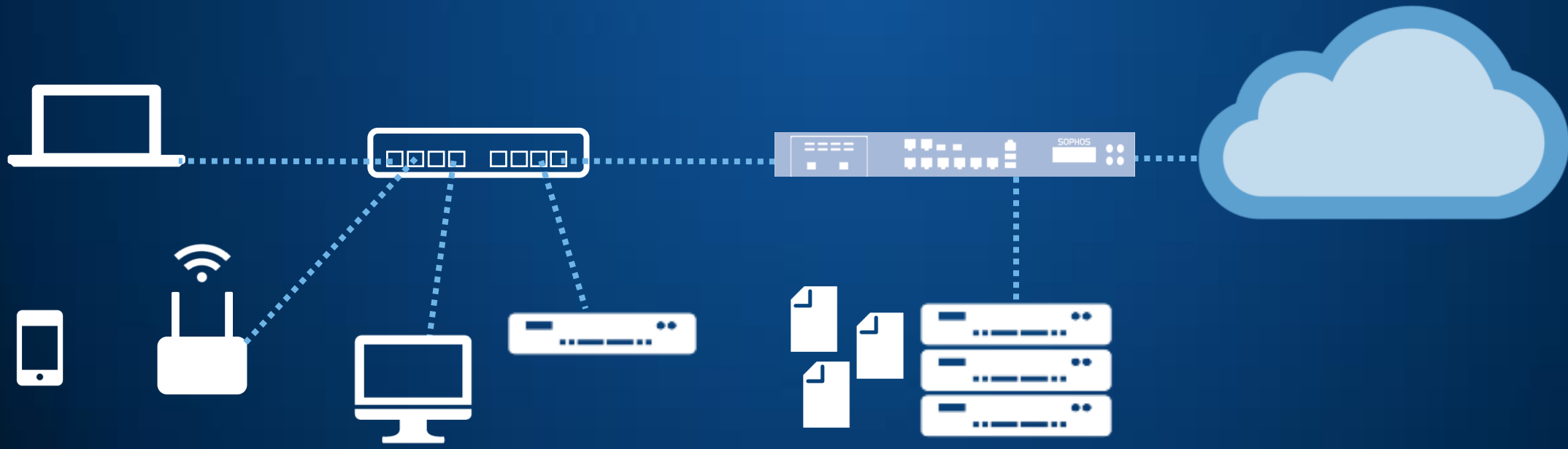
- Bezpečnostní komponenty jednají jako systém
- Výměna informací mezi komponentami
  - Bezpečnostní stav zařízení
  - Přenosy aplikací
  - Kontext uživatele
- Cíle
  - Zlepšení detekce hrozeb a aktivit hackerů
  - Automatická izolace hrozeb
  - Ochrana kritických dat
  - Lepší viditelnost aplikací

Proč potřebujeme Synchronized Security?

SOPHOS

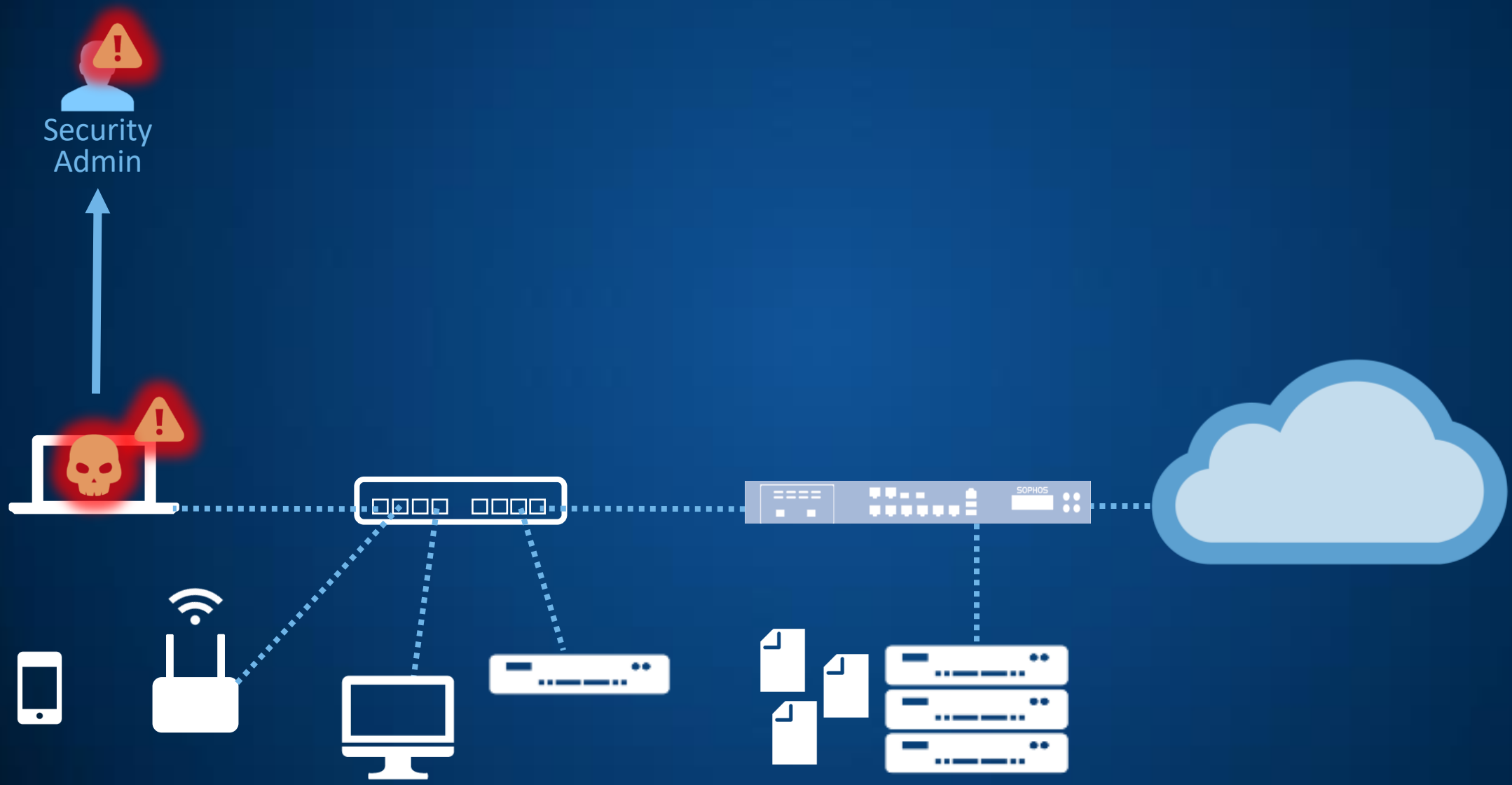

IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Zpracování hrozeb bez Synchronized Security



