IoT a IoMT Bezpečnosť

V zdravotníctve

• Výzvy IoMT and IoT zariadení v zdravotníctve

1.3B IoMT zariadení do 2030
18B IoT zariadení do 2030

OHROZENIE PACIENTA

Need to ensure patient safety with IoMT availability, location and risk insights

COMPLIANCE RIZIKO

Limited IoMT visibility and manual assessment makes it difficult to meet regulatory, audit and HIPAA requirements

BEZPEČNOSTNÉ RIZIKO

Limited visibility, unpatched vulnerabilities & unfettered access make it difficult to adopt Zero Trust

TLAK NA ZISK

Need to maximize device usage based on operational analytics

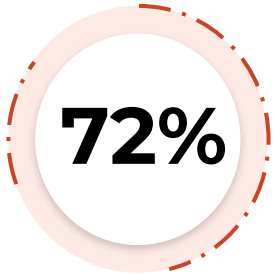
Unit 42 IoT Threat Report: Vysoko zraniteľné zdravotnícke zariadenia

komunikácie všetkých IoT zariadení je nezašifrovaná

všetkých IoT zariadení sú zraniteľné na stredne alebo vysoko závažné útoky

“83% zobrazovacích zariadení používajú OS po životnosti”

Infúznych púmp obsahuje nezaplátané zraniteľností



zdravotníckych organizácií má mix IT a IoT zariadení v rovnakých VLANách.

3M útokov na IoT zariadenia v roku 2021

>40M uniknutých zdravotných záznamov pacientov v roku 2021

- **Ransomware v Nemocnici Rudolfa a Stefanie Benešov**
- **Psychiatrická nemocnice v Kosmonosech**
- **Fakultní nemocnice u sv. Anny v Brně (FNUSA)**

Bloomberg

150,000 Verkada cameras footage stolen affecting **Hospitals, Tesla, Nissan, Schools, and Jails**.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Ransomware Activity Targeting the Healthcare and Public Health Sector

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

82% IoT devices of Health Providers, vendors **targeted by cyberattacks**

BECKER'S HEALTH IT

Cyberattack on Alabama hospital linked to **1st alleged ransomware death**

Source: Kaspersky analysis of IoT attacks
Source: Healthcare data breaches

paloalto NETWORKS

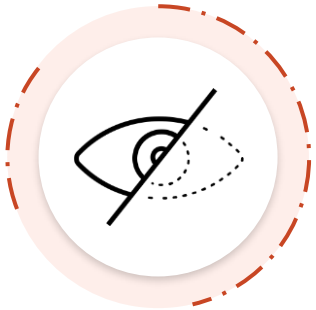
Zdravotníckych zariadení pokladá prevenciu kybernetických hrozieb ako najdôležitejší parameter pri výbere IoT/IoMT riešenia

2021 HIMSS Market Intelligence Research

Celosvetovo priemerná cena výpadku servera alebo sieťovej infraštruktúry je viac ako 300,000 USD za hodinu

Prečo niektoré riešenia nefungujú?

Chýbajúca viditeľnosť

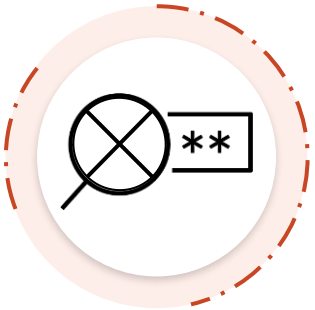


Detekcia na základe signatúr je nepresná a nedokáže detekovať nové neznáme zariadenia

Žiadna ochrana

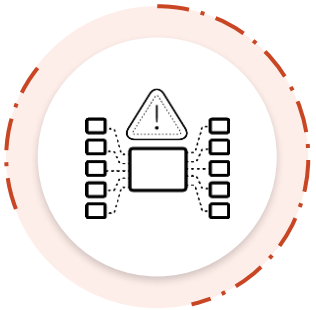
Existujúce riešenia dokážu len alerovať, musia sa integrovať s iným riešením na ochranu

