

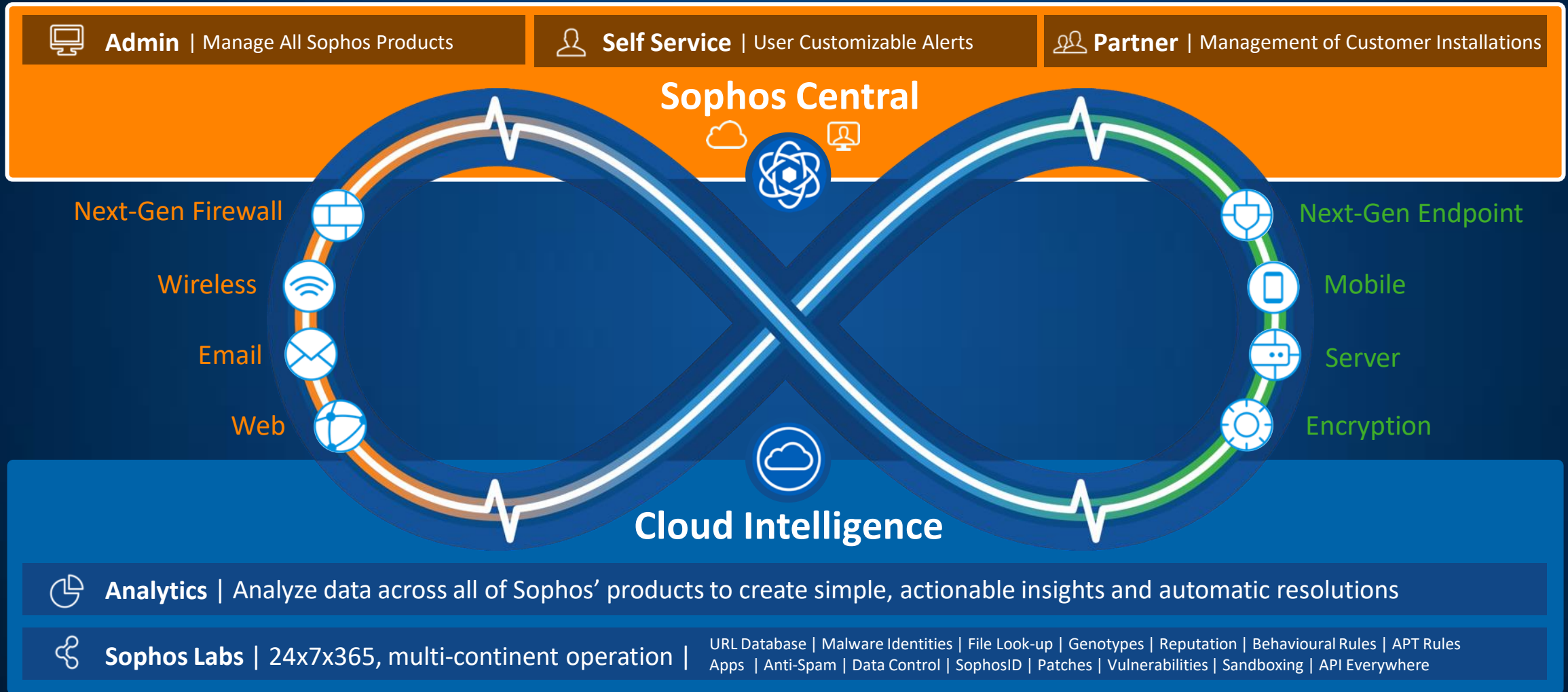
# Sophos Synchronized Security

## Bezpečnost jako systém

Michal Hebeda  
Sales Engineer

**SOPHOS**

# Platforma Synchronized Security a Strategie

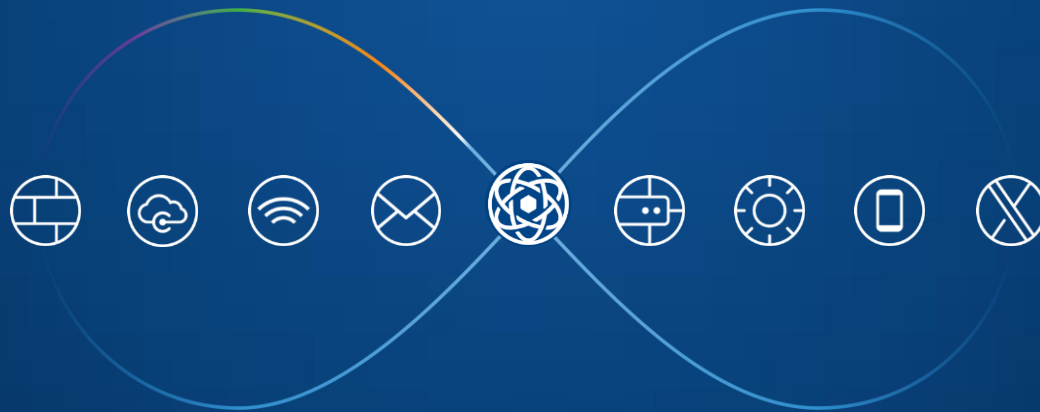


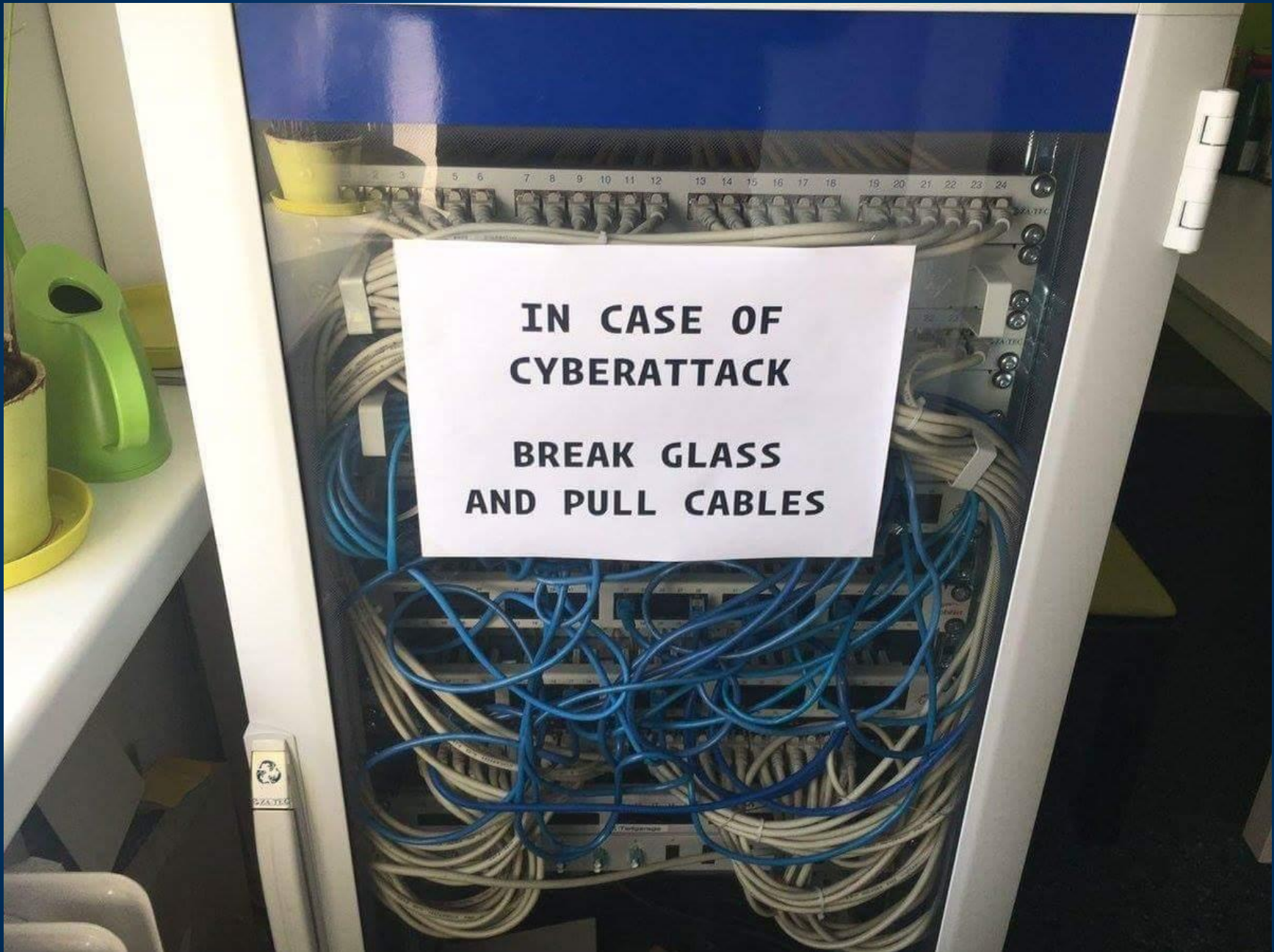
# Synchronized Security - Koncept



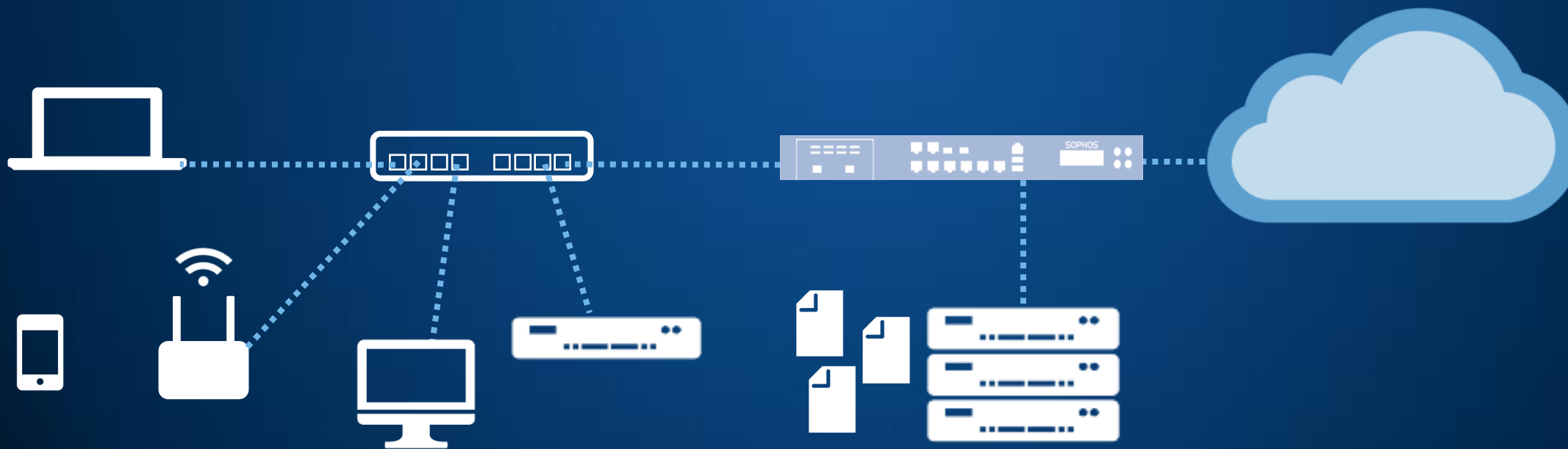
- Bezpečnostní komponenty jednají jako **system**
- Výměna informací mezi komponentami
  - **Bezpečnostní stav** zařízení
  - **Přenosy aplikací**
  - **Kontext uživatele**
- Cíle
  - Zlepšení **detekce** hrozeb a aktivit hackerů
  - Automatická **izolace** hrozeb
  - **Ochrana** kritických dat
  - Lepší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

