# Infrastruktura sieciowa kluczem do poprawy jakości usług medycznych

Extreme®
Connect Beyond the Network

# Co stoi za marką Extreme Networks?

## Historia innowacji

- Rok założenia: **1996**
- **Ponad 20 lat** doświadczenia w technologiach sieciowych
- **Pierwsze na rynku** przełączniki Gig-E / 10 Gig-E
- **Ponad 500** aktywnych partnerów
- Pełna gama rozwiązań, od sieci **przewodowej** przez **bezprzewodową,** po **SDN**
- **100% własnych pracowników** działu obsługi i wsparcia

## Globalna wartość

- Przychód: **$1.2 Billion**
- **3000+** pracowników
- NASDAQ: **EXTR**
- Główna siedziba w **San Jose, CA**
- **30,000 klientów**
- **2000** lokalnych partnerów technologicznych

 ©2016 Extreme Networks, Inc. All rights reserved

# Extreme Networks dla służby zdrowia

- Ponad 1200 wdrożeń na całym świecie
- Zapewnianie skalowalnej i całościowej architektury sieci
- Pełna widoczność w ramach zarządzania, kontroli i analityki


©2016 Extreme Networks, Inc. All rights reserved

# Przykłady wdrożeń - Uniwersytecki Szpital Dziecięcy w Krakowie, Centralny Szpital Kliniczny MSWiA w Warszawie

UNIWERSYTECKI SZPITAL DZIECIĘCY W KRAKOWIE
UL. WIELICKA 265, 30-663 KRAKÓW

SŁUŻBA ZDROWIA
MSWiA
CSK MSWiA

©2016 Extreme Networks, Inc. All rights reserved

# W jaki sposób zmienia się wykorzystanie technologii w służbie zdrowia

©2016 Extreme Networks, Inc. All rights reserved

# Czynniki sprzyjające wprowadzaniu zmian w sieciach komputerowych placówek medycznych

- Rola systemów informatycznych w medycynie nabiera coraz większego znaczenia. **Mobilność** jest głównym wyznacznikiem IT w medycynie. Dotyczy ona zarówno personelu jak i urządzeń - w tym także tych ratujących i podtrzymujących życie.
- W zastosowaniach medycznych używane są różne sieci mobilne: telefonii lokalnej (DECT), Bluetooth , 3G i 4G, ZigBee (sensory), WMTS (Wireless Medical Telemetry Service) ale przede wszystkim sieci **WiFi**.


©2016 Extreme Networks, Inc. All rights reserved

# Przykład: Nowe wyzwania dotyczące IoT

Pompy infuzyjne - **System Symbiq Infusion System od Hospira:**

- Zapewnia, że niewykorzystywane porty są zamknięte, w tym port 20/FTP i port 23/Telnet.
- Monitorowanie i rejestrowanie całego ruchu sieciowego próbującego dotrzeć do danego produktu poprzez port 20/FTP, 23/Telnet oraz 8443.
- Należy skontaktować się ze wsparciem technicznym Hospira w celu zmiany domyślnego hasła dostępu do portu 8443 lub zamknąć go.


©2016 Extreme Networks, Inc. All rights reserved

# Podatność urządzeń medycznych na ataki hakerskie


By ASHLEY WELCH / CBS NEWS / August 4, 2015, 11:29 AM

**U.S. officials warn medical devices are vulnerable to hacking**

- Producent urządzeń medycznych potwierdził, że skomputeryzowane pompy, które mają za zadanie dostarczanie leków w sposób ciągły – **jest podatne na ataki hakerskie.**
- Może to potencjalnie umożliwić nieautoryzowanym użytkownikom sterowanie urządzeniem i **zmieniać dawki leków**, które pompa dostarcza pacjentowi.


©2016 Extreme Networks, Inc. All rights reserved

# BYOD zmienia model świadczenia usług

- Kliniczne przepływy pracy są realizowane w sposób mobilny wewnątrz i na zewnątrz szpitala
- Spójne świadczenie usług pomiędzy sieciami Wi-Fi i komórkowymi to nowy standard
- Dział IT nie ma już kontroli nad urządzeniem, musi obsługiwać użytkownika i dane
- Zgodność z przepisami to kluczowy wymóg, ale użytkownicy końcowi się nim nie przejmują


©2016 Extreme Networks, Inc. All rights reserved

# Geolokalizacja

- Sieć WiFi może być stosowana do realizacji uslug **geolokalizacji**, czyli lokalizacji przedmiotów i osób w przestrzeni. Geolokalizacja wykorzystuje specjalne miniaturowe nadajniki WiFi (tzw. "***tagi***"), które śledzone są przez sieć bezprzewodową, a ich położenie jest na bieżąco przedstawiane w aplikacji geolokalizacyjnej. Program geolokalizacyjny zapamiętuje tez historię przemieszczania się monitorowanych obiektów. Bateria wbudowana w tag wystarcza zazwyczaj na 1-4 lat ciągłej pracy. Dokładnosć geolokalizacji z wykorzystaniem tagów wynosi ok 1m.
- W branży medycznej monitoruje się sprzęt przenośny (aparaturę diagnostyczną, pompy infuzyjne) oraz pracowników.