Chýbajúca Zero Trust



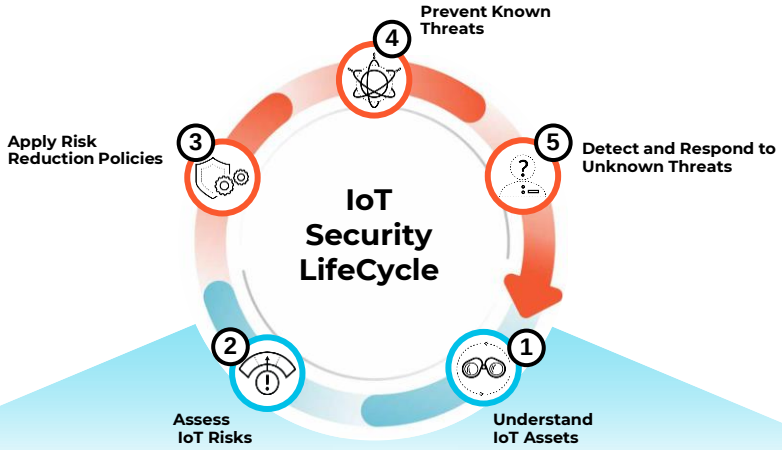
Chýbajúca Zero Trust inteligencia pre návrh politík a redukciu bezpečnostných pravidiel

Zložitá implementácia



Nové procesy, senzory, integrácie a ľudia sú potrebný pre základnú bezpečnosť v IOT

Správna metodológia pre životný cyklus a manažment zariadení



Identifikácia	Nasadenie	Optimalizácia	Vyradenie
Pasívne	Automatizované	CapEx a OpEx	Ochrana dát
Machine Learning	Context-aware	Resource allocation	Compliance
Odhalenie zraniteľností	NAC/CMMS integrácia	Sledovanie prevádzky	Vyradenie z prevádzky
Určenie rizika			

Čo by malo dobré IoMT riešenie spĺňať?

Rýchla a presná identifikácia

Používa ML a crowdsourcing na poskytovanie viditeľnosti a prehľadov o všetkých zariadeniach, dokonca aj o tých, ktoré ste ešte nevideli

Ochrana pred hrozbami

Analyzuje správanie s cieľom odhaliť riziko zariadenia a anomálnu aktivitu a predchádza známym a neznámym hrozbám IoT

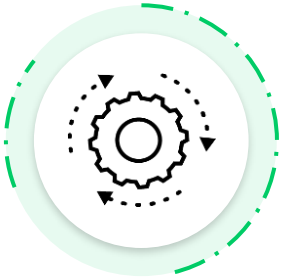
Automatické Zero Trust

Uľahčuje prijatie zero trust vďaka automatickým pravidlám s najmenšími oprávneniami a vynúteniu jedným kliknutím

Starostlivosť o pacienta

Dôveruje mu 1 z 5 nemocníc v USA so sústredenými prevádzkovými prehľadmi, zdieľanými informáciami výrobcu a vylepšeným zabezpečením

Integrované procesy



Zjednodušené nasadenie bez senzora a automatizácia pracovného postupu v rámci existujúcich IT a bezpečnostných riešení

IoT Security rieši IoMT a IoT výzvy pre zdravotnícke organizácie

Lepšia starostlivosť o pacientov

Umožňuje biomedicínskym a klinickým tímom pochopiť využitie zariadení na optimalizáciu starostlivosti o pacienta a riadenie životného cyklu aktív

Automatický Compliance

Umožňuje manažérom rizík, biomedicínskym a klinickým tímom vyhodnotiť stav zabezpečenia zariadení a nedostatky v compliance

Redukcia rizika

Umožňuje bezpečnostným tímom implementovať Zero Trust s automatickým zisťovaním IoMT/IoT, hodnotením rizík, segmentáciou a nepretržitým monitorovaním rizík

Zvýšenie utilizácie

Pomáha čo najlepšie využiť zdravotnícke zariadenia a automatizovať pracovné postupy v rámci existujúcich technológií

SJSIVUS1

Risk Score 42

Category	UltraSound Machine
Profile	Volcano UltraSound Machine
Confidence Level	High
Confidence Score	98
Last Activity	13:06 March 25, 2021

