BEZPEČNOSŤ NIELEN ZDRAVOTNÍCKYCH ZARIADENÍ VO VAŠEJ SIETI

Ján Benka, Tomáš Ondruš

SOITRON

ARMIS

ZRANITEĽNOSTI

Nezaplátané a zastaralé zdravotnícke zariadenia tvoria príležitosti pre kybernetické útoky

53%	Zariadenia:	63%
Pripojených medicínskych zariadení obsahuje kritické zraniteľnosti	Inzulínové pumpy, implant. defibrilátory, kardio-telemetrie, kardiostimulátory …	Zdravotníckych organizácií v USA čelilo útoku zahŕňajúcemu nemanažované a IoT zariadenia

Zdroj: FBI Private Industry Notification September 2022: https://www.ic3.gov/Media/News/2022/220912.pdf
Zdroj: Forrester, 2019: https://www.armis.com/blog/state-of-enterprise-iot-security-in-north-america-unmanaged-and-unsecured/

ÚTOKY

Nárast útokov na nemocnice v strednej Európe v 11/2021 o 145%

Ransomware v Nemocnici Rudolfa a Stefanie Benešov

V nemocnici v Benešově došlo k útoku na konci roku 2019. Kvůli omezení lékařských výkonů, zrušení plánovaných vyšetření, operací, výroby a nákladům na obnovu se škody za necelé tři týdny omezení provozu vyšplhaly na 59 milionů korun.