SOPHOS

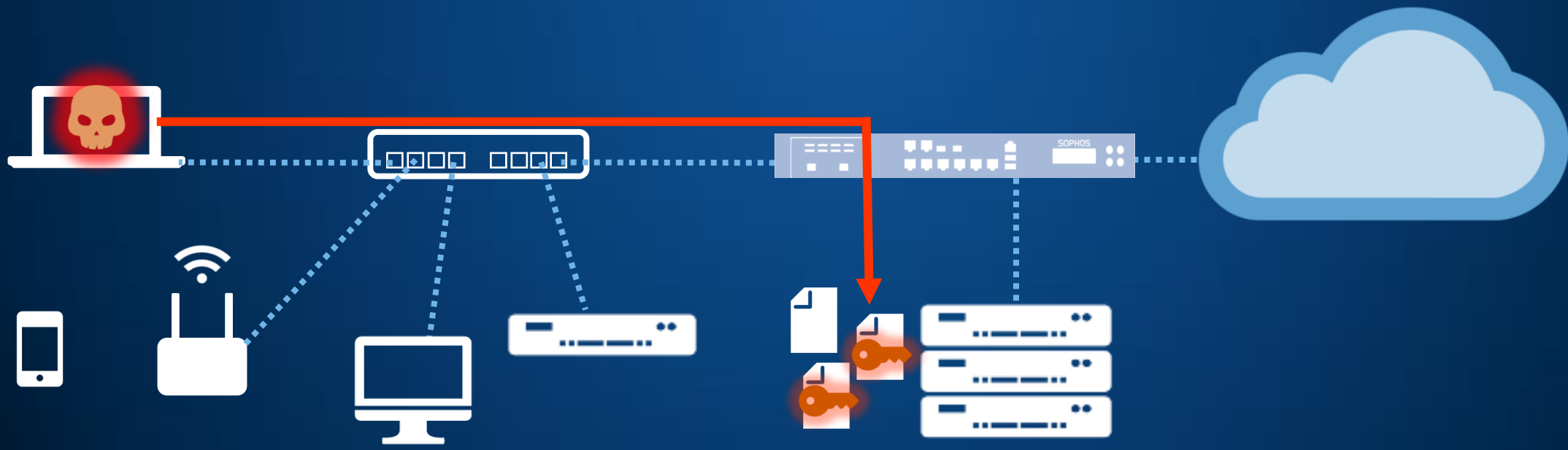
Hrozba je rozpoznána



.. a analyzována

Security Admin

Soubory jsou zašifrovány na souborovém serveru

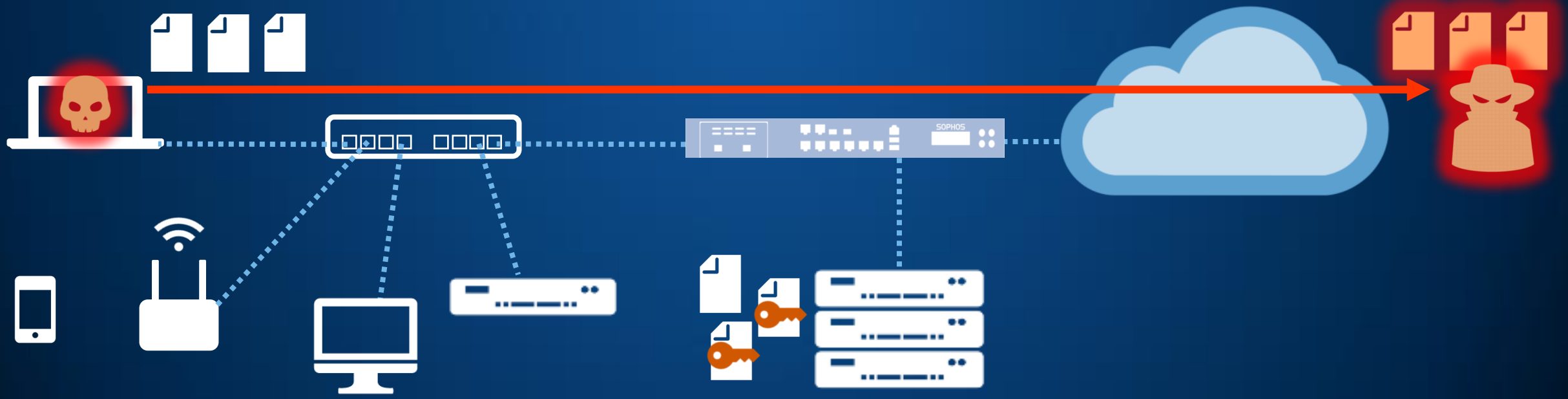


SOPHOS

.. a analyzována

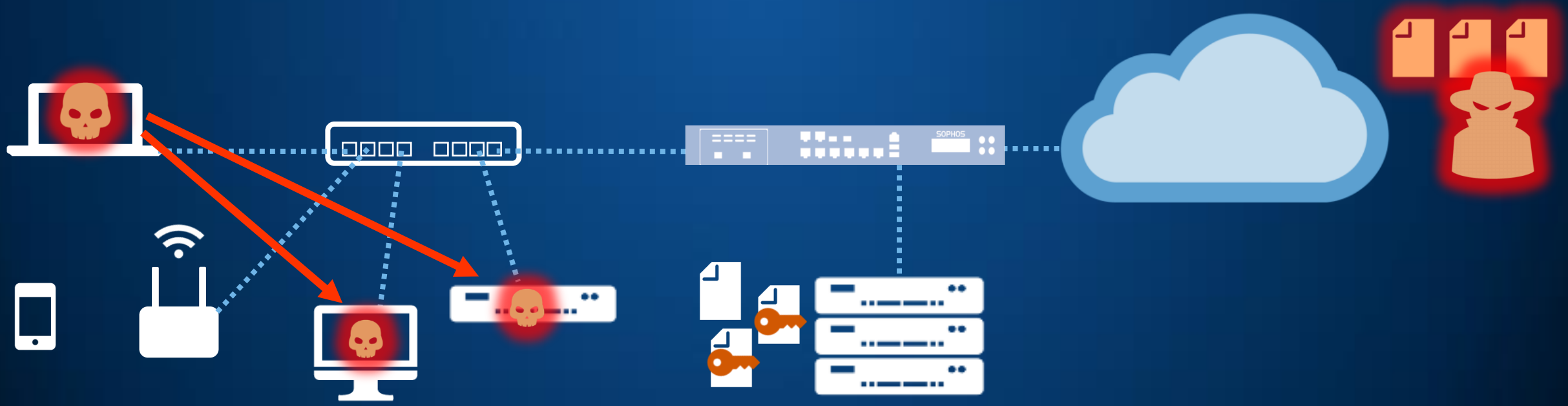
Security Admin

..a citlivá data odeslána útočníkovi v internetu

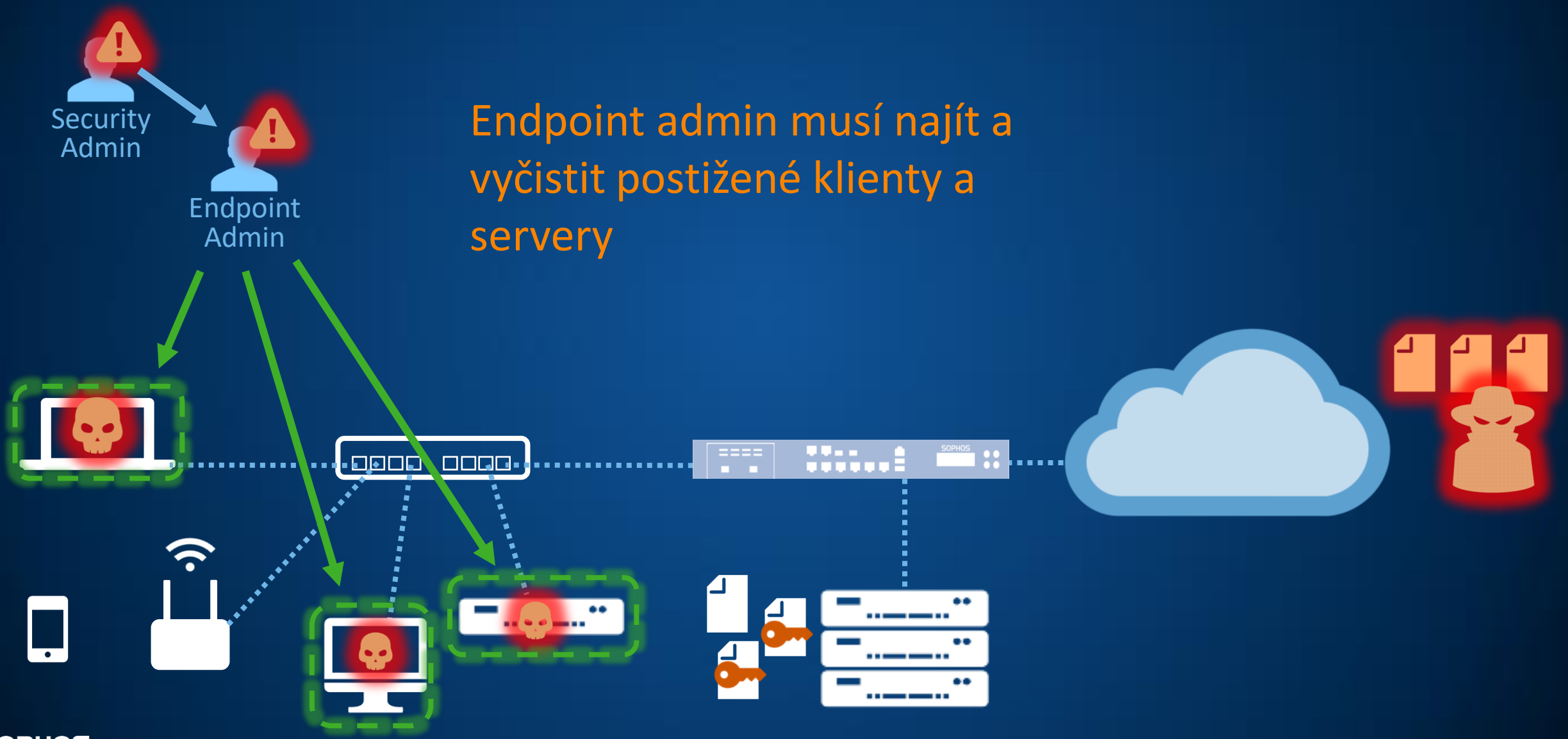


.. a analyzována

.. navíc i ostatní endpointy
a servery jsou infikovány

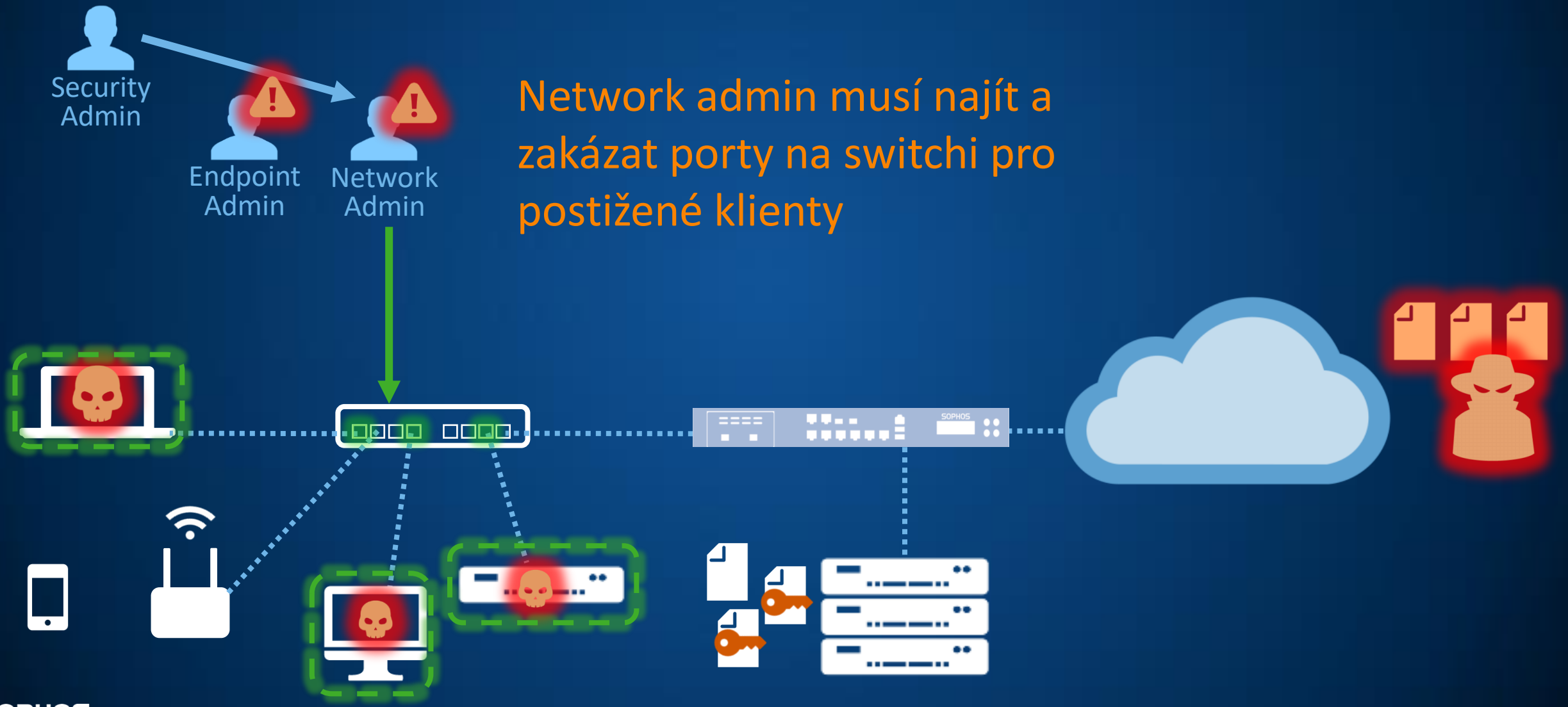


Akce!!!