# Proč potřebujeme Synchronized Security?

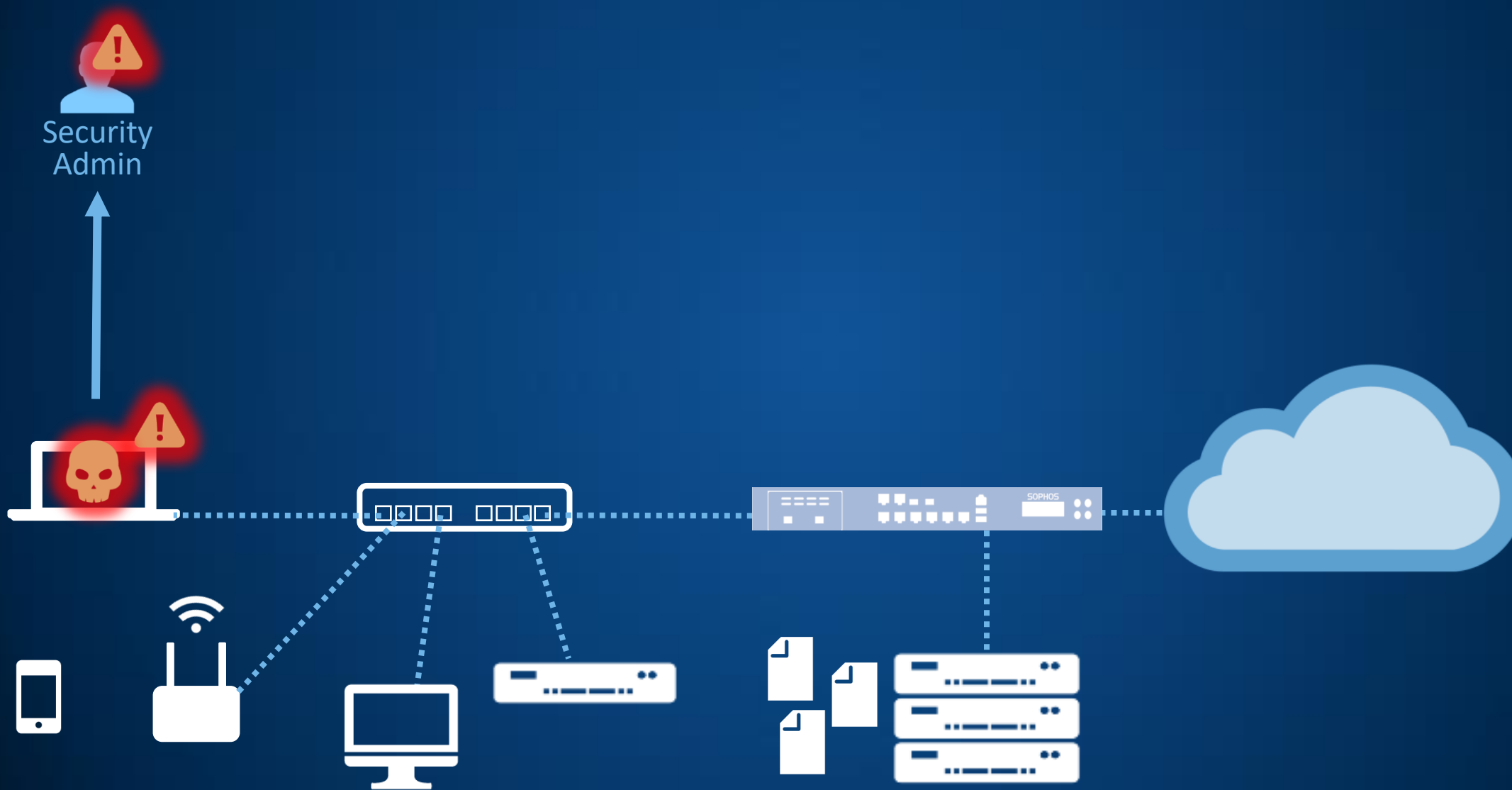




# Zpracování hrozeb **bez** Synchronized Security



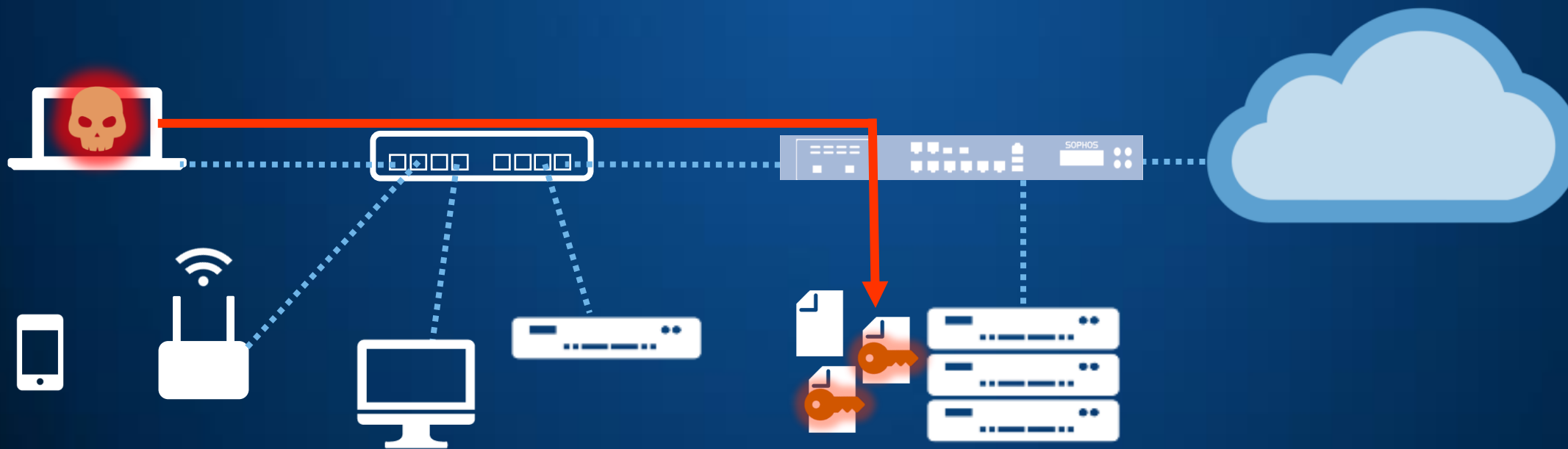
# Hrozba je rozpoznána



# .. a analyzována



Soubory jsou zašifrovány  
na souborovém serveru

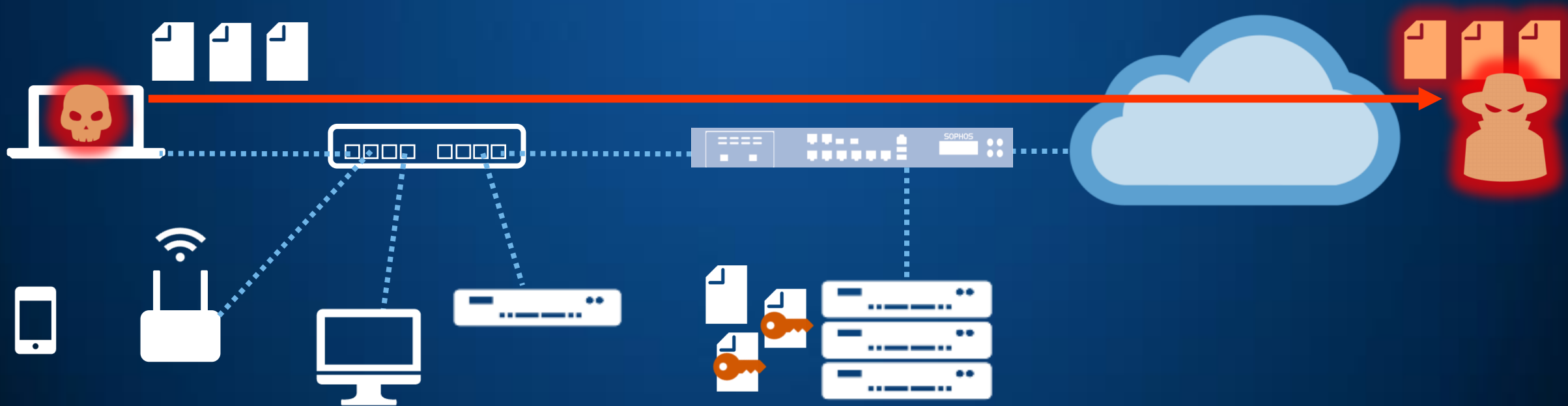




# .. a analyzována



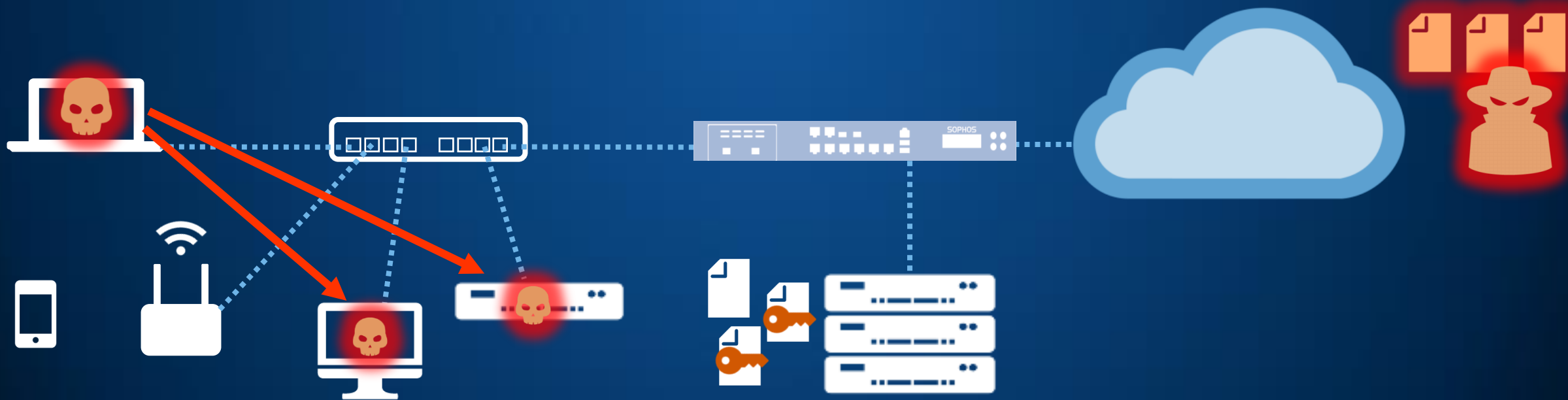
..a citlivá data odeslána  
útočníkovi v internetu