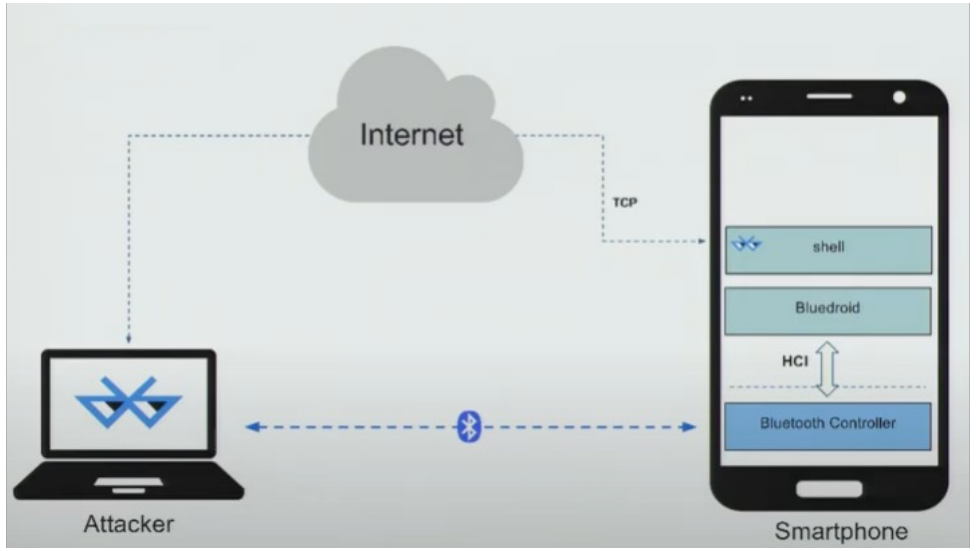
Psychiatrická nemocnice v Kosmonosech

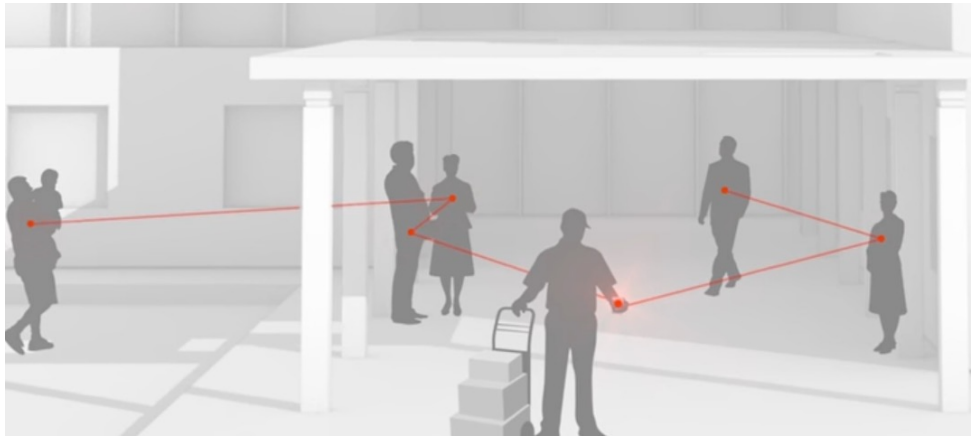
Následoval útok na psychiatrickou nemocnici, který proběhl jen o několik málo dnů později. 27. března došlo k ransomwarovému útoku, který s největší pravděpodobností zneužil slabá, nedostatečně zabezpečená místa na serverech. Útočníci se v takovém případě přihlásí, vypnou v zařízení bezpečnostní řešení a ručně spustí škodlivý kód, jenž

Fakultní nemocnice u sv. Anny v Brně (FNUSA)

Útok oficiálně začal 13. března minulého roku, a tentokrát šlo o cílený útok ransomwaru Defray (Defray777). Útočníci se po úspěšném napadení zařízení pokusili z instituce vymámit výkupné, které jim však neposkytla, naopak se zaměřila na forenzní analýzu útoku společně s NÚKIBem a Avastem, jeho investigaci a co nejrychlejší nápravu. Provoz byl obnoven po čtyřech týdnech.