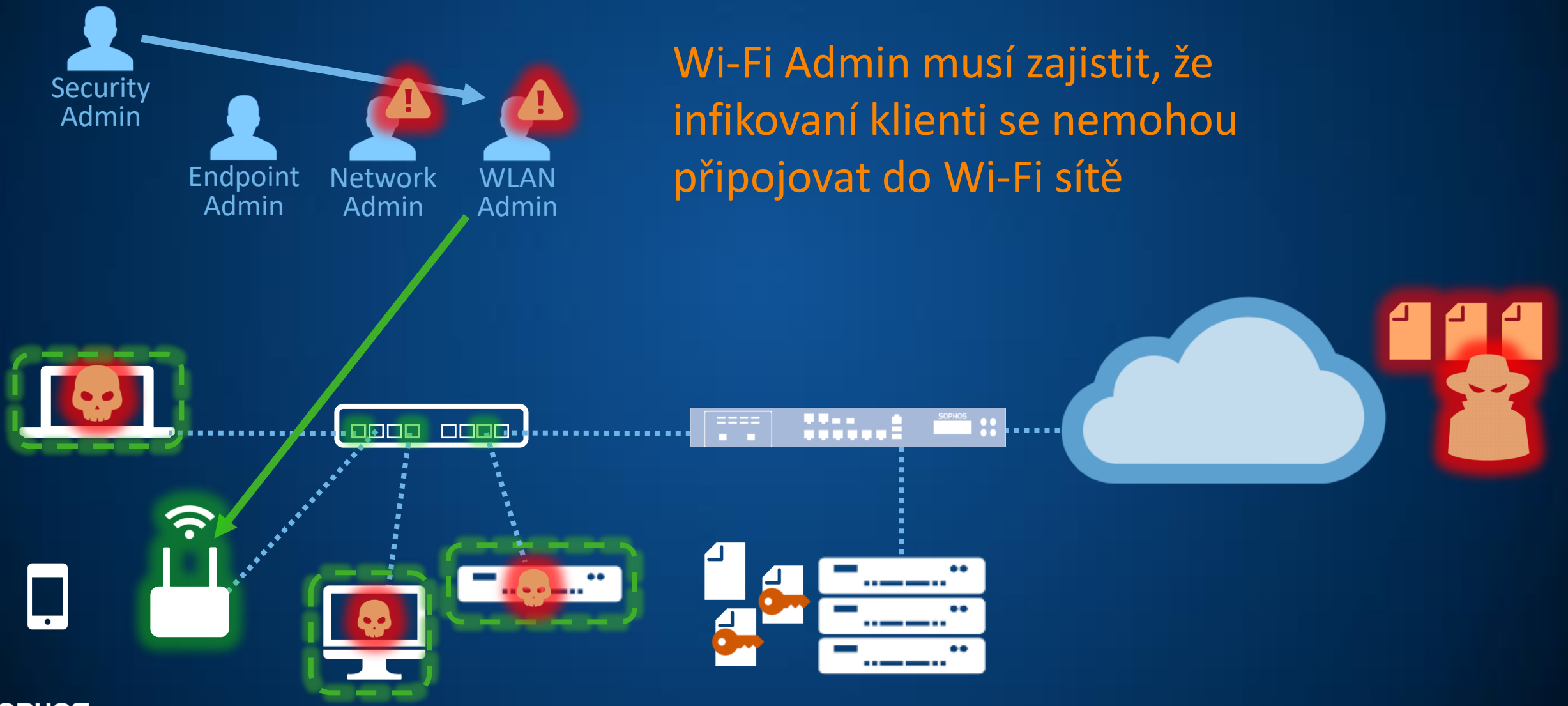
Endpoint admin musí najít a vyčistit postižené klienty a servery

Akce!!!



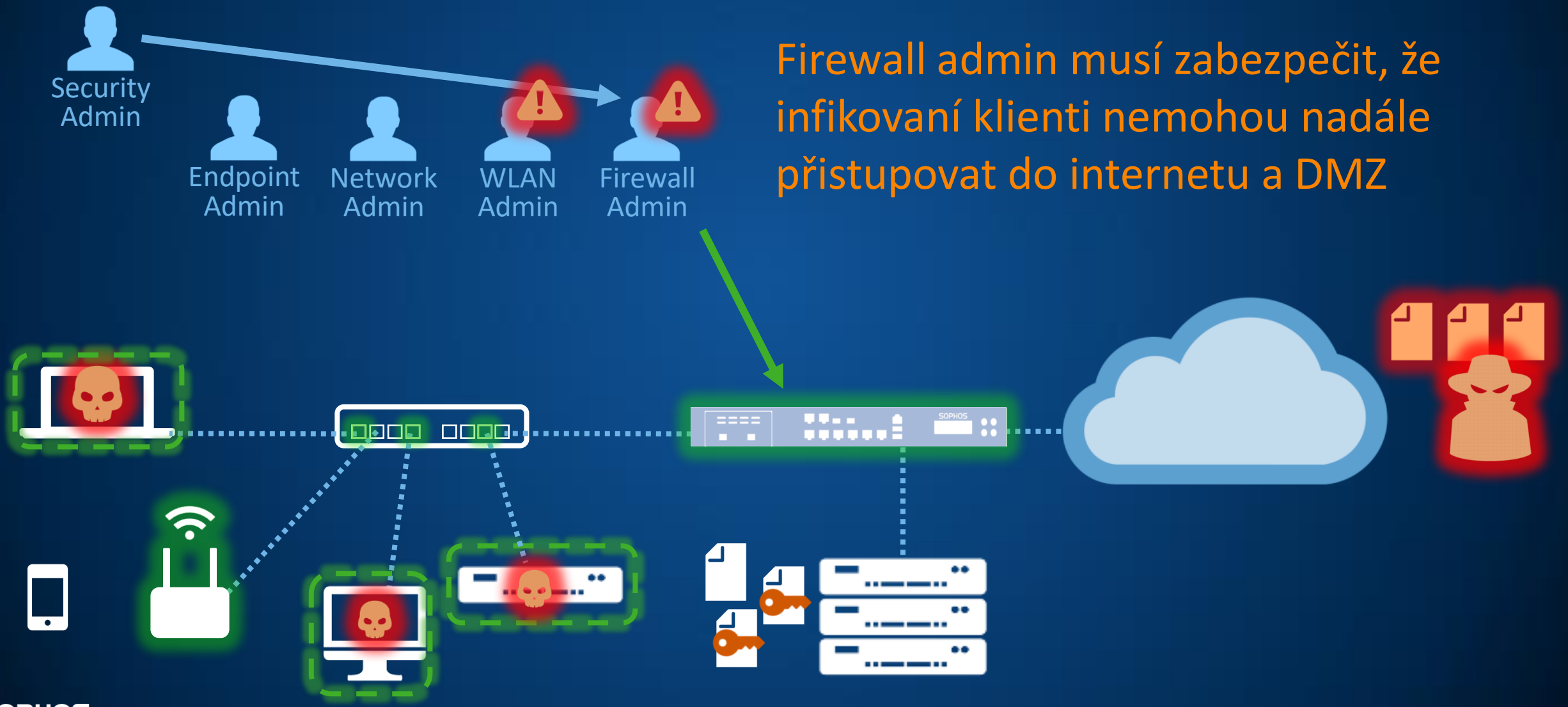
Network admin musí najít a zakázat porty na switchi pro postižené klienty

Akce!!!