# .. a analyzována

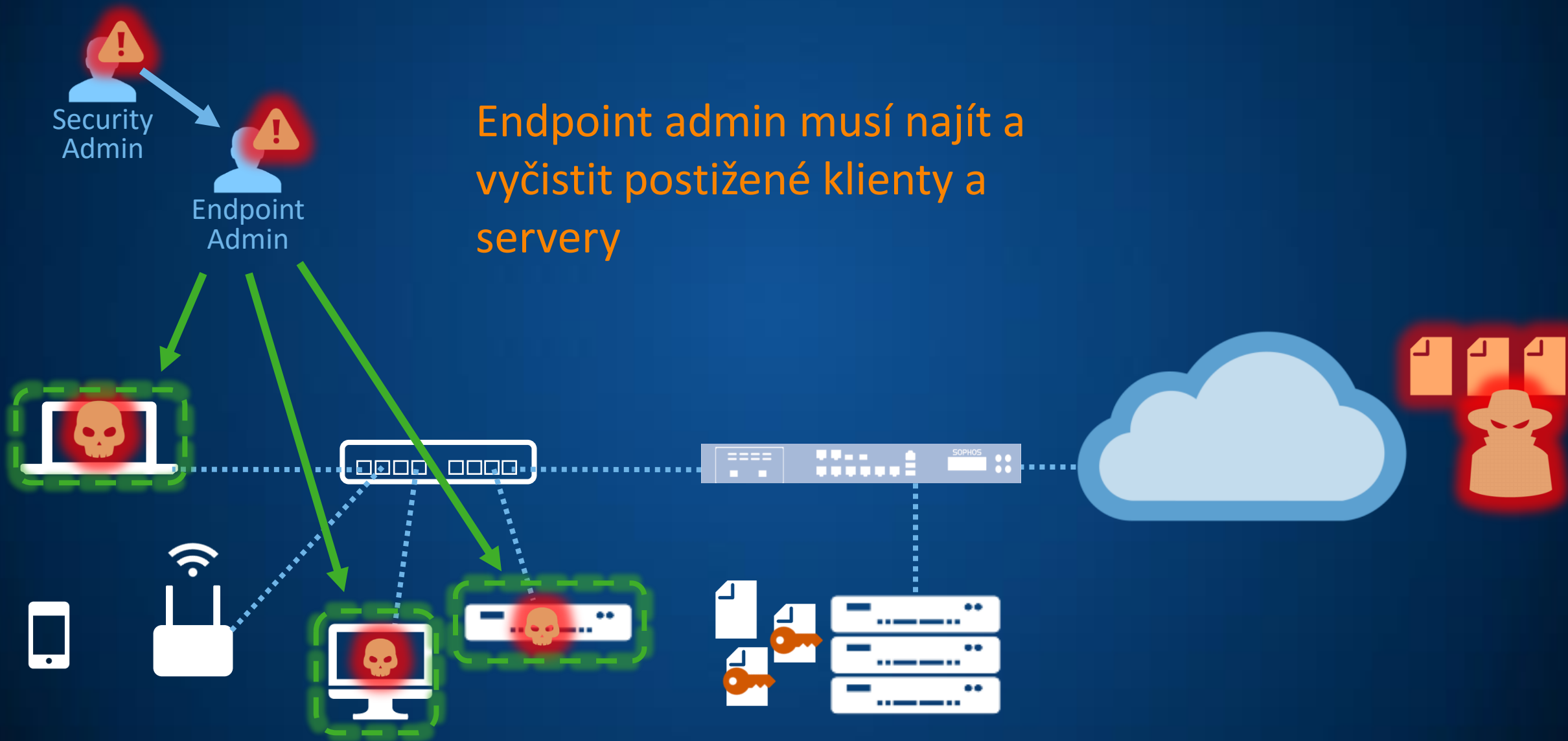


.. navíc i ostatní endpointy  
a servery jsou infikovány

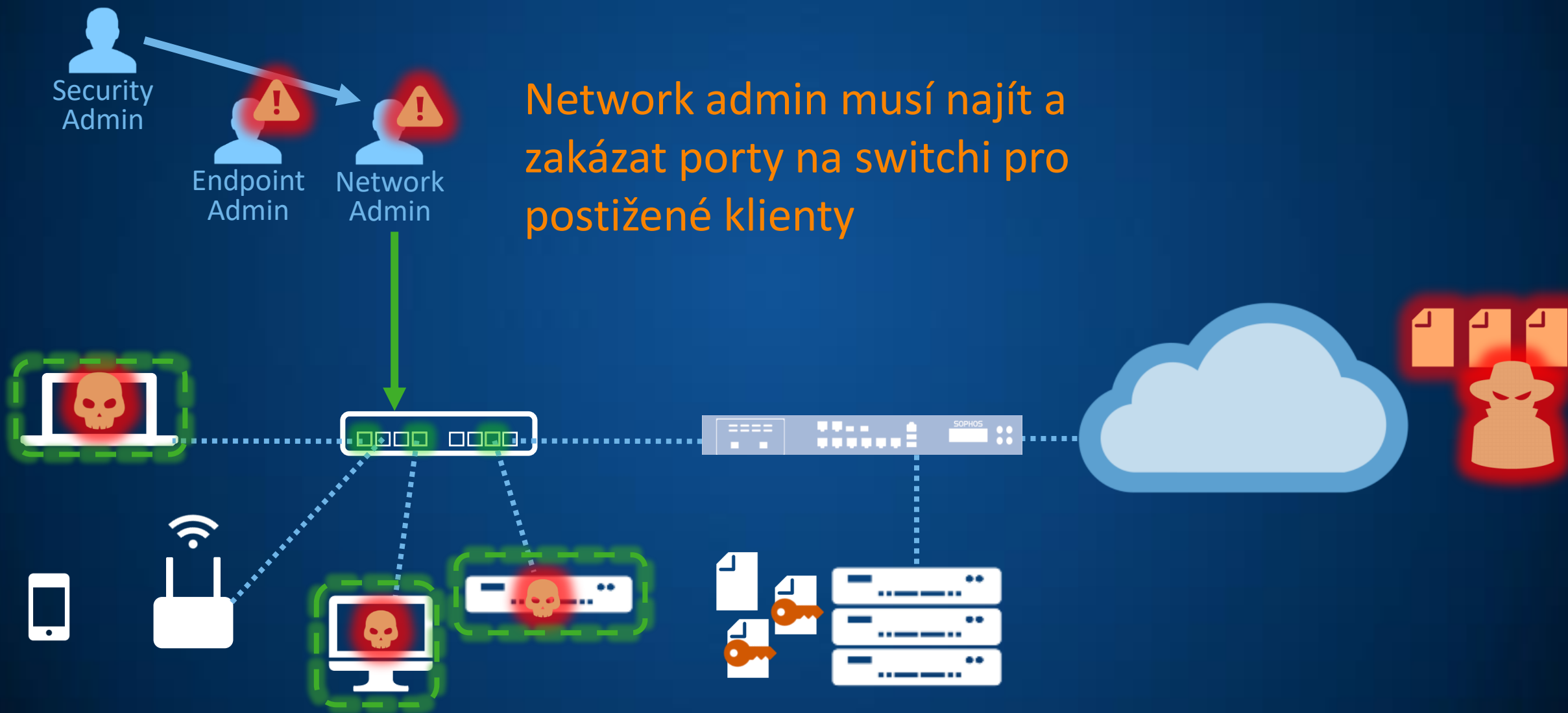


# Akce!!!

Endpoint admin musí najít a vyčistit postižené klienty a servery



# Akce!!!

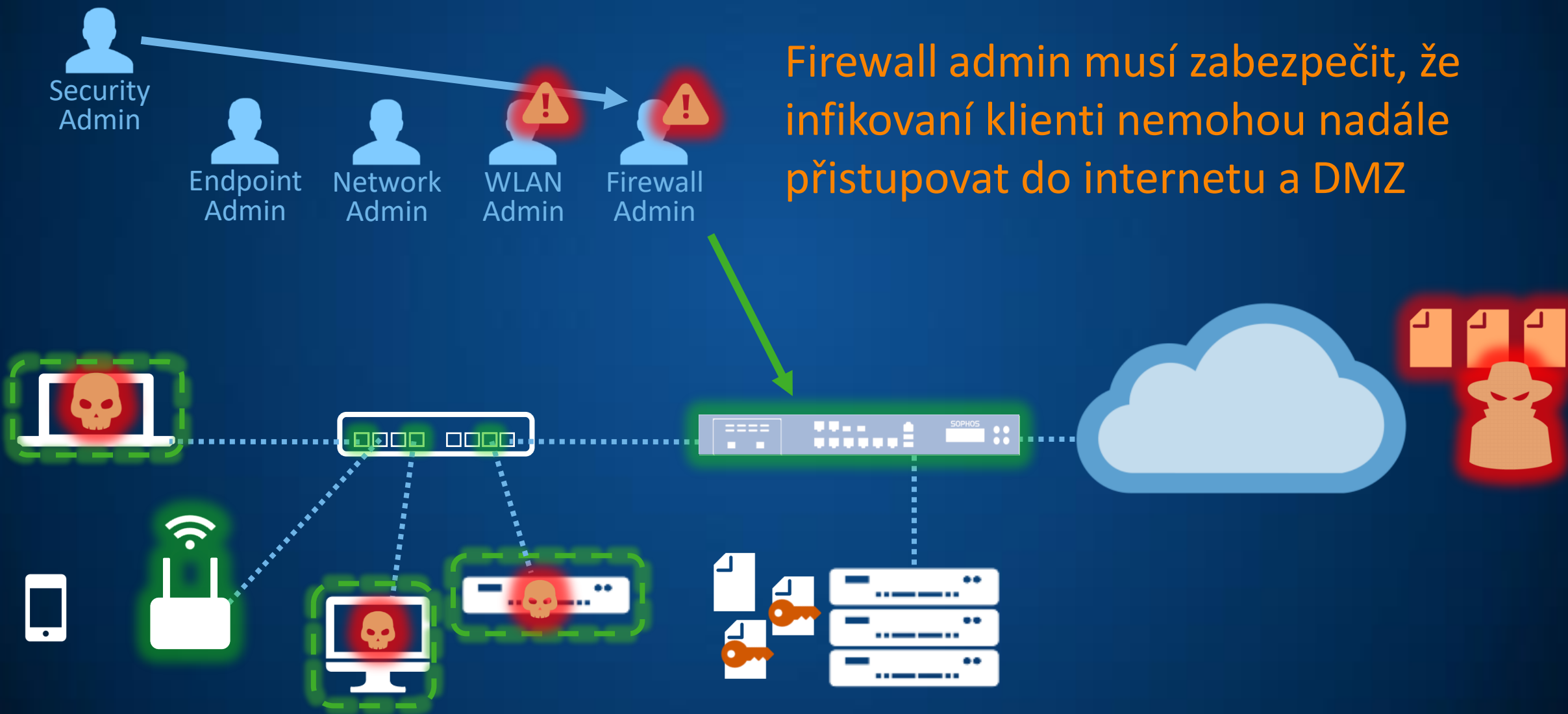