BlueBorn

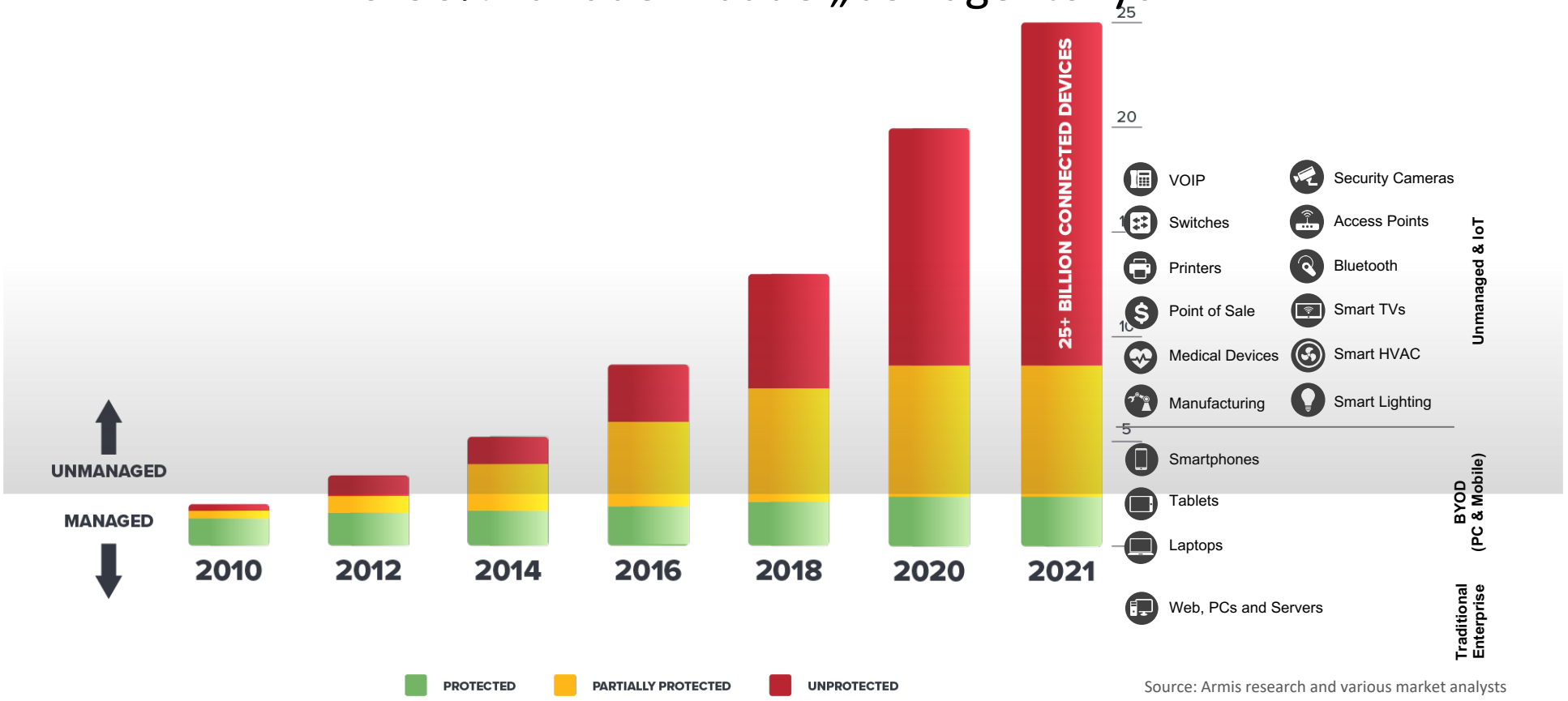




Zdroj: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

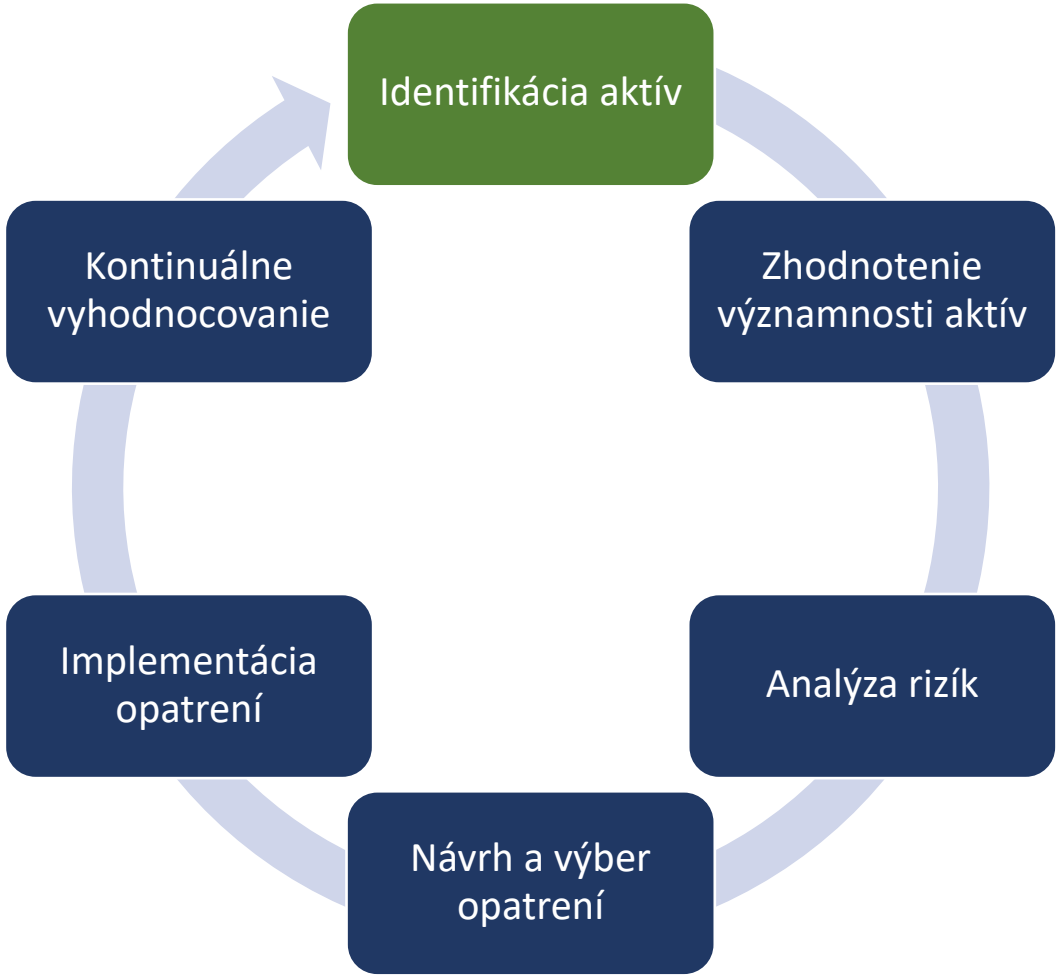
NÁRAST NEMANAŽOVANÝCH ZARIADENÍ

Asi 90% zariadení bude „bez-agentových“



Source: Armis research and various market analysts

ZAVEDENIE PROGRAMU INFORMAČNEJ BEZPEČNOSTI



§ 6 ods. 3 Vyhlášky 362/2018 Z.z.:

Riadenie aktív pozostáva z identifikácie a evidencie všetkých **aktív, od ktorých závisí poskytovanie základnej služby**

Najčastejšie základné služby v zdravotníckom segmente:

- Poskytovanie zdravotnej starostlivosti
- Laboratórne služby

VIDITEĽNOSŤ

WarCraft II: Tides of Darkness

ARMIS

Identifikuje a klasifikuje VŠETKY zariadenia

Riziká, zraniteľnosti, anomálne správania, útoky, politiky …

Incident response / Orchestrácia

pasívne • bez agentov • v reálnom čase • kontinuálne

AdventHealth East Orlando
DocuSign
Booking.com
Stanford HEALTH CARE
McKESSON
PEPSICO
NHS
FRESENIUS MEDICAL CARE
ARMIS
ECOLAB
NVIDIA
ups
Tampa International Airport
institut Curie
Red Bull ENERGY DRINK