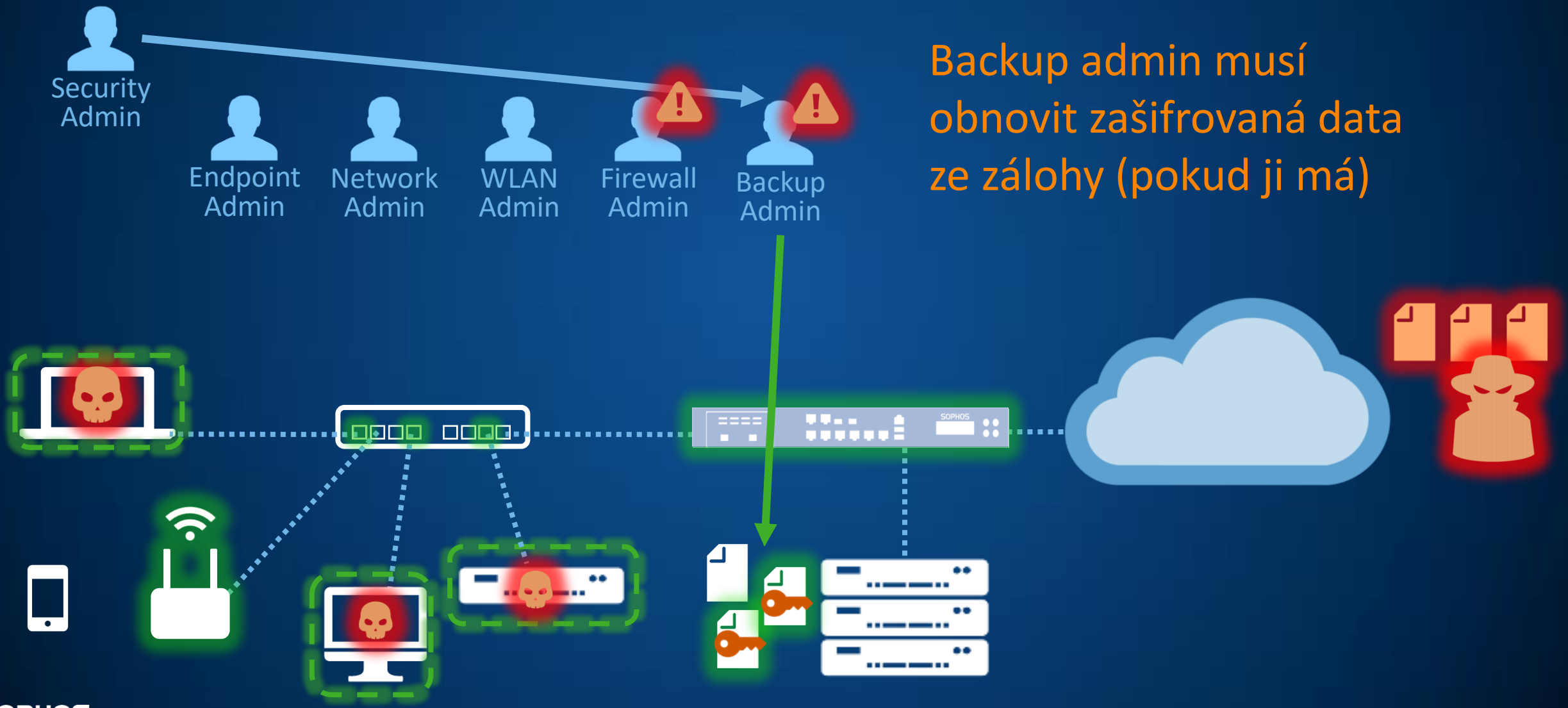
Wi-Fi Admin musí zajistit, že infikovaní klienti se nemohou připojovat do Wi-Fi sítě

Akce!!!



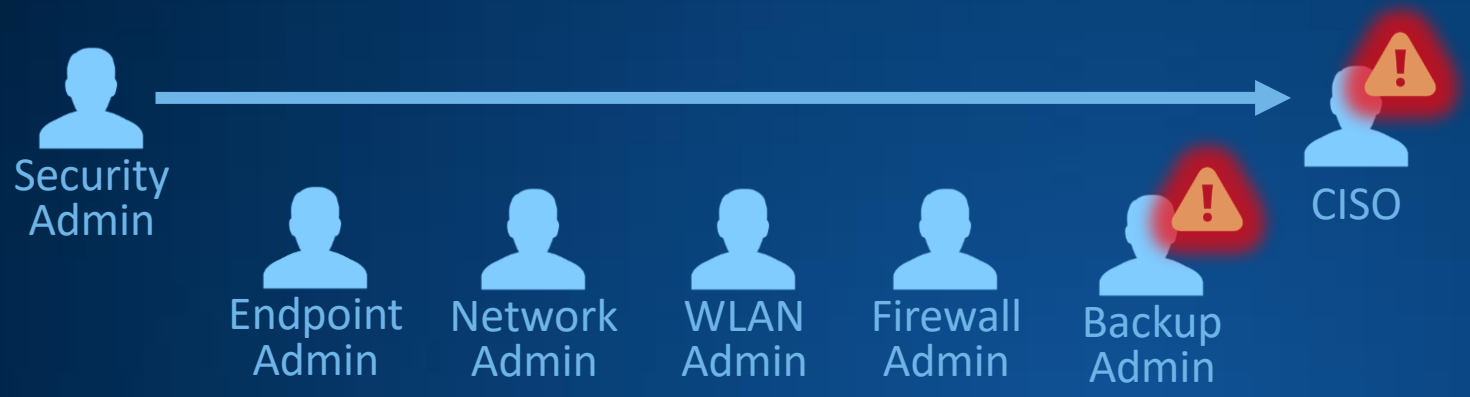
Firewall admin musí zabezpečit, že infikovaní klienti nemohou nadále přistupovat do internetu a DMZ

Akce!!!

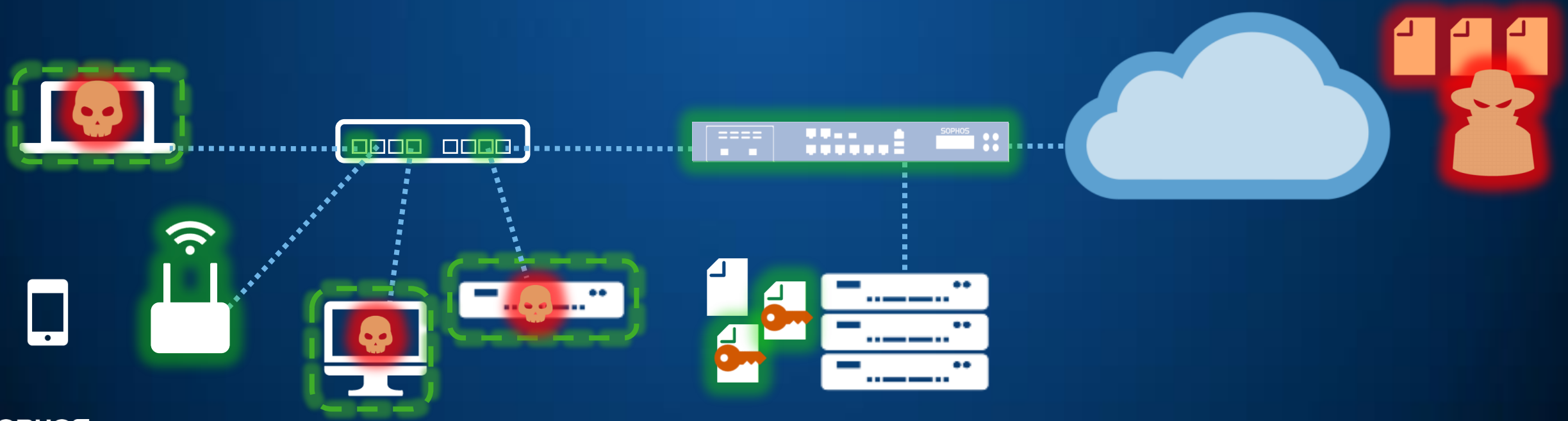


Backup admin musí obnovit zašifrovaná data ze zálohy (pokud ji má)

Akce!!!



Nyní je informován CISO...



Akce!!!