# Akce!!!



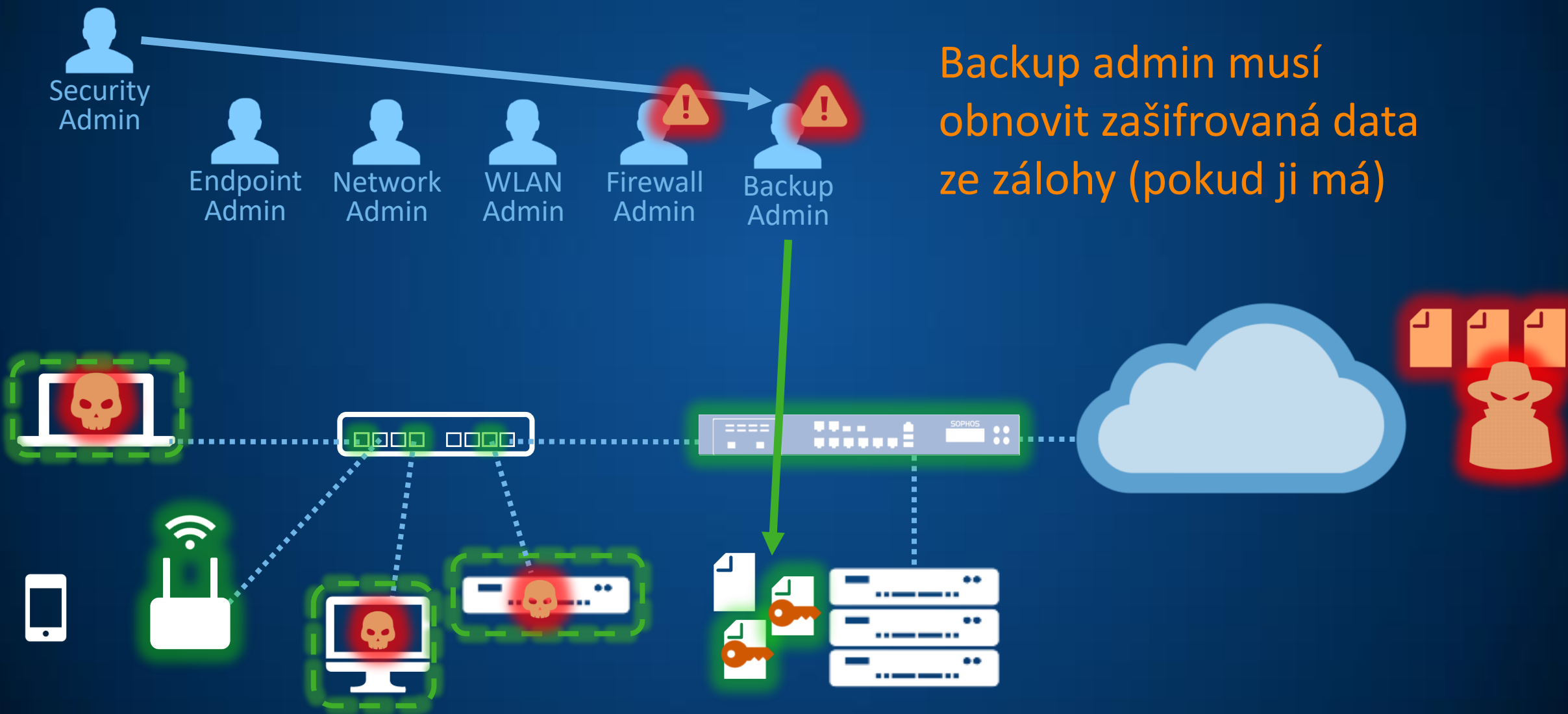
Wi-Fi Admin musí zajistit, že infikovaní klienti se nemohou připojovat do Wi-Fi sítě

# Akce!!!

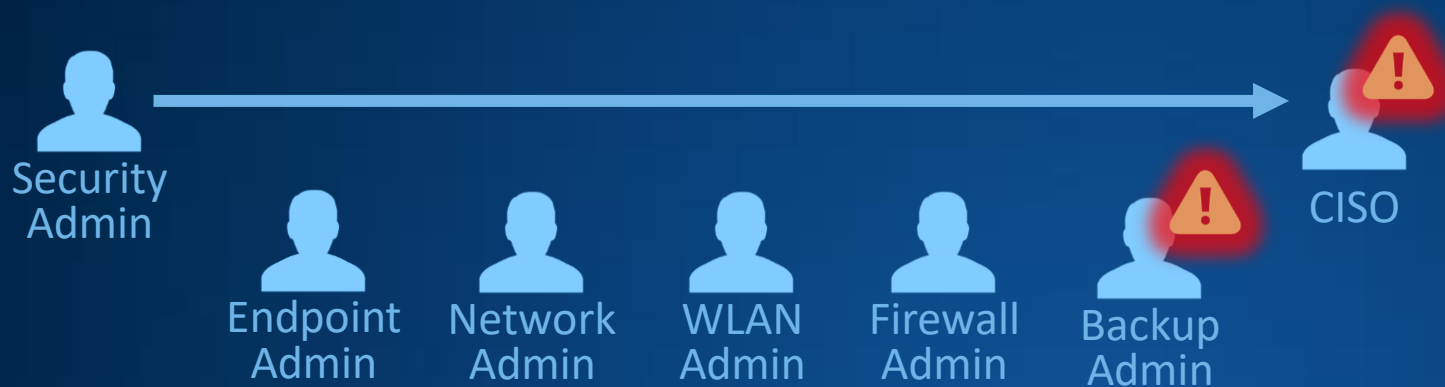


Firewall admin musí zabezpečit, že infikovaní klienti nemohou nadále přistupovat do internetu a DMZ