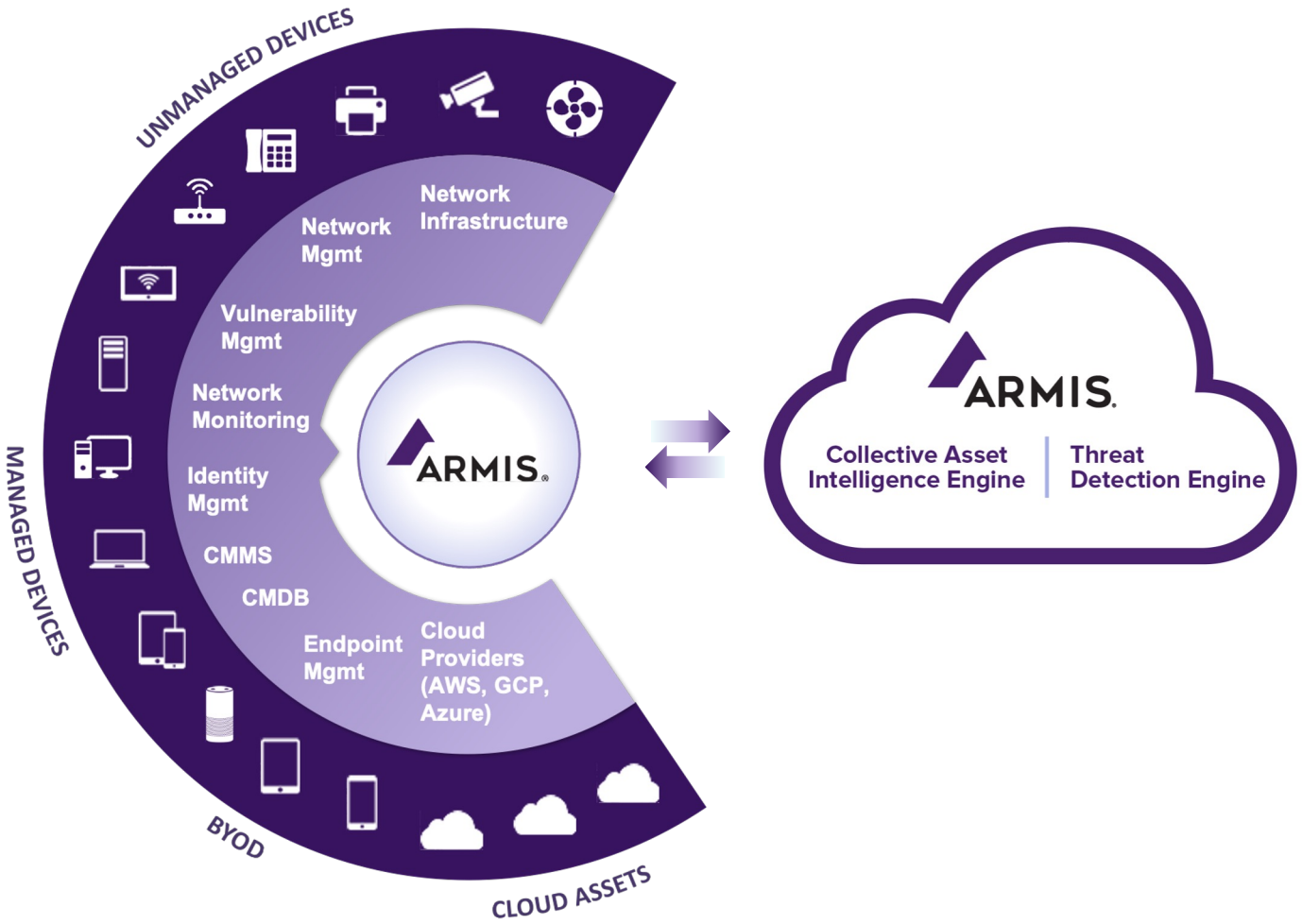
Identifikuje a klasifikuje VŠETKY zariadenia

Riziká, zraniteľnosti, anomálne správania, útoky, politiky …

Incident response / Orchestrácia