Security Admin

Endpoint Admin

Network Admin

WLAN Admin

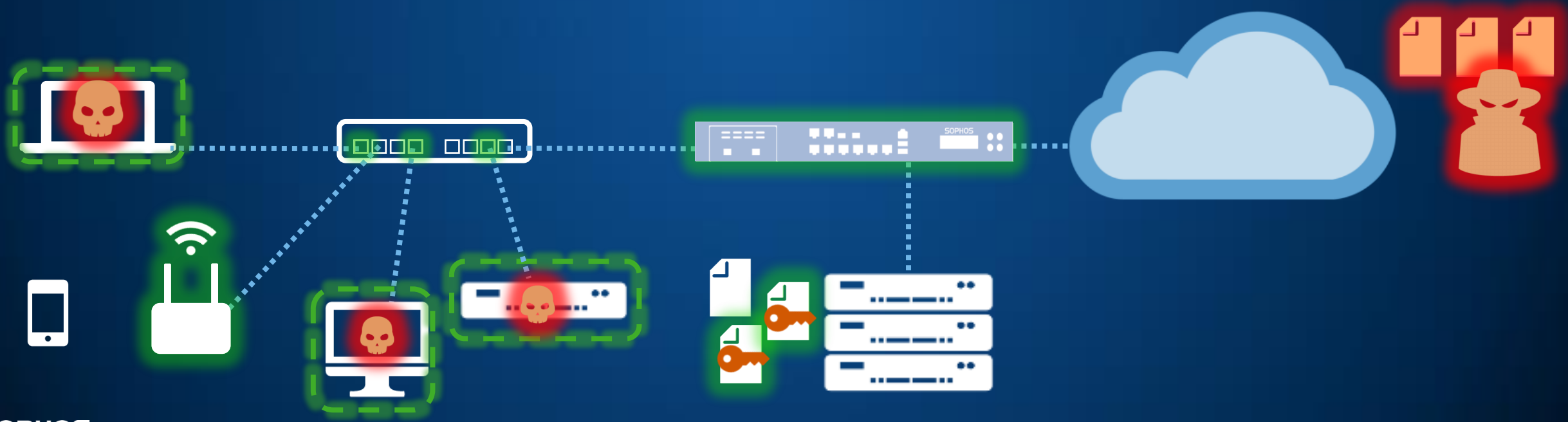
Firewall Admin

Backup Admin

CISO

CEO

.. Informování managementu, že data byla odcizena

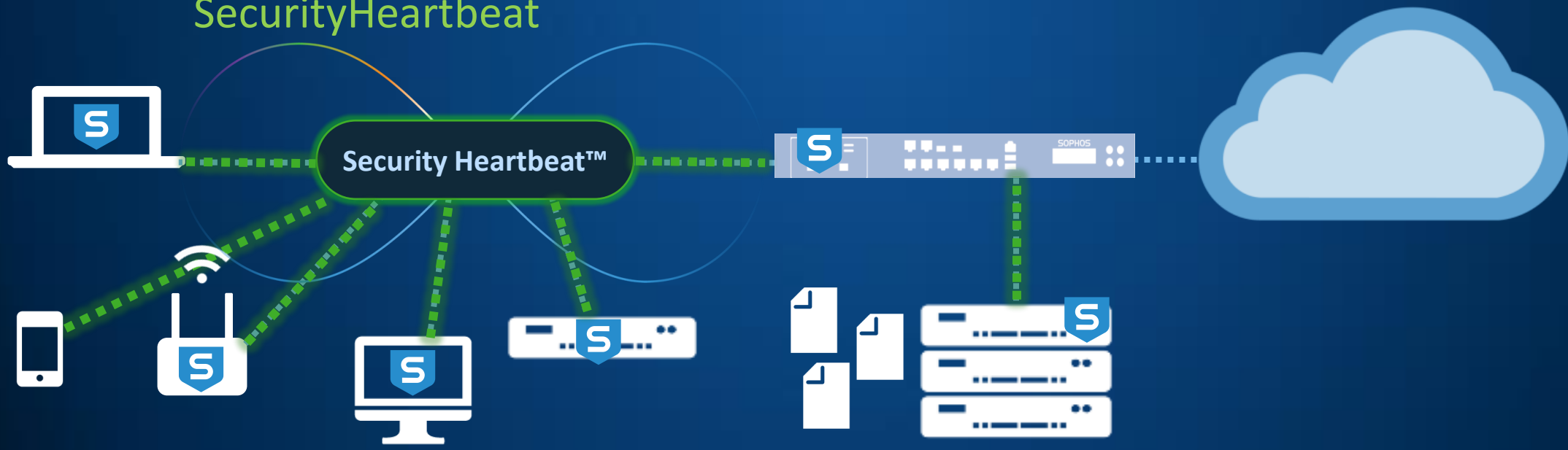


Procedura pro bezpečnostní incidenty se Synchronized Security

SOPHOS

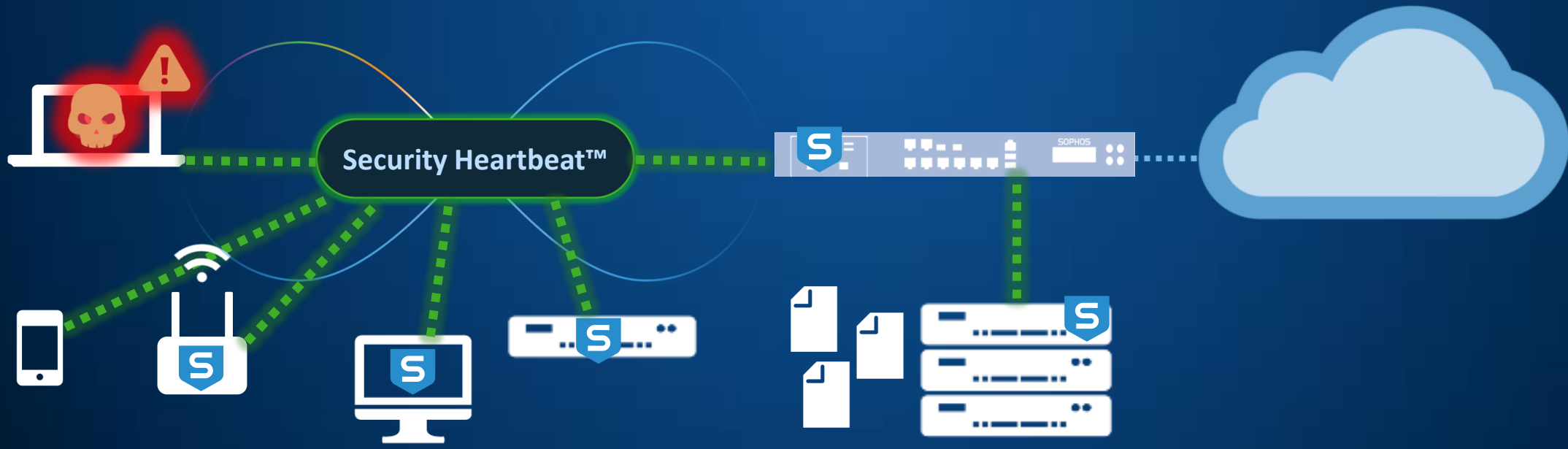
Zpracování hrozeb se Synchronized Security

Klienti, servery, mobilní zařízení, WiFi APs a firewally komunikují přímo se sebou navzájem pomocí SecurityHeartbeat



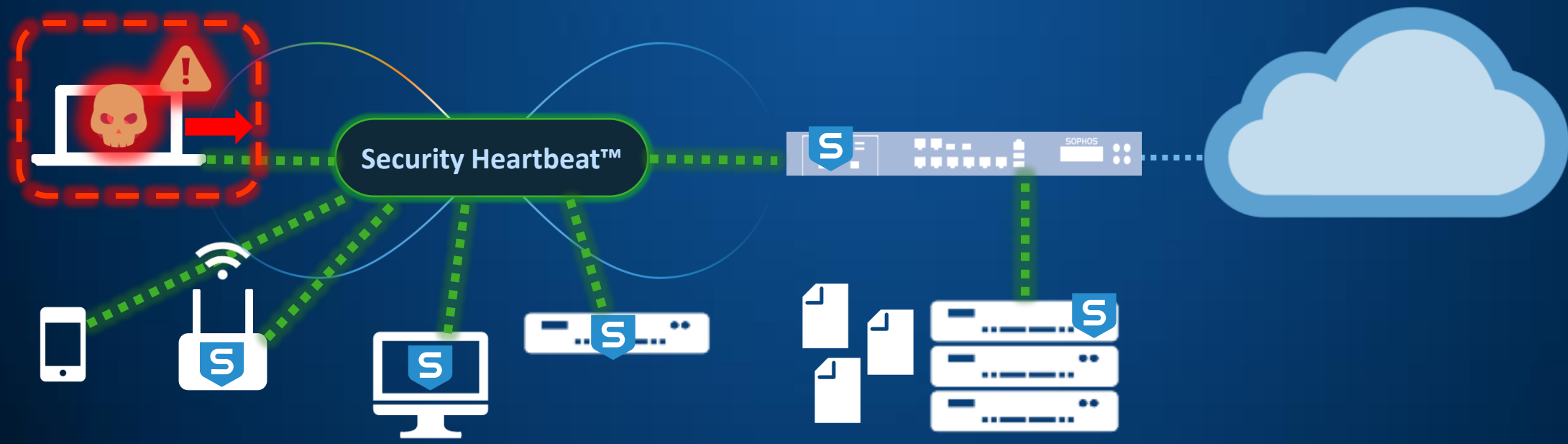
Zpracování hrozeb se Synchronized Security

V případě hrozby jsou všechny komponenty informovány a reagují automaticky



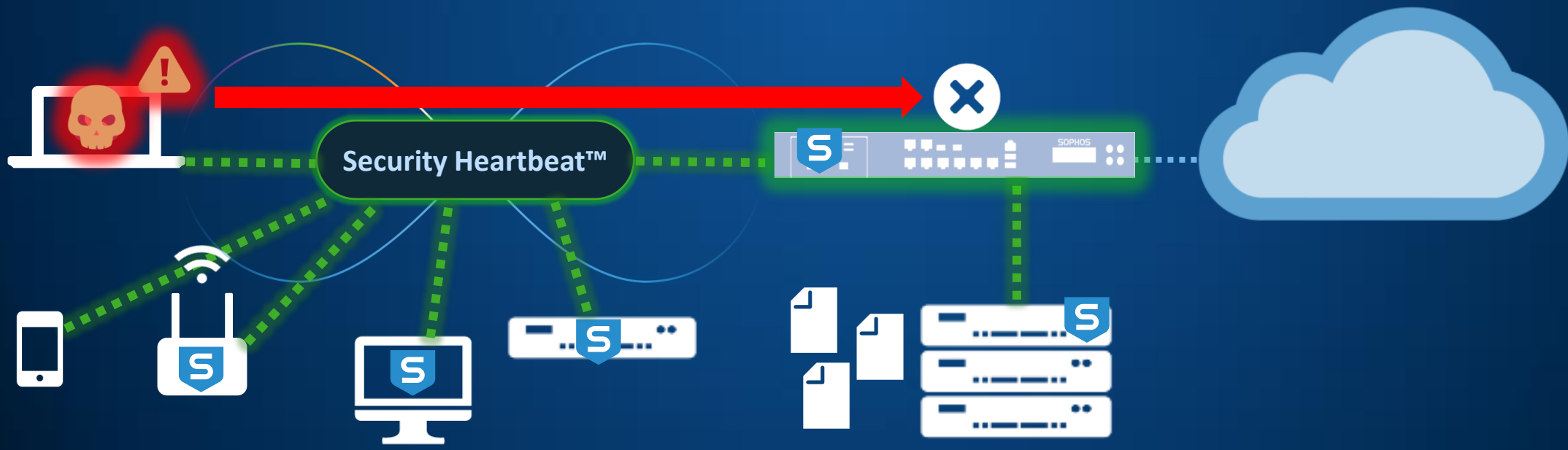
Zpracování hrozeb se Synchronized Security

Klient izoluje sám sebe ...