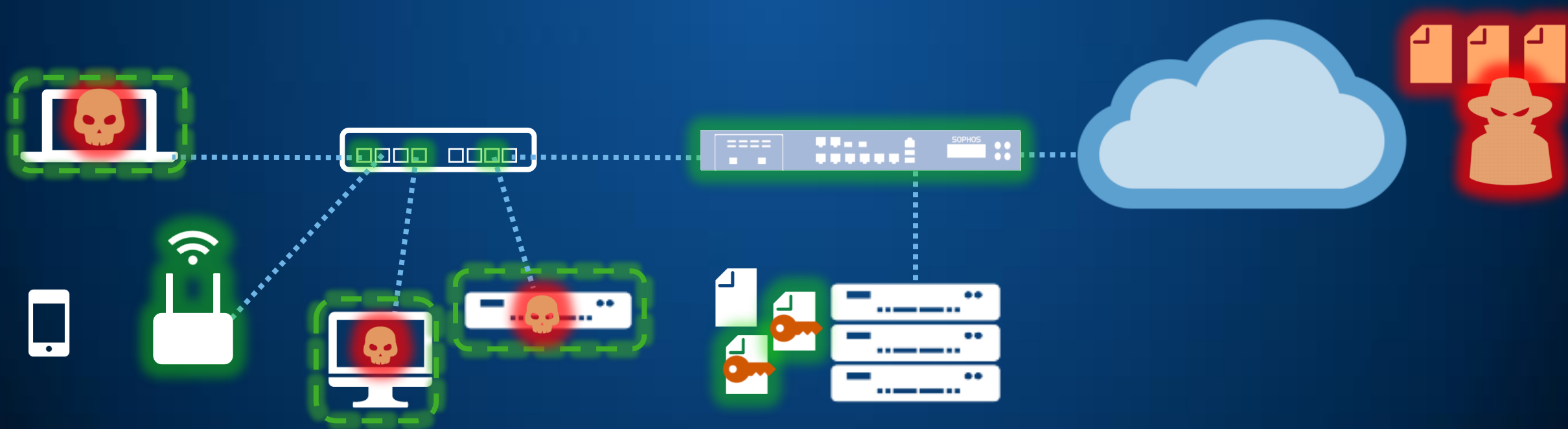
# Akce!!!



# 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

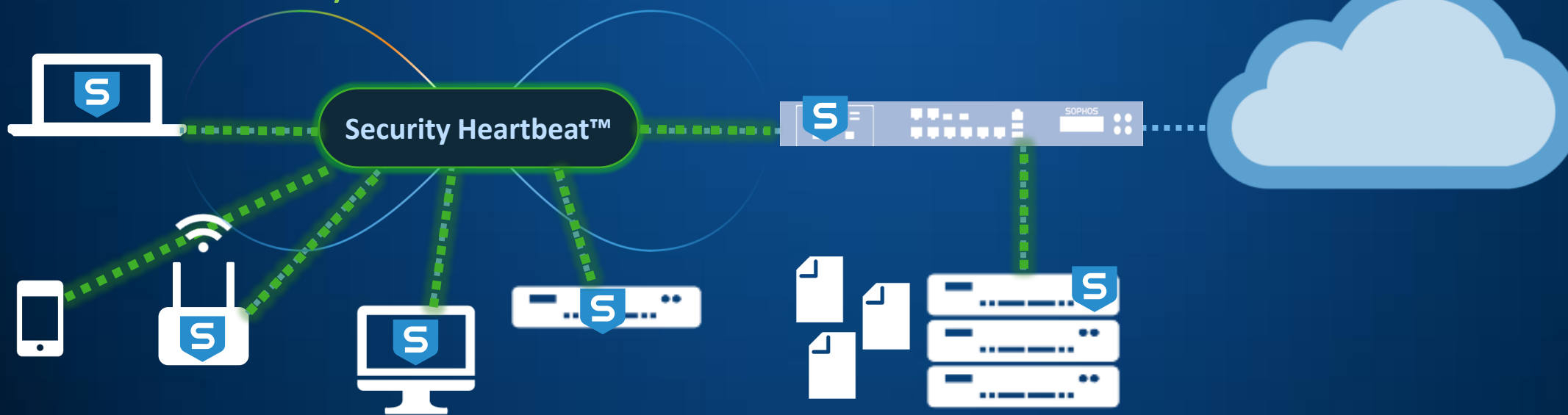
## Synchronized Security



**SOPHOS**

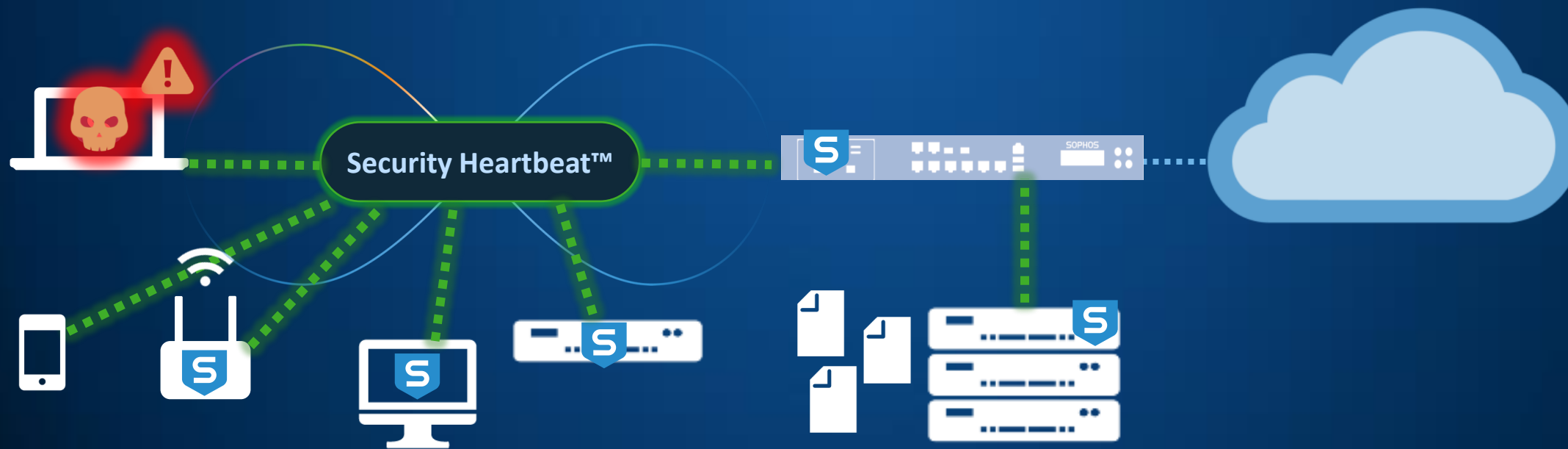
# Zpracování hrozeb **se** Synchronized Security

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



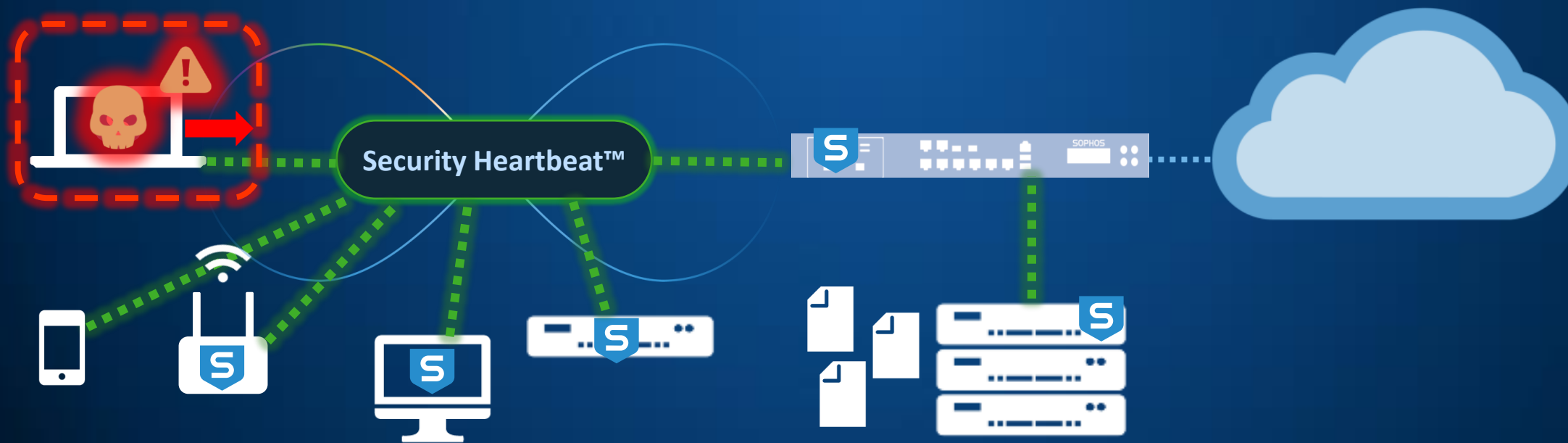
# Zpracování hrozeb **se** Synchronized Security