pasívne • bez agentov • v reálnom čase • kontinuálne

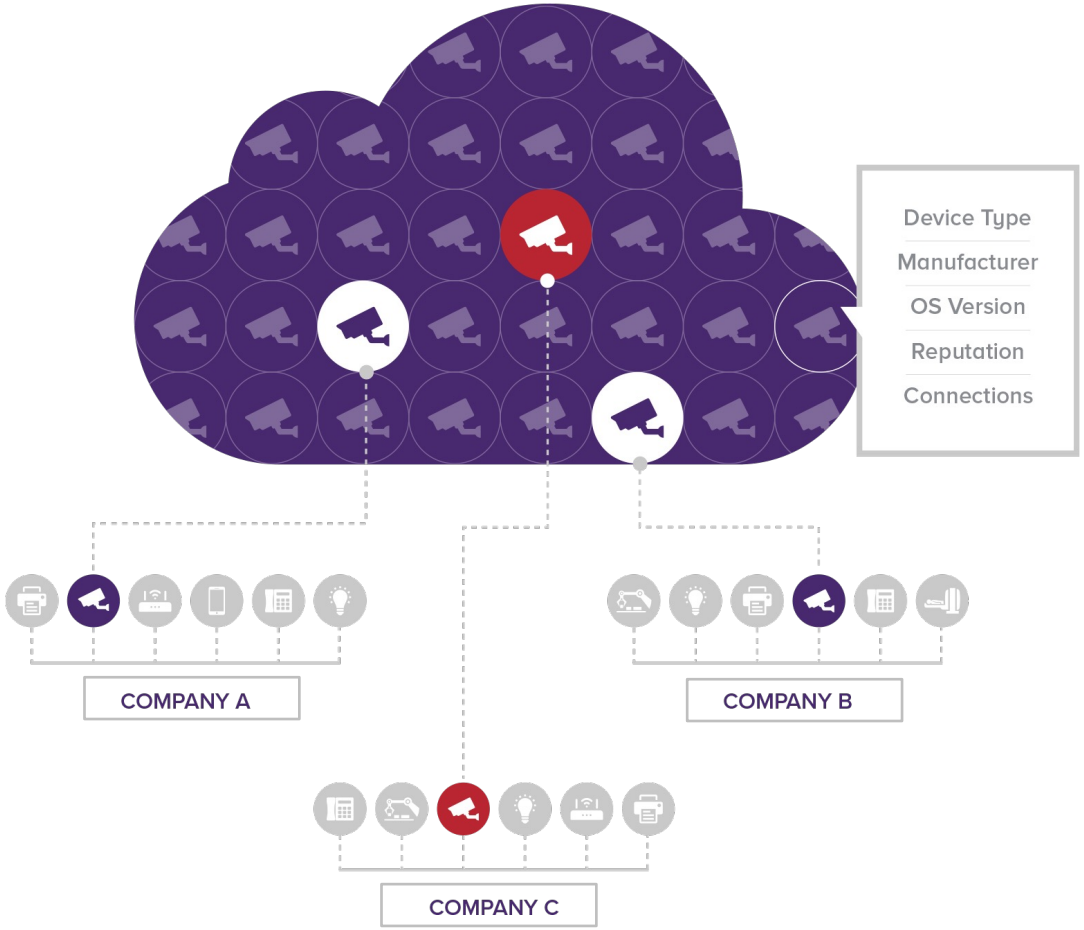
AT&T
extended STAY AMERICA
MassMutual
Charter COMMUNICATIONS
intel
NBA