IDENTITY

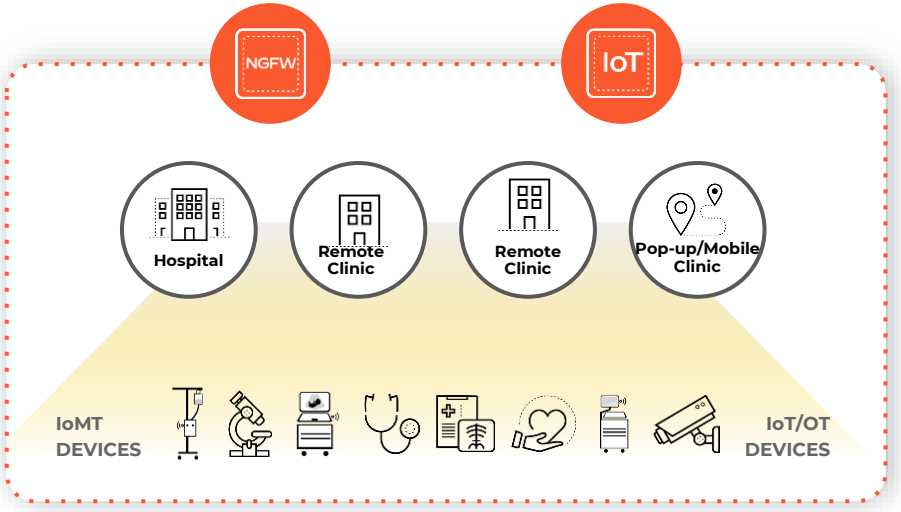
Vendor	Philips/Volcano
OS Group	Windows
OS Version	Windows XP
OS / Firmware Version	XP
OS Support	No
AE Title	SJSIVUS1
MAC Address	0c:c4:7a:02:91:e2
IP Address	10.163.23.72
VLAN	110
Subnet	10.0.0.0/8
International Access	No

Monitoring prevádzky

Optimalizácia CAPEX a OPEX

- Presná identifikácia a reporting
- Plánovanie nákupu na základe presných štatistík
- Plánovanie údržby na základe času kedy sa zariadenie používa
- Zlepšenie “užívateľskej skúsenosti” pacienta

Prečo Palo Alto Networks IoT Security ?



BEZ Senzorov

BEZ Investícii do infra

BEZ Ďalších nákladov

Best in Class — 1 z 5 Nemocíc v USA chránená PAN

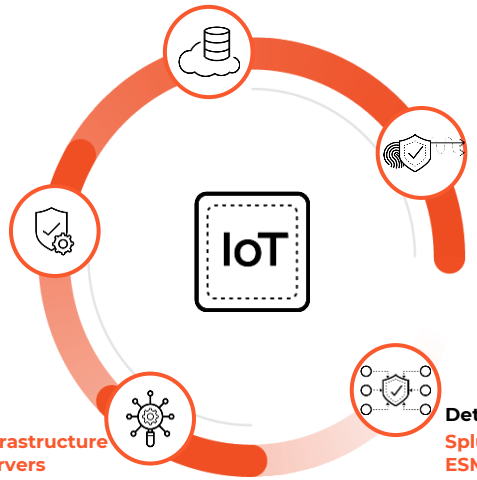
90% — Všetkých zariadení sú zdetekované do 48 hodín pomocou strojového učenia

1-Click — Posúdenie rizika a compliance

70X — Rýchlejšie nasadenie do prevádzky

Integrované pracovné postupy

So zabudovanými integráciami, odomyká silu existujúcich IT a bezpečnostných riešení



Asset Management/CMMS
ServiceNow | AIMS by Phoenix | Nuvolo

Network Access Control (NAC)
CiscoISE | Aruba ClearPass | Forescout

Vulnerability Management
Qualys | Rapid7 | Tenable

Network Management
Cisco DNA Center | Prime Infrastructure WLC | Aruba WLC | SNMP Servers

Detection and Response
Splunk | Micro Focus ArcSight ESM | LogRhythm | Cortex XDR

Zabudované integrácie
Vyhnite sa časovo náročnému programovaniu vďaka predpripravenými šablónami