V případě hrozby jsou všechny komponenty informovány a reagují automaticky



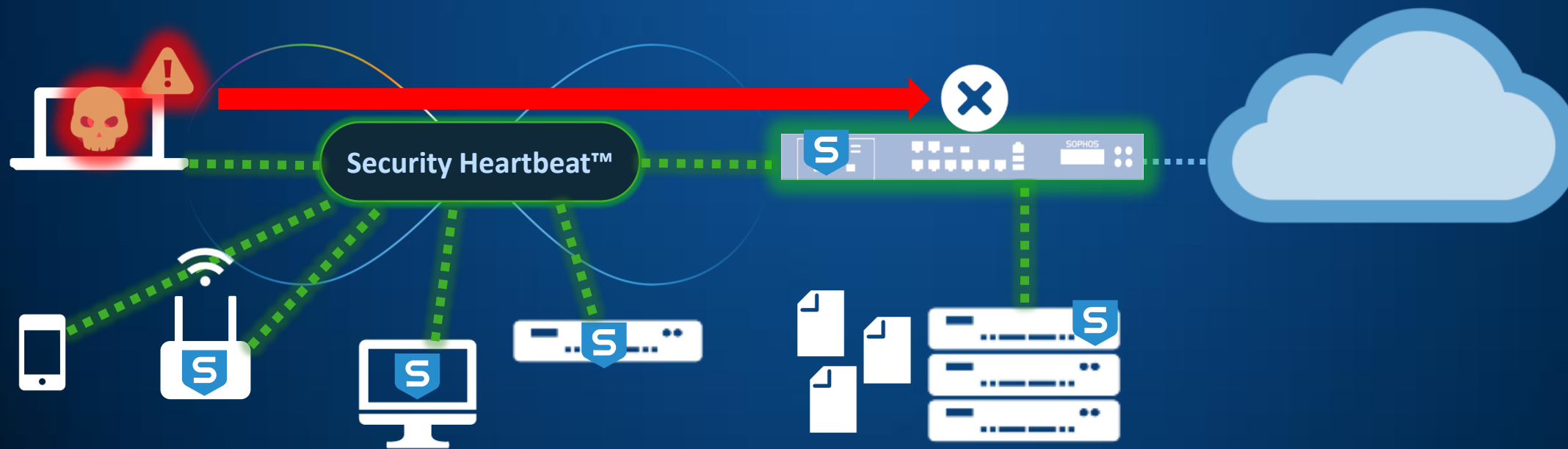
# Zpracování hrozeb **se** Synchronized Security

Klient izoluje sám sebe ...



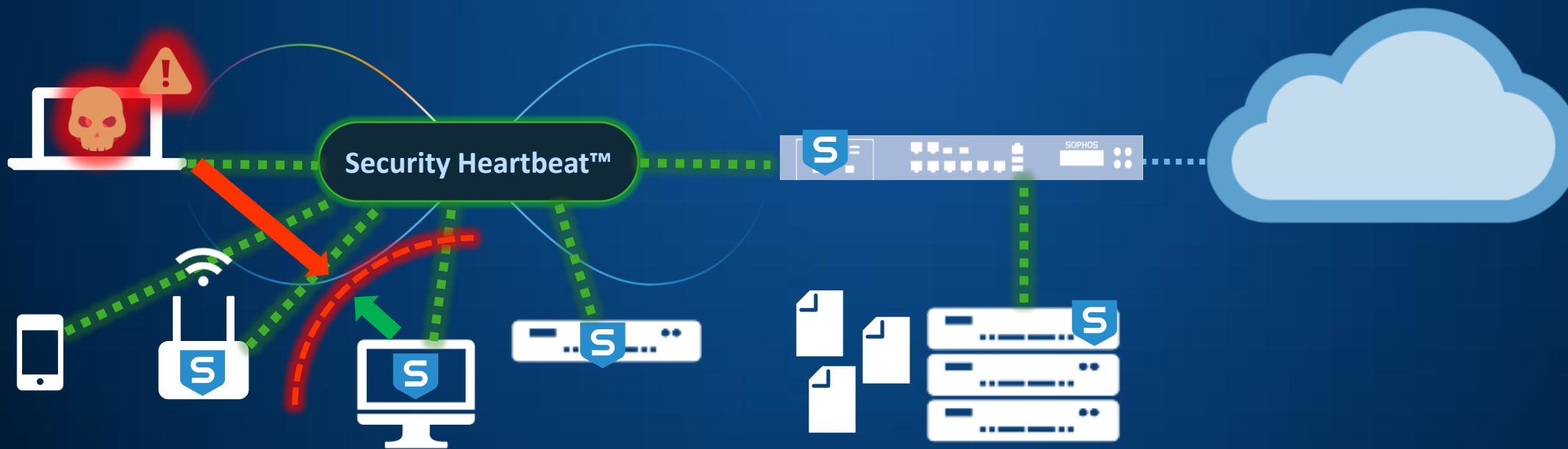
# Zpracování hrozeb **se** Synchronized Security

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



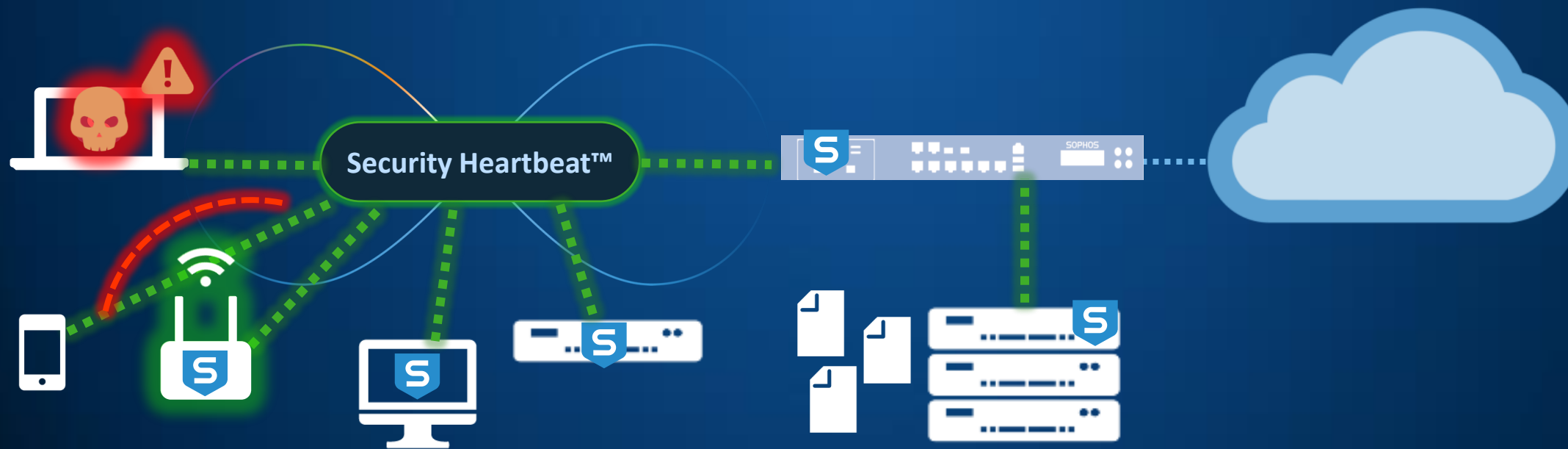
# Zpracování hrozeb **se** Synchronized Security

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



# Zpracování hrozeb **se** Synchronized Security

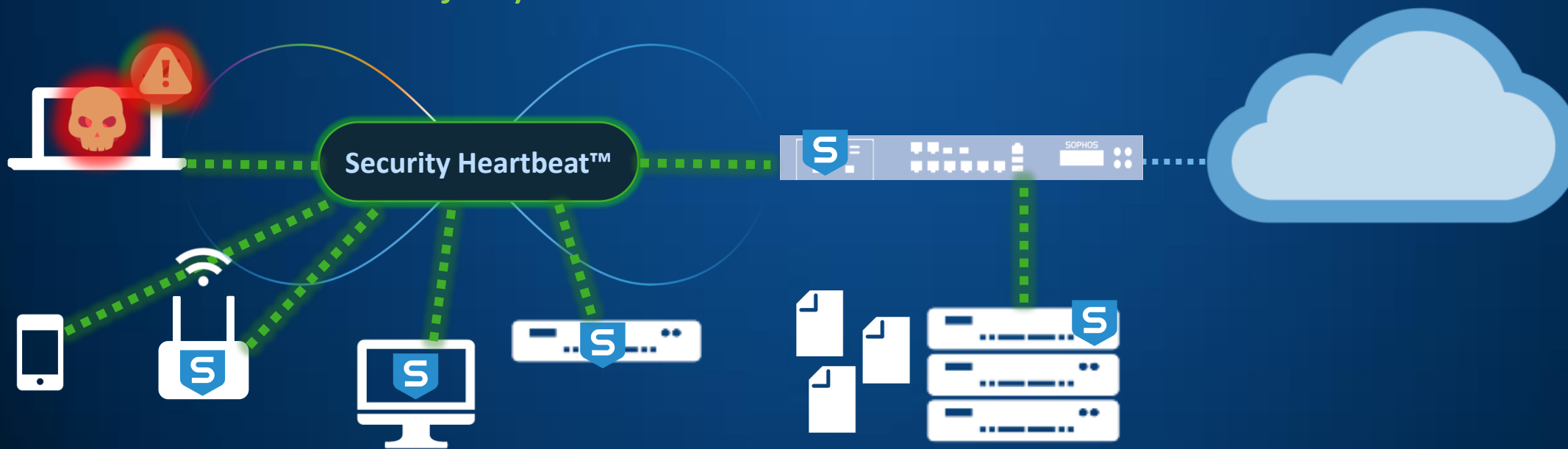
WiFi přístupové body nedovolí  
infikovaným klientům přístup do  
interní LAN sítě