Rýchle nasadenie

- Bez agentov
- Výsledky do niekoľkých hodín
- Integrácie s existujúcimi IT a security nástrojmi
- Bez vplyvu na sieťovú prevádzku

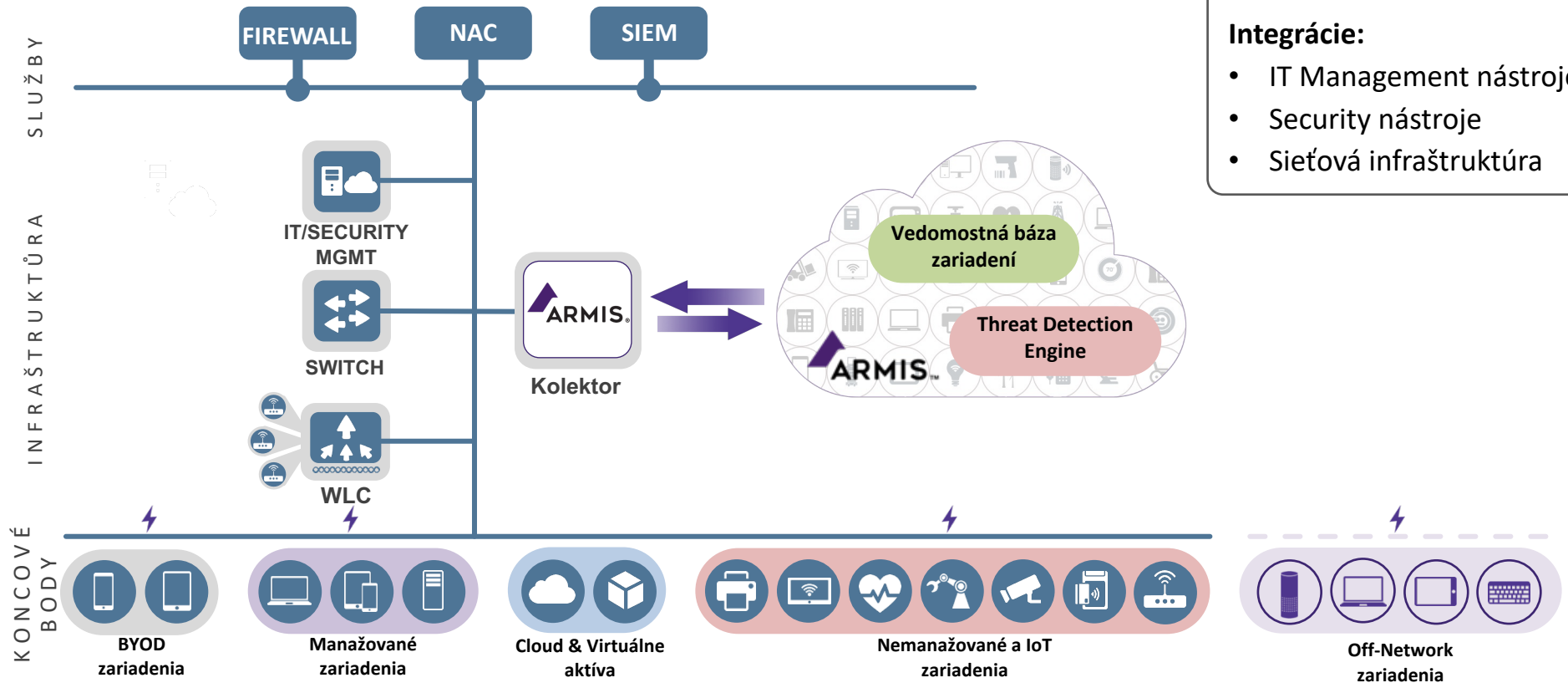
ARMIS VEDOMOSTNÁ BÁZA



Na kontexte záleží:

- 2+ miliardy sledovaných zariadení
- 20 miliónov profilov zariadení
- Najväčšia cloud-based, crowd-sourced, vedomostná báza zariadení
- Porovnáva správanie zariadení v reálnom čase voči „známemu dobrému" správaniu
- Identifikuje porušenie politík, nesprávne konfigurácie, abnormálne správanie
- Rýchle nasadenie & sprevádzkovanie