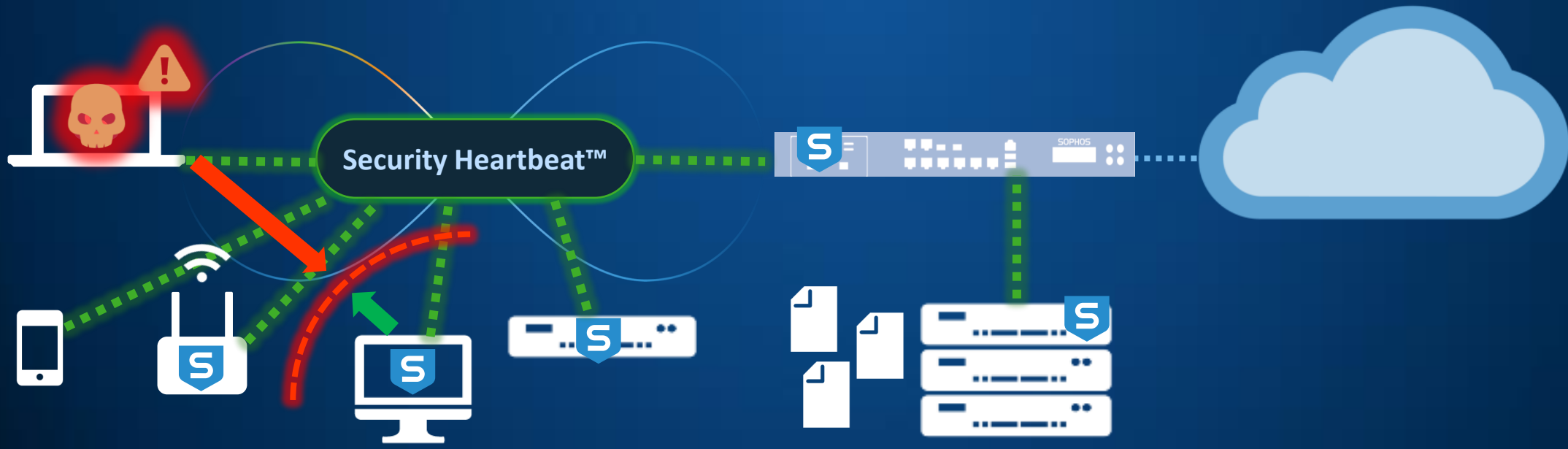
Zpracování hrozeb se Synchronized Security

Firewall přesune klienta do šíťové karantény a znemožní další komunikaci do internetu nebo DMZ



Zpracování hrozeb se Synchronized Security

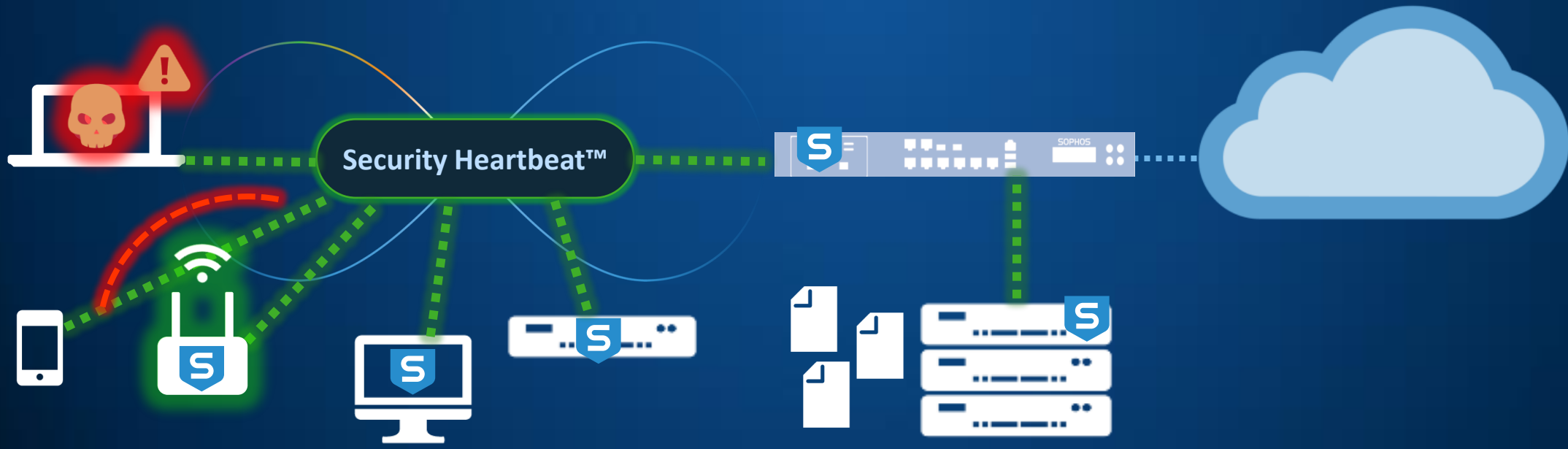
Klienti a servery ve stejné síti
(broadcastové doméně) nemohou
nadále komunikovat
s infikovaným klientem



SOPHOS

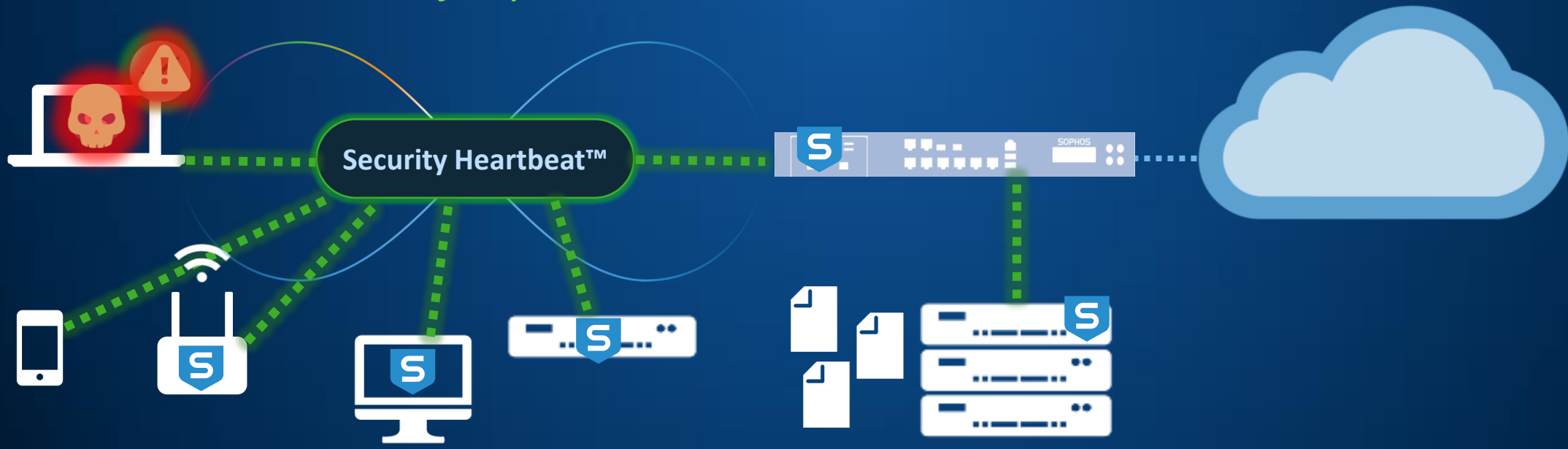
Zpracování hrozeb se Synchronized Security

WiFi přístupové body nedovolí infikovaným klientům přístup do interní LAN sítě

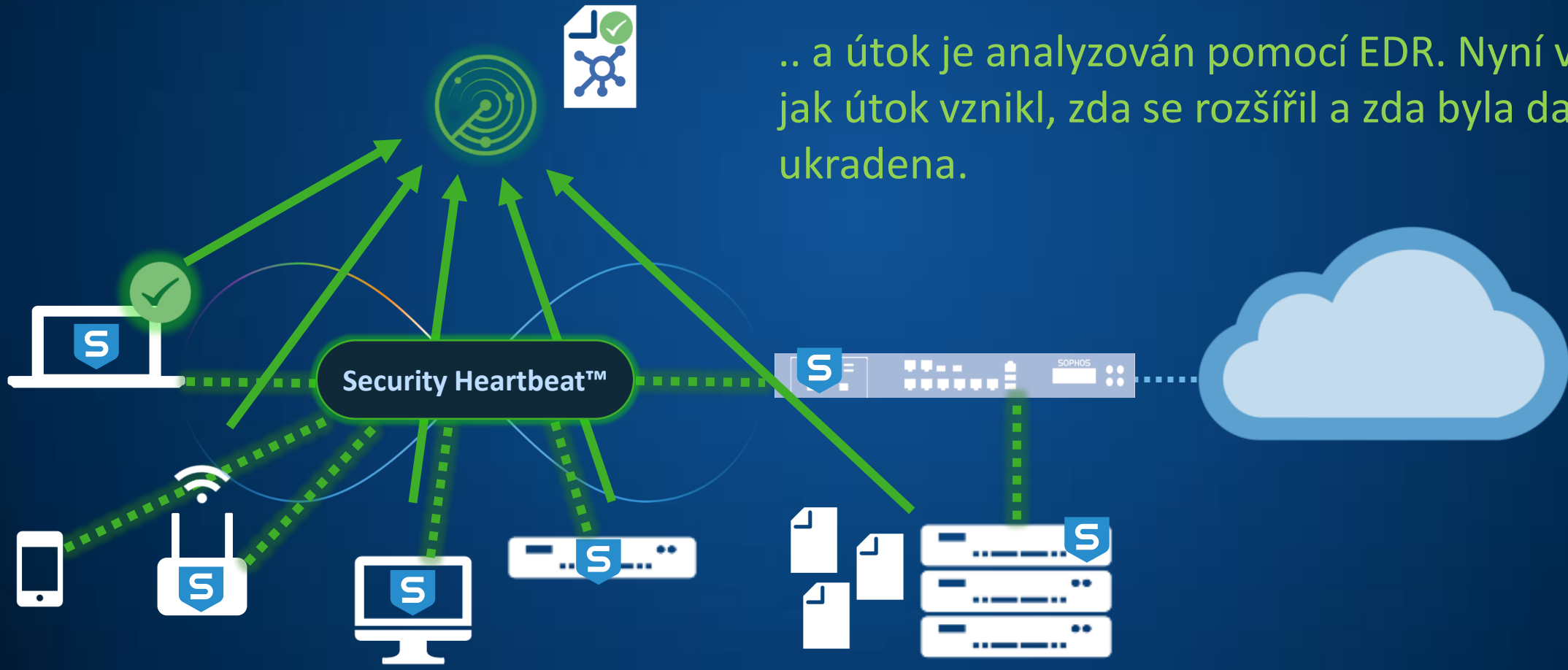


Zpracování hrozeb se Synchronized Security

..a hrozba je vyřešena..