©2016 Extreme Networks, Inc. All rights reserved

# Coraz więcej urządzeń mobilnych w sieci

- Sieci bezprzewodowe coraz częściej **zastępują** tradycyjne, bazujące na **fizycznym okablowaniu miedzianym**.
- Sieci WiFi zgodne z najnowszym **802.11ac, 802.11ax** pozwalają na realizację szybkiej i niezawodnej transmisji danych dla wielu użytkowników pracujących jednocześnie.
- Przykładem mobilności w placówkach medycznych mogą być:
  - Tablety i smartfony wykorzystywane przez personel medyczny do dostępu do systemów i baz danych (np. zdjęć RTG, historii pacjenta, itp.)
  - Telefony przenośne VoIP wykorzystywane do komunikacji wewnętrznej.
  - Ruchome systemy monitorujące i telemetryczne (np. mobilne monitory pracy serca)
  - Stacjonarne systemy monitorujące, pompy infuzyjne, itp. – ich połączenie z siecią bezprzewodową eliminuje konieczność instalacji kosztownego okablowania w salach chorych.


©2016 Extreme Networks, Inc. All rights reserved

# Rekomendacje technologiczne

- Szyfrowanie danych przesyłanych siecią i stosowanie silnych algorytmów uwierzytelniających, np. **802.1x**
- Wdrożenie infrastruktury kontroli dostępu do sieci przeznaczonej dla personelu, tj. **autoryzowanie użytkowników oraz urządzeń**. Autoryzacja użytkowników może bazować na już istniejących w zasobach informatycznych – np. na autoryzacji w domenie
- Stosowanie odrębnych identyfikatorów sieci SSID przypisanych do wydzielonych sieci VLAN, co zapewnia separację systemów i danych krytycznych oraz pozostałych (np. separacji systemów medycznych od sieci zapewniającej dostęp pacjentów do Internetu)
- Idea „Single SSID”
- Rozwiązanie wspierające polityki bezpieczeństwa
- Wsparcie dla MDM


©2016 Extreme Networks, Inc. All rights reserved

# Rozwiązania dla służby zdrowia

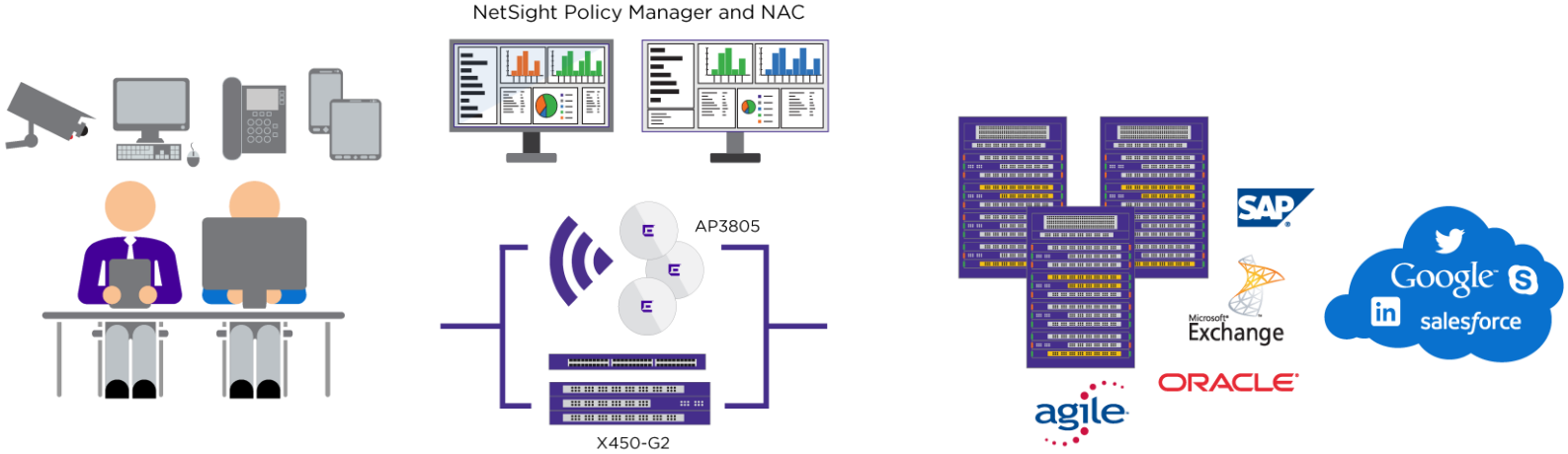
©2016 Extreme Networks, Inc. All rights reserved