NASADENIE

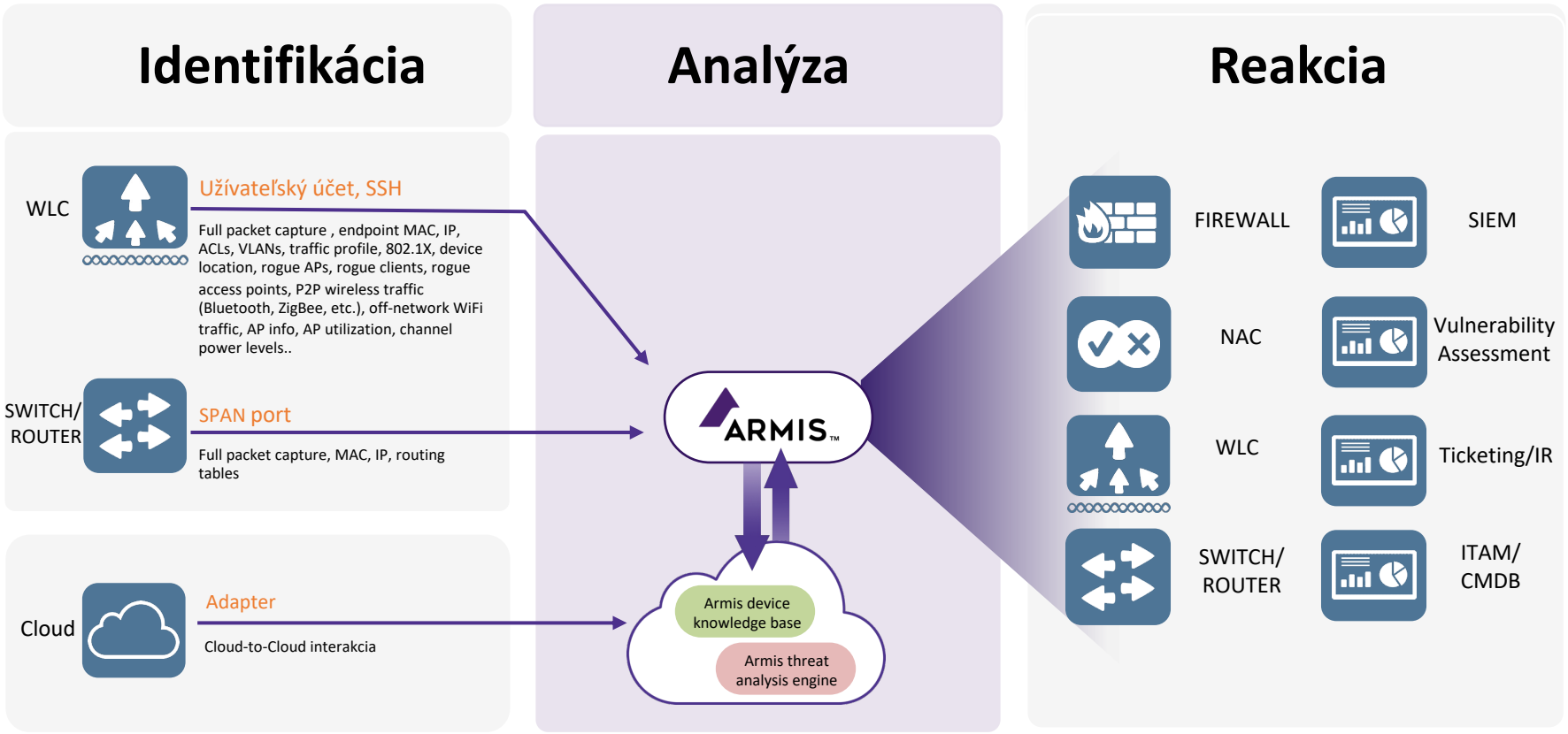


Nasadenie v priebehu minút:

- Kolektor
- SaaS Backend

Integrácie:

- IT Management nástroje
- Security nástroje
- Sieťová infraštruktúra


Identifikácia
Analýza
Reakcia
WLC
Užívateľský účet, SSH
Full packet capture , endpoint MAC, IP, ACLs, VLANs, traffic profile, 802.1X, device location, rogue APs, rogue clients, rogue access points, P2P wireless traffic (Bluetooth, ZigBee, etc.), off-network WiFi traffic, AP info, AP utilization, channel power levels..
SWITCH/ ROUTER
SPAN port
Full packet capture, MAC, IP, routing tables
Cloud
Adapter
Cloud-to-Cloud interakcia
ARMIS
Armis device knowledge base
Armis threat analysis engine
FIREWALL
SIEM
NAC
Vulnerability Assessment
WLC
Ticketing/IR
SWITCH/ ROUTER
ITAM/ CMDB

DEMO


ARMIS
in:devices timeFrame:"30 Days" ltype:"Access Point Interface"
All Sites
All Boundaries
Last 30 Days
Dashboard
Inventory
Alerts
Activity Log
Vulnerabilities
Policies
Reports
Inventory
Overview
Catalog
4,460 Total | 4,460 new
Devices
3,348
High Risk Devices
1,060
Medium Risk Devices
51
Low Risk Devices
0
Enforced Devices
Type
4,460
Devices
2,237 Handhelds
1,621 Computers
347 Automations
95 Medical
160 Others
50%
16%
16%
7%
10%
Mobile Phones
Virtual Machines
Laptops
Measuring Instruments
Others
Operating Systems
See more
Android 48%
Windows 18%
macOS 9%
iOS 8%
Other 16%
Show More Info
4,460 Devices
Risk
Alerts
Name
Data Sources
Category
Type
Model
Brand
10 High
30100 +1
Medical
Infusion Pumps
PlumA+ Infusion Pump
Hospira
6 Medium
Arecont Vision AV5585PM Roof Camera
Imaging
IP Cameras
AV5585PM
Arecont Vision