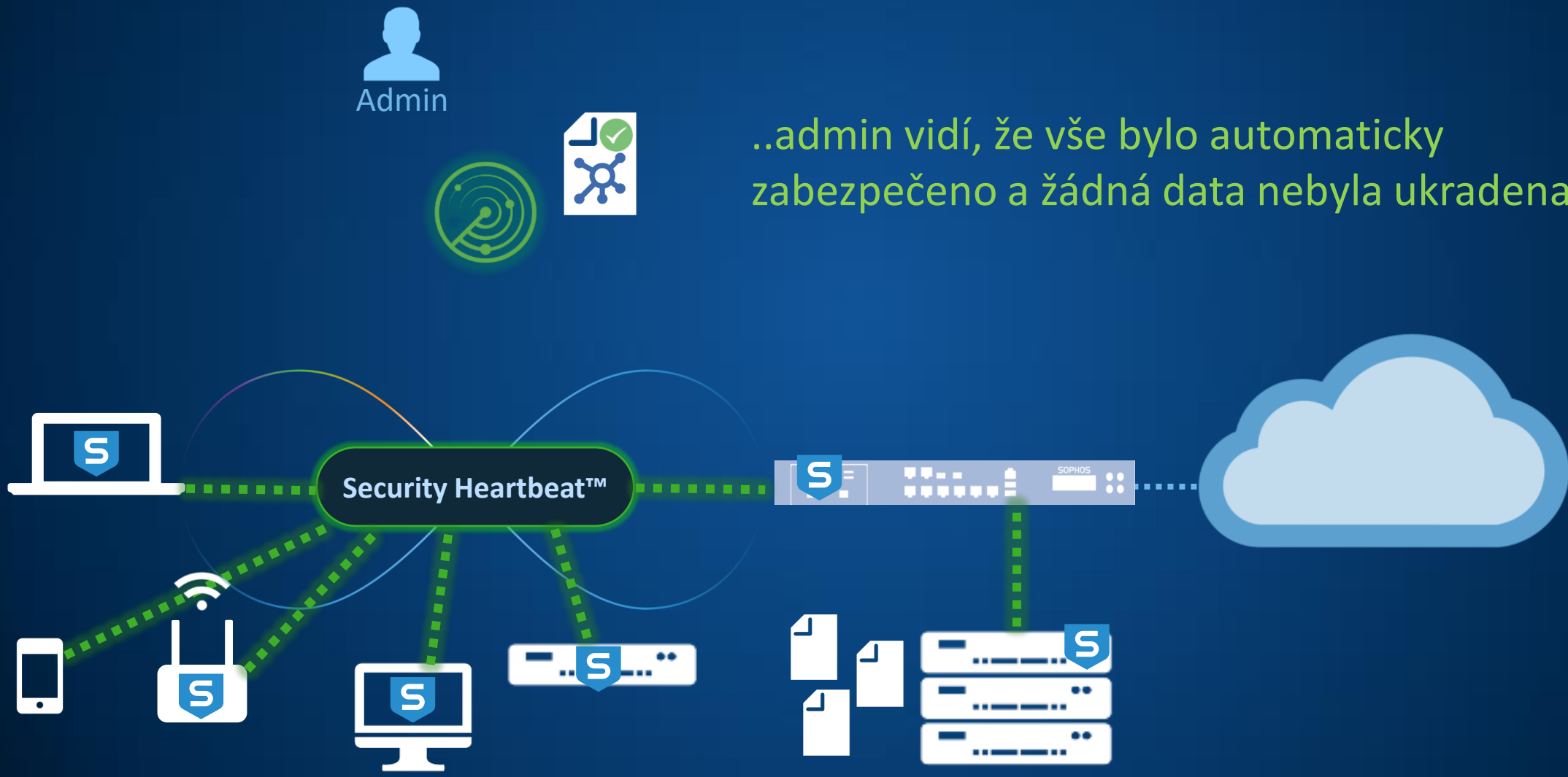
Zpracování hrozeb se Synchronized Security



.. a útok je analyzován pomocí EDR. Nyní víme, jak útok vznikl, zda se rozšířil a zda byla data ukradena.

SOPHOS

Zpracování hrozeb se Synchronized Security



..admin vidí, že vše bylo automaticky zabezpečeno a žádná data nebyla ukradena ..

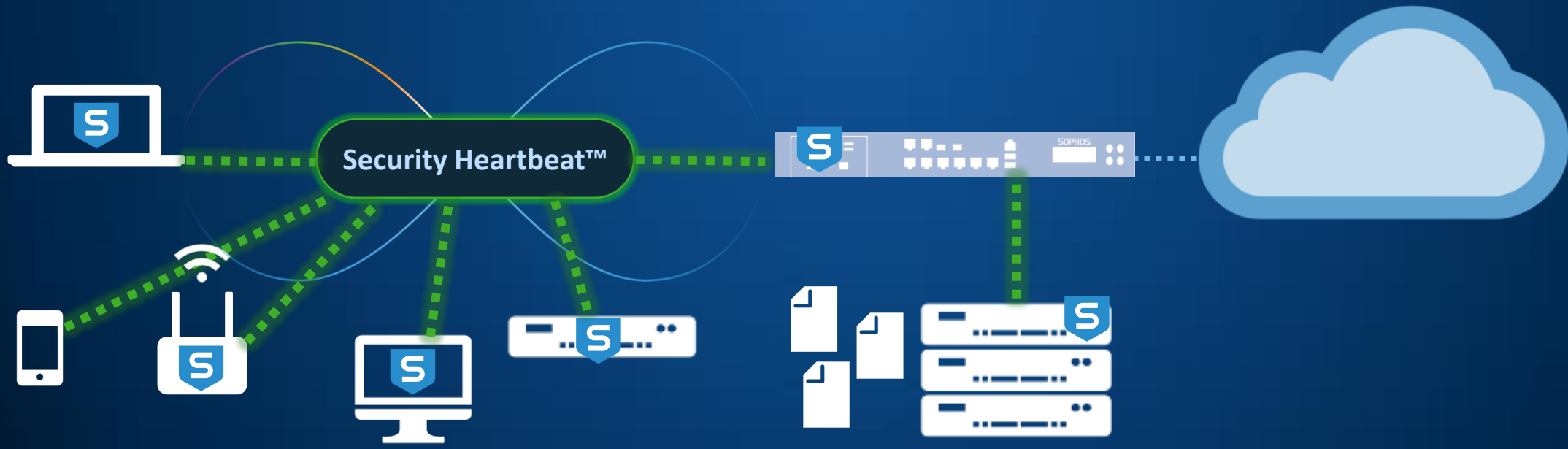
SOPHOS

Zpracování hrozeb se Synchronized Security

Admin

CEO

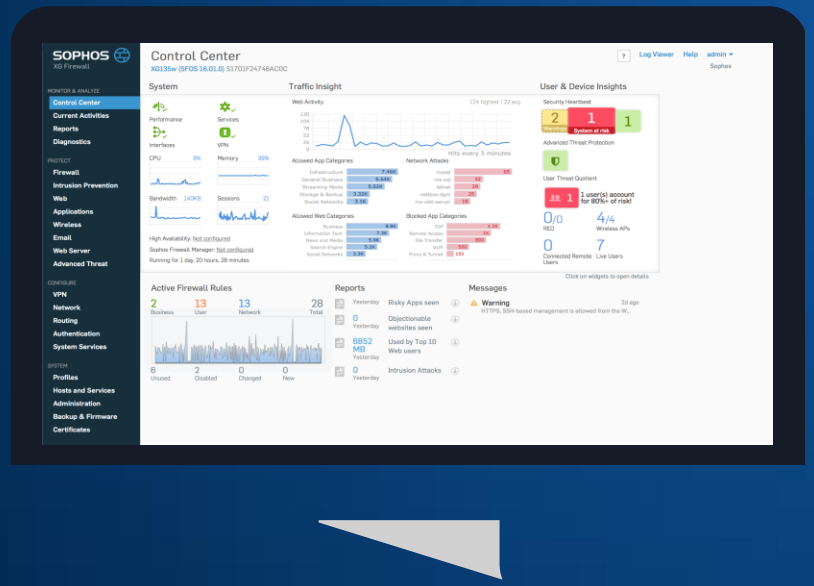
..a šéf je spokojen, že IT bezpečnost funguje.

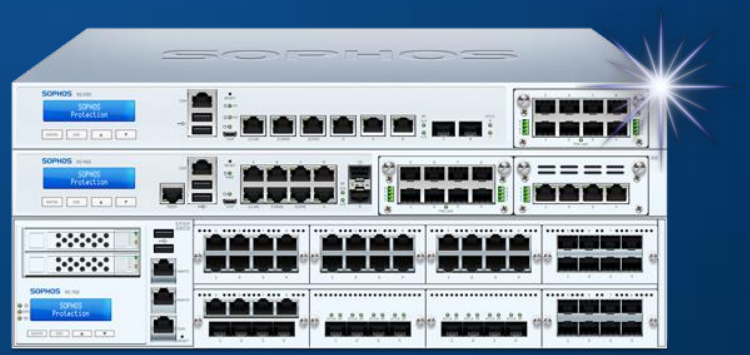


SOPHOS

Sophos XG

Firewall





SOPHOS

Filozofie designu XG Firewallu

Zlepšený přehled

Filozofie designu XG Firewallu

- Připraveno pro běžného IT managera střední společnosti
- Vše důležité o co se musíte starat – na jednom přehledu se semaforovými indikátory
- Na 2 kliknutí kamkoliv = Rychlý přístup k podrobnějším informacím
- Interaktivní widgety s podrobnějšími informaci na prokliknutí