# Rozwiązania bezprzewodowe spełniające normy

- Wykorzystanie punktów dostępowych WiFi posiadających wymagane certyfikaty i atesty, np. certyfikat środowiskowy EN-60601-1-2 (dot. zakłóceń elektromagnetycznych)


©2016 Extreme Networks, Inc. All rights reserved

# Wbudowane polityki – bezpieczeństwo organizacji

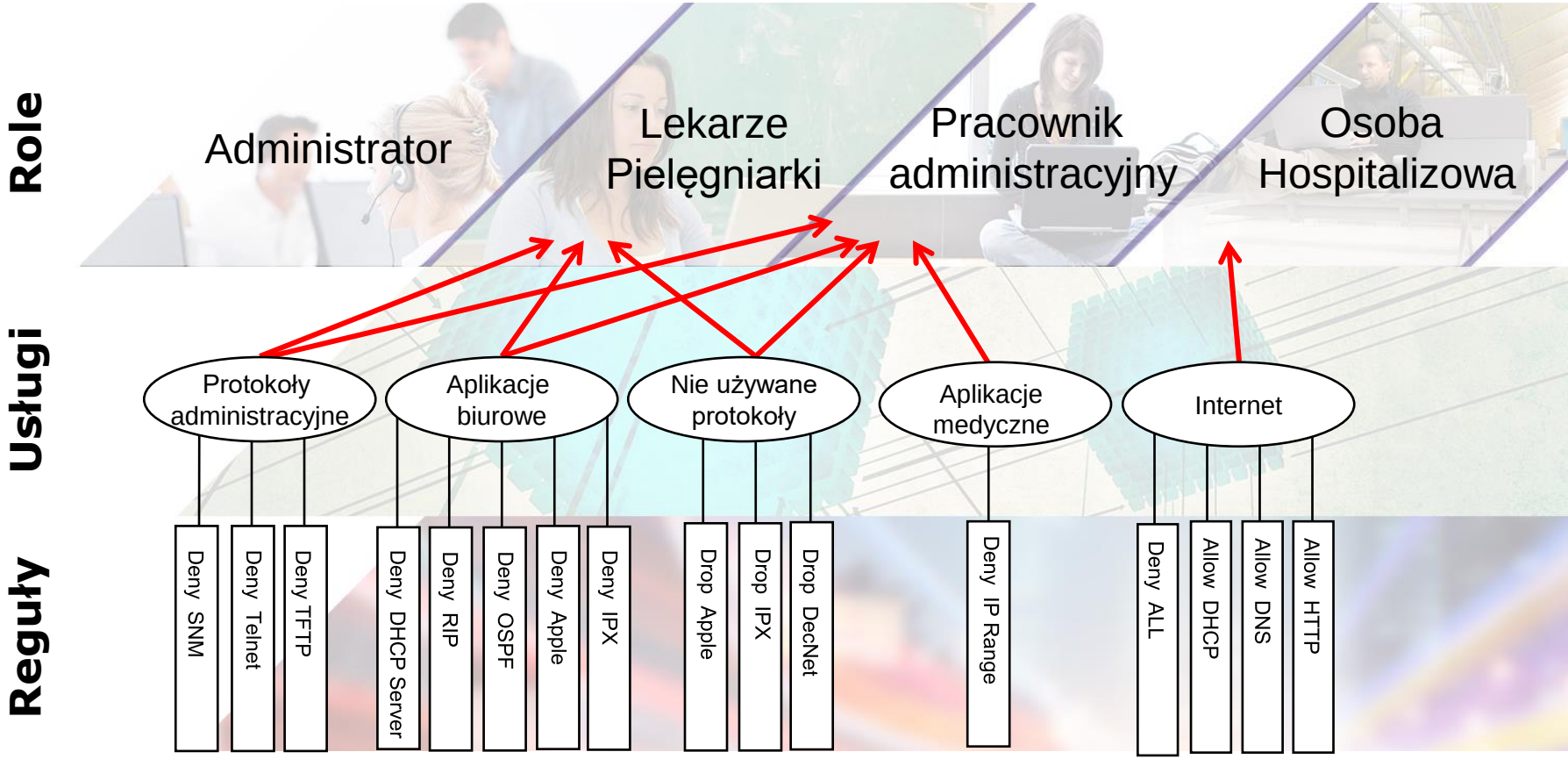



## Polityki budowane w oparciu o role

1. Rola użytkownika (Lekarz/Księgowość/Gość/Administratorzy/Urządzenie medyczne)
2. Autentykacja użytkownika/urządzenia, definicja polityki i zarządzanie
3. Reguły i usługi – egzekwowanie polityk dla bezpiecznego dostępu
4. Bezpieczny dostęp do aplikacji