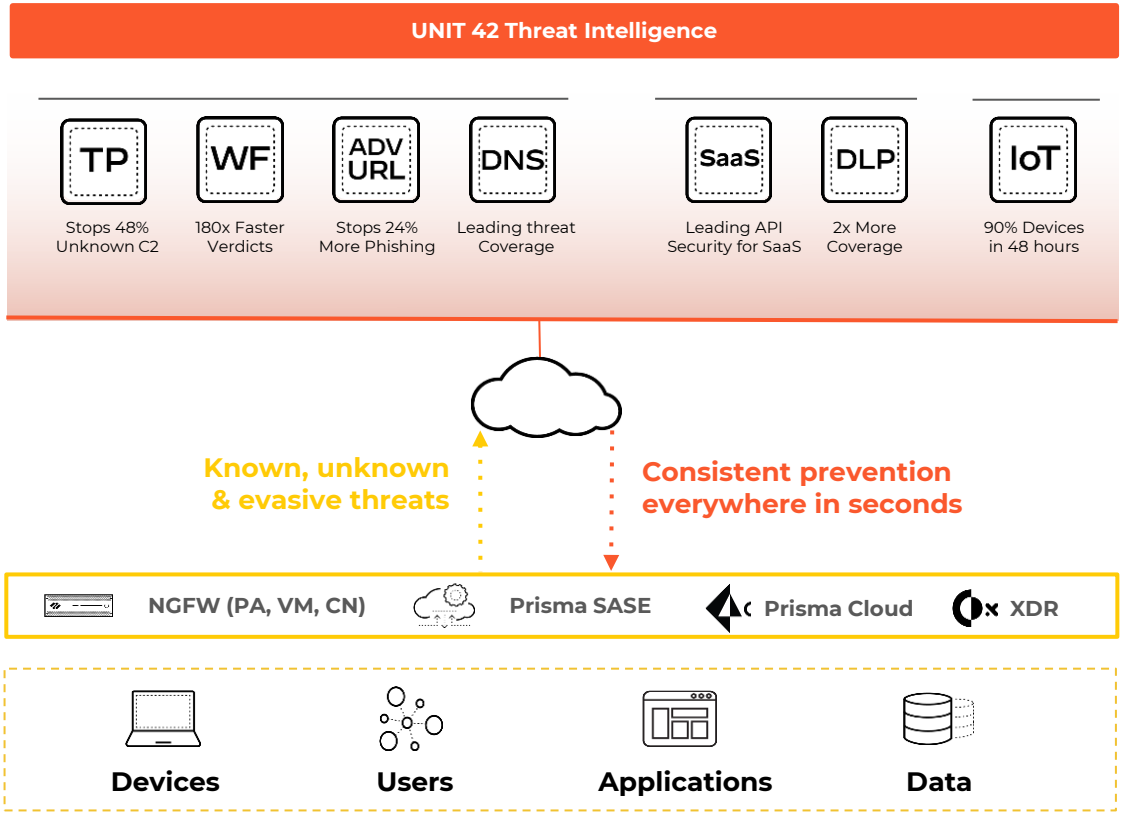
Automatizujte existujúce postupy
Bezproblémová integrácia do existujúcich pracovných postupov v IT a bezpečnosti

Objavte nové spôsoby použitia
Nájdite IoT zariadenia, automatizujte onboarding, mikrosegmentáciu, vyradenie z používania a ďalšie

Rozsiahly ekosystém
Upgradujte na Cortex XSOAR a odomknite použitie pre viac ako 700 integrácií

CMMS= Computerized maintenance management system
WLC= Wireless LAN Controller

Bezpečnostné služby od Palo Alto Networks-najlepšie vo svojej triede



- Kompletná a **dokázateľne najlepšia ochrana** na trhu
- **Zdieľaná threat inteligencia** cez viacero bezpečnostných produktov zaručuje kompletné pokrytie všetkých attack vektorov
- **Network effect viac ako 85,000 zákazníkov** premení neznáme hrozby na vzorky 180x rýchlejšie a denne poskytneme 4.3M updatov
- **Efektivita a návrat investície** o 30% rýchlejšie

Ďakujem za pozornosť

Priestor pre Vaše otázky