Zajišťuje adminům jednotný přehled všeho, co je důležité

Výhody XG Firewallu

Co dělá XG Firewall lépe a jak…

1. Blokuje neznámé hrozby

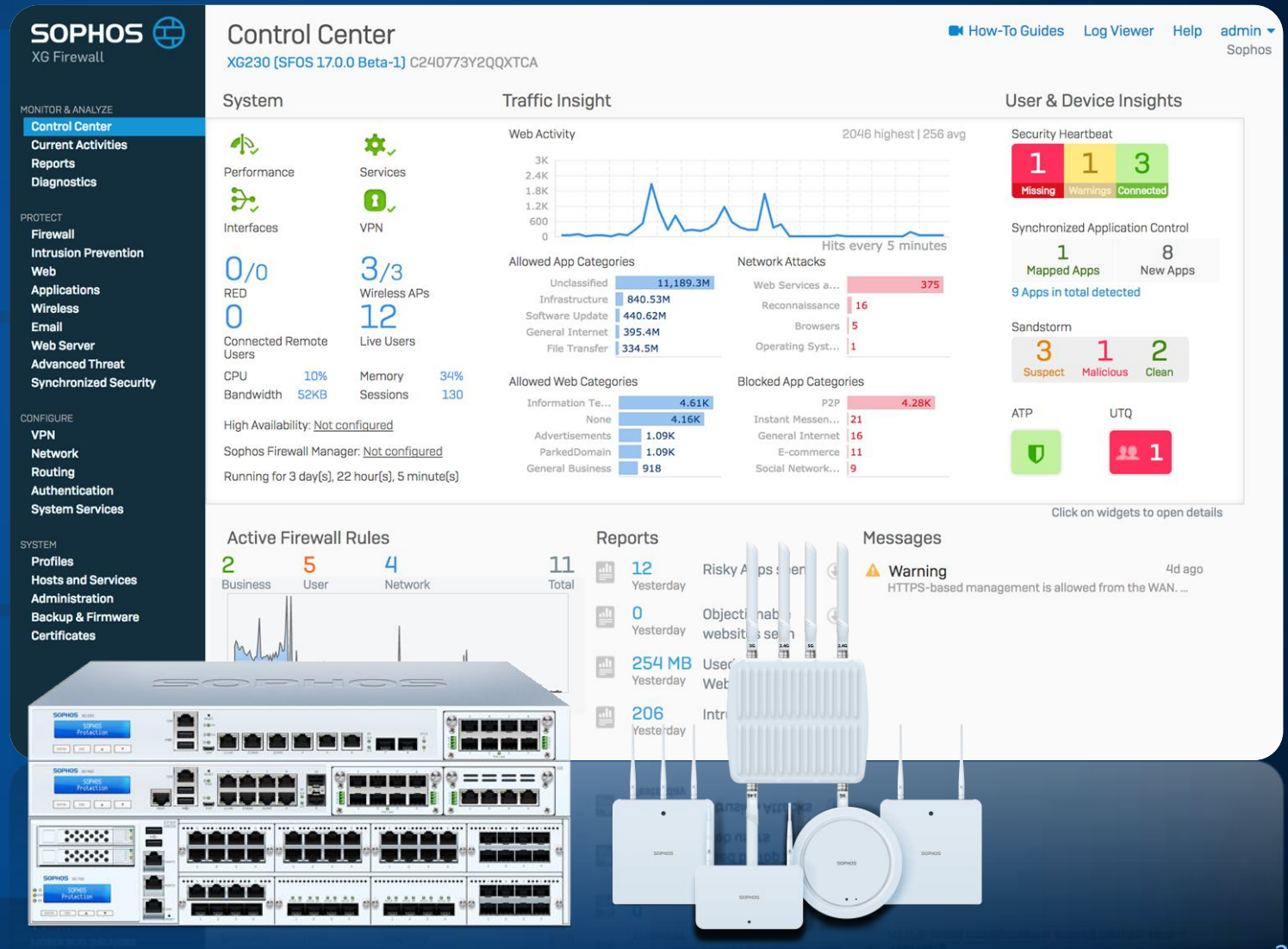
- ✓ Celá sada ochran – vše jednoduše
- ✓ Vysocevýkonný IPS Engine
- ✓ Sandboxing s Deep Learning

2. Vyzdvihuje skrytá rizika

- ✓ Přehledný dashboard & bohaté reportování
- ✓ Identifikace rizikových uživatelů (UTQ)
- ✓ Identifikace neznámých aplikací (Sync App Control)

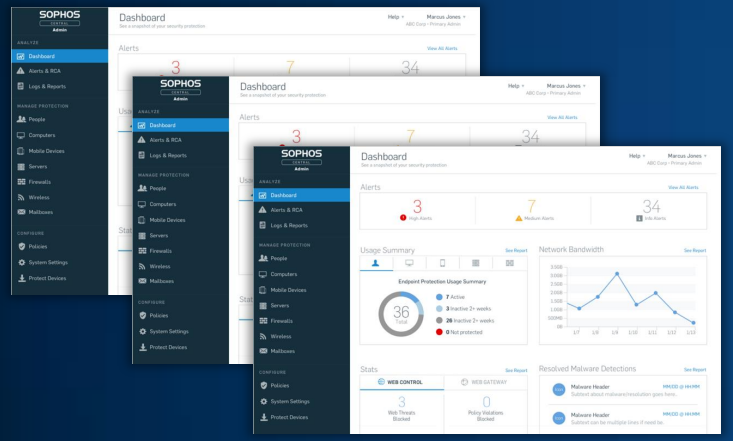
3. Automatická odezva na incident

- ✓ Unikátní Security Heartbeat™
- ✓ Integruje zdraví endpointu do pravidel
- ✓ Automatická izolace infikovaných systémů



Sophos Central - Správa

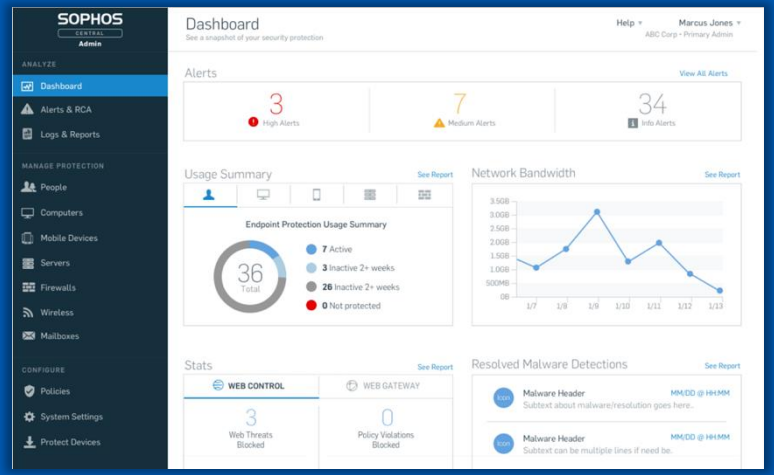
Enterprise Dashboard



Správa násobných škol / institucí / organizací

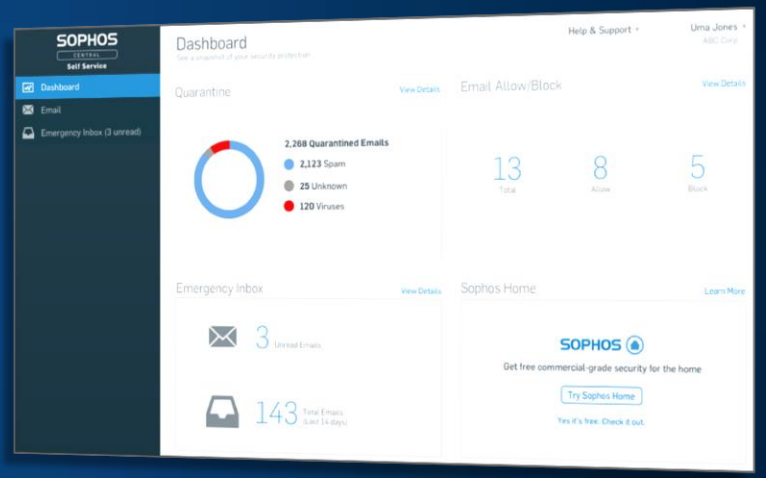
- Licence
- Administrátoři
- Bezpečnostní události
- Politiky

Admin



- Endpoint
- Mobile
- Server
- Encryption
- Wireless
- Phish Threat
- Email Security
- Firewall

Samoobslužný portál



Přístup koncového uživatele

- Emailová karanténa
- Pohotovostní Inbox
- Obnova šifrování
- BYOD mobilní zařízení

SOPHOS

Sophos Endpoint Protection

	Central Endpoint Protection	Intercept X	Intercept X Advanced	Intercept X Advanced with EDR
AV Signatures / HIPS / Live Protection	✓	3rd Party Endpoint Protection	✓	✓
Device / Web / App Control	✓		✓	✓
Data Loss Protection (DLP)	✓		✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓	✓
Security Heartbeat	✓	✓	✓	✓
Deep Learning		✓	✓	✓
CryptoGuard		✓	✓	✓
WipeGuard		✓	✓	✓
Anti-Hacker-Technologies (CredGuard etc.)		✓	✓	✓
Exploit Protection		✓	✓	✓
Root Cause Analysis		✓	✓	✓
Automatic / manual Client-Isolation	✓/-	✓/-	✓/-	✓/✓
SophosLabs Malware-Analysis				✓
Cross Estate Threat Searching				✓

Licence (per Server)

	Central Server Protection	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR
AV Signatures / HIPS / Live Protection	✓	✓	✓
Automatic Scan Exclusions	✓	✓	✓
Cloud Workload Discovery	✓	✓	✓
Device Control	✓	✓	✓
Web Control	✓	✓	✓
Application Control	✓	✓	✓
Data Loss Protection (DLP)	✓	✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓
Synchronized Security Heartbeat	✓	✓	✓
Server Lockdown		✓	✓
CryptoGuard (Anti-Ransomware)		✓	✓
WipeGuard (Master Boot Record protection)		✓	✓
Active Adversary Mitigation (CredGuard etc.)		✓	✓
Exploit Prevention		✓	✓
Root Cause Analysis		✓	✓
Deep Learning		✓	✓
Cross Estate Threat Search			✓
Deep Learning Malware Analysis			✓
Advanced On-Demand SophosLabs Threat Intelligence			✓
Forensic Data Export			✓
On-demand Endpoint Isolation			✓
Single-click „Clean and Block“			✓

SOPHOS

Demo

SOPHOS


Recycle Bin
Dokumente
Acrobat Reader DC
Secrets
Google Chrome
Microsoft Word
Microsoft Outlook
prog
INTERCEPT
ENG
3:46 PM
3/3/2017

SOPHOS

Security made simple.