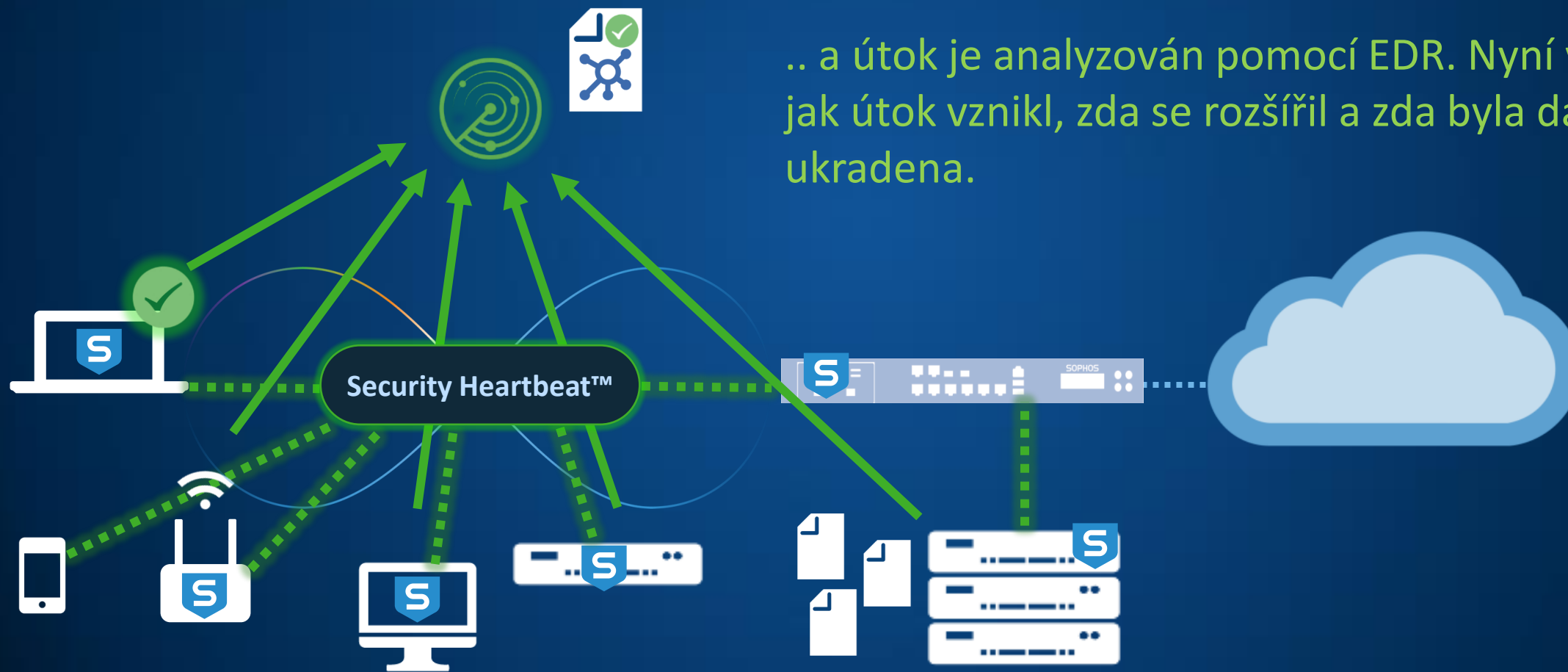
# Zpracování hrozeb **se** Synchronized Security

..a hrozba je vyřešena..



# Zpracování hrozeb **se** Synchronized Security

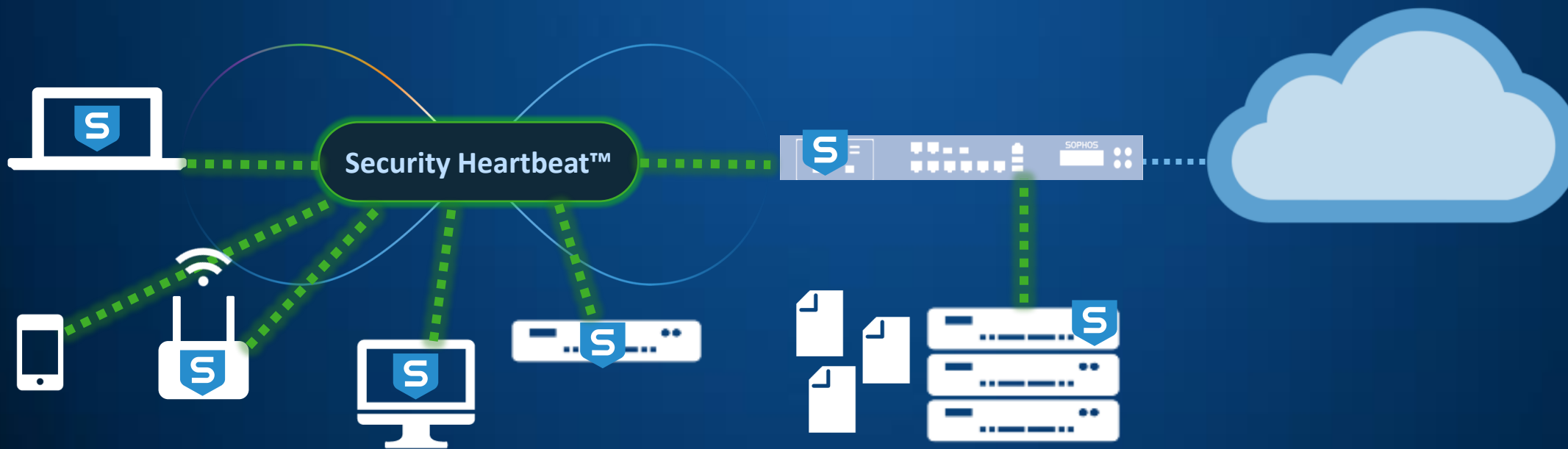
.. a útok je analyzován pomocí EDR. Nyní víme, jak útok vznikl, zda se rozšířil a zda byla data ukradena.



# Zpracování hrozeb **se** Synchronized Security



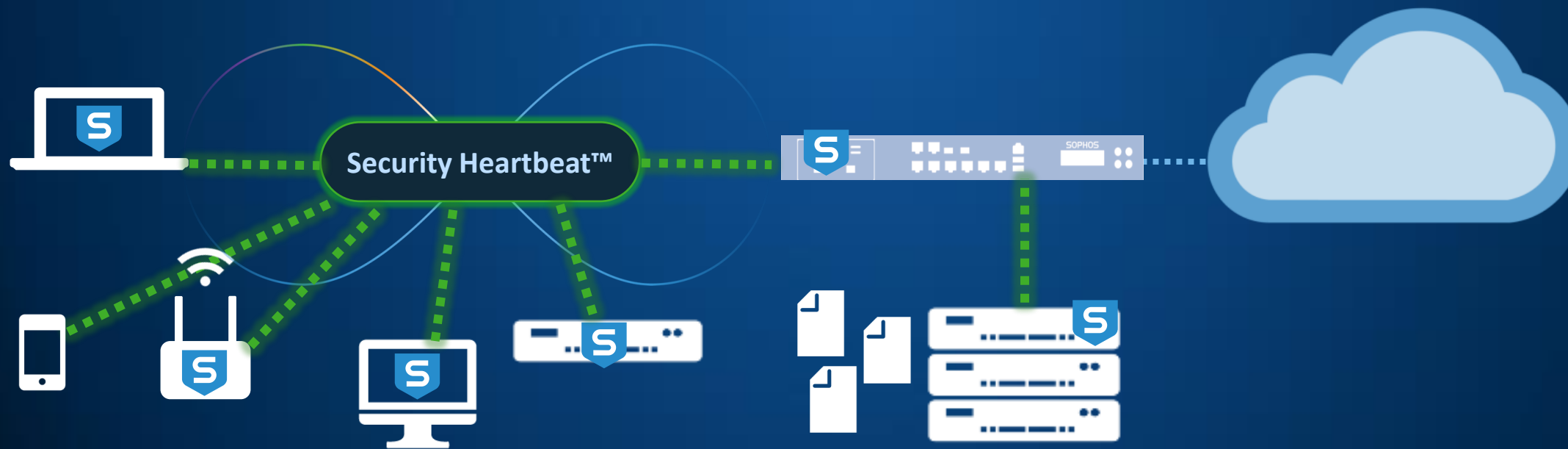
..admin vidí, že vše bylo automaticky zabezpečeno a žádná data nebyla ukradena ..