©2016 Extreme Networks, Inc. All rights reserved

# Polityki bezpieczeństwa w oparciu o role






©2016 Extreme Networks, Inc. All rights reserved

# Widoczność: zarządzanie użytkownikami i urządzeniami

Overview | Wireless Details | AP History | Client History | **NAC End-System Details**

**Access Profile** | End-System | End-System Events | Health Results

Refresh View

**Identity and Access**
User Name: CORP\estinson
AuthType: 802.1X
State: ACCEPT
Policy: Extreme-Corp
Profile: Extreme-Corp

**Custom Data**
Custom 1: Phone: +1 603-952-5829

**Physical Device Identity**
3C:A9:F4:6F:84:88
134.141.68.217
estinson-ws6.corp.extremenetworks.com

**Location**
Zone:
134.141.104.29/nhsal3825iap10 Extreme -Corp , 9 Northeastern Blvd Salem, NH 03079
Production
NAC Gateway: 134.141.104.82

**Activity**
Last seen 08/18/2014 02:16:01 PM
First seen 12/16/2013 11:54:00 AM

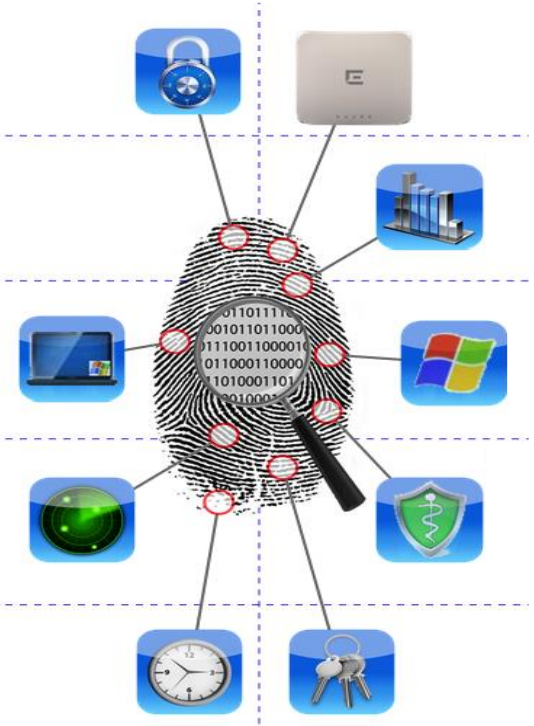
**Access Type**
AP: 14121556085A0000
Port Alias: Extreme-Corp,
AP Port: nhsal3825iap10 (20-B3-99-D8-22-F0)

**Top Applications**
Outlook Office365 165.67 kB
LogMeIn 33.01 kB
Microsoft Sharepoint 24.94 kB
NTLMSSP 22.59 kB
134.141.68.217 20.51 kB

**Device Family**
Windows
Windows Vista/ 7/ 2008

**Health**
Risk: NO_RISK
Total Score: 0
Last Scan: 8/18/2014 1:50:02 PM

**Registration**
State: Not Registered



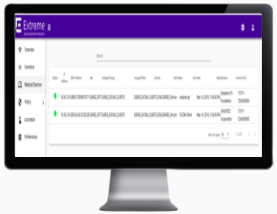

©2016 Extreme Networks, Inc. All rights reserved

# Defender IoT – komponenty rozwiązania

## ExtremeCloud Appliance

Urządzenie do terminacji ruchu - aplikacja do zarządzania dostępna jako fizyczny appliance lub maszyna wirtualna

## Defender Application



Aplikacja do kreowania profili bezpieczeństwa, inwentaryzacji zasobów i podłączonych urządzeń

## Defender Access Hardware

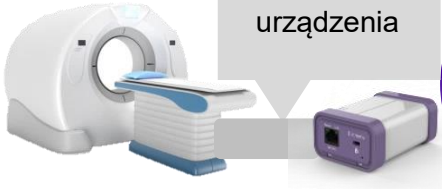
Urządzenie monitorujące ruch, nakładające profile ruchu, zapewnienie widoczności w warstwach L2-7 (aplikacje)


©2016 Extreme Networks, Inc. All rights reserved

# Przykłady zastosowania

Nieautoryzowane urządzenie podłącza się do adaptera. Dostęp do sieci jest blokowany i zgłaszany.

Maszyna MRI została zainfekowana wirusem; próbuje zainfekować inne urządzenia