# Zpracování hrozeb **se** Synchronized Security

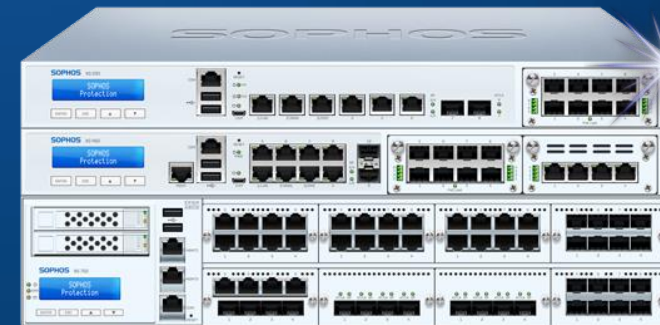
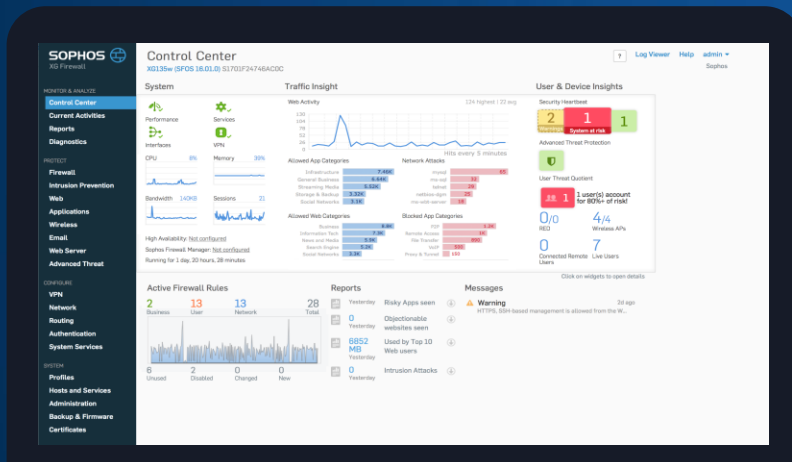


..a šéf je spokojen, že IT bezpečnost funguje.



# Sophos XG

## Firewall



SOPHOS

# Filozofie designu XG Firewallu

## Zlepšený přehled

### Filozofie designu XG Firewallu

- Připraveno pro běžného IT manažera 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 informacemi na prokliknutí

Zajišťuje adminům jednotný přehled všeho, co je důležité

**SOPHOS**  
XG Firewall

### Control Center

XG135w (SFOS 16.01.0) S1701F24746AC0C

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

SYSTEM

- Profiles
- Hosts and Services
- Administration
- Backup & Firmware
- Certificates

#### System

Performance Services  
Interfaces VPN

CPU 8% Memory 39%

Bandwidth 140KB Sessions 21

High Availability: Not configured  
Sophos Firewall Manager: Not configured  
Running for 1 day, 20 hours, 28 minutes

#### Traffic Insight

Web Activity 124 highest | 22 avg

Allowed App Categories

Infrastructure	7.46K
General Business	6.64K
Streaming Media	5.52K
Storage & Backup	3.32K
Social Networks	3.1K

Network Attacks Hits every 5 minutes

mysql	65
ms-sql	32
telnet	29
netbios-dgm	25
ms-wbt-server	18

Allowed Web Categories

Business	8.8K
Information Tech	7.3K
News and Media	5.9K
Search Engine	5.2K
Social Networks	3.3K

Blocked App Categories

P2P	1.2K
Remote Access	1K
File Transfer	890
VoIP	500
Proxy & Tunnel	150

#### User & Device Insights

Security Heartbeat

Warnings 2 System at risk 1

Sandstorm

Suspect 17 Malicious 4 Clean 6

ATP 1 UTQ 1

RED 0/0 Wireless APs 4/4

Connected Remote Users 0 Live Users 7

Click on widgets to open details

#### Active Firewall Rules

2 Business 13 User 13 Network 28 Total

6 Unused 2 Disabled 0 Changed 0 New

#### Reports

Yesterday Risky Apps seen

Yesterday Objectionable websites seen

Yesterday 6852 MB Used by Top 10 Web users

Yesterday 0 Intrusion Attacks

#### Messages

Warning 2d ago  
HTTPS, SSH-based management is allowed from the W...

# 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** XG Firewall

### Control Center

XG230 (SFOS 17.0.0 Beta-1) C240773Y2QQXTCA

How-To Guides Log Viewer Help admin Sophos

#### MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

#### PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat
- Synchronized Security

#### CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

#### SYSTEM

- Profiles
- Hosts and Services
- Administration
- Backup & Firmware
- Certificates

#### System

Performance: 0/0 RED  
Interfaces: 0  
Connected Remote Users: 0

Services: 3/3  
Wireless APs: 12  
Live Users: 130

CPU: 10%  
Bandwidth: 52KB

Memory: 34%  
Sessions: 130

High Availability: **Not configured**  
Sophos Firewall Manager: **Not configured**  
Running for 3 day(s), 22 hour(s), 5 minute(s)

#### Traffic Insight

##### Web Activity

2046 highest | 256 avg

Hits every 5 minutes

##### Allowed App Categories

Unclassified	11,189.3M
Infrastructure	840.53M
Software Update	440.62M
General Internet	395.4M
File Transfer	334.5M

##### Network Attacks

Web Services a...	375
Reconnaissance	16
Browsers	5
Operating Syst...	1

##### Allowed Web Categories

Information Te...	4.61K
None	4.16K
Advertisements	1.09K
ParkedDomain	1.09K
General Business	918

##### Blocked App Categories

P2P	4.28K
Instant Messen...	21
General Internet	16
E-commerce	11
Social Network...	9

#### User & Device Insights

##### Security Heartbeat

1 Missing	1 Warnings	3 Connected
-----------	------------	-------------

##### Synchronized Application Control

1 Mapped Apps	8 New Apps
---------------	------------

9 Apps in total detected

##### Sandstorm

3 Suspect	1 Malicious	2 Clean
-----------	-------------	---------

##### ATP

1
---

##### UTQ

1
---

Click on widgets to open details

#### Active Firewall Rules

2 Business	5 User	4 Network	11 Total
------------	--------	-----------	----------

#### Reports

12	Risky Apps seen
0	Object hab...
254 MB	User Web
206	Intr...

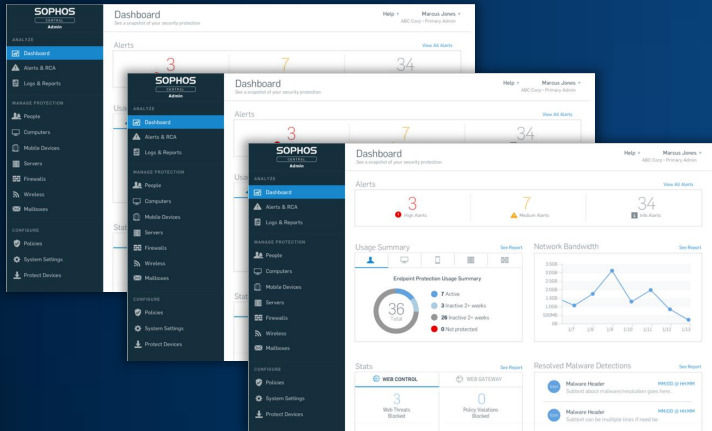
#### Messages

Warning: HTTPS-based management is allowed from the WAN...

# Sophos Central - Správa



## Enterprise Dashboard

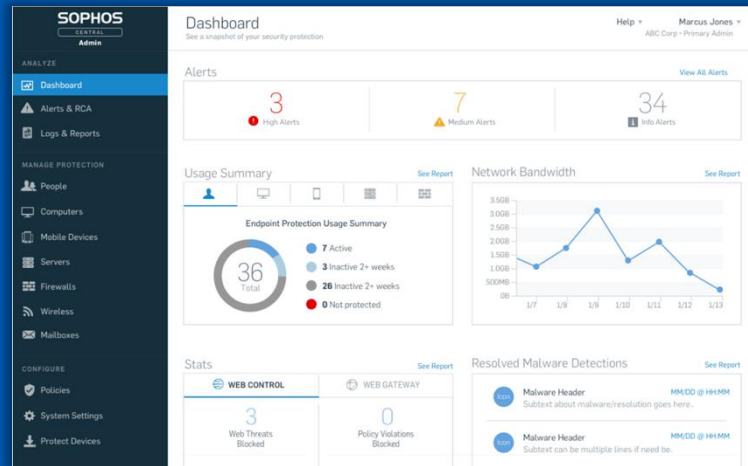


Správa násobných škol / institucí / organizací

- Licence
- Administrátoři
- Bezpečnostní události
- Politiky

SOPHOS

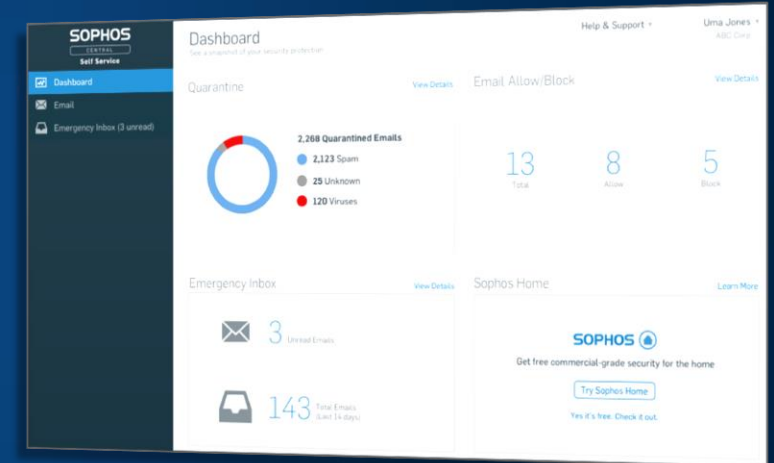
## Admin



- Endpoint
- Mobile
- Server
- Encryption

- Wireless
- Phish Threat
- Email Security
- Firewall

## Samooobslužný portál






Přístup koncového uživatele

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



# Sophos Endpoint Protection

	CENTRAL ENDPOINT PROTECTION		 Advanced	 Advanced with EDR
AV Signatures / HIPS / Live Protection	✓	3 <sup>rd</sup> 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“			✓

**Demo**

**SOPHOS**



Recycle Bin



Dokumente



Acrobat Reader DC



Secrets



Google Chrome



Microsoft Word



Microsoft Outlook



prog

# INTERCEPT



**SOPHOS**  
Security made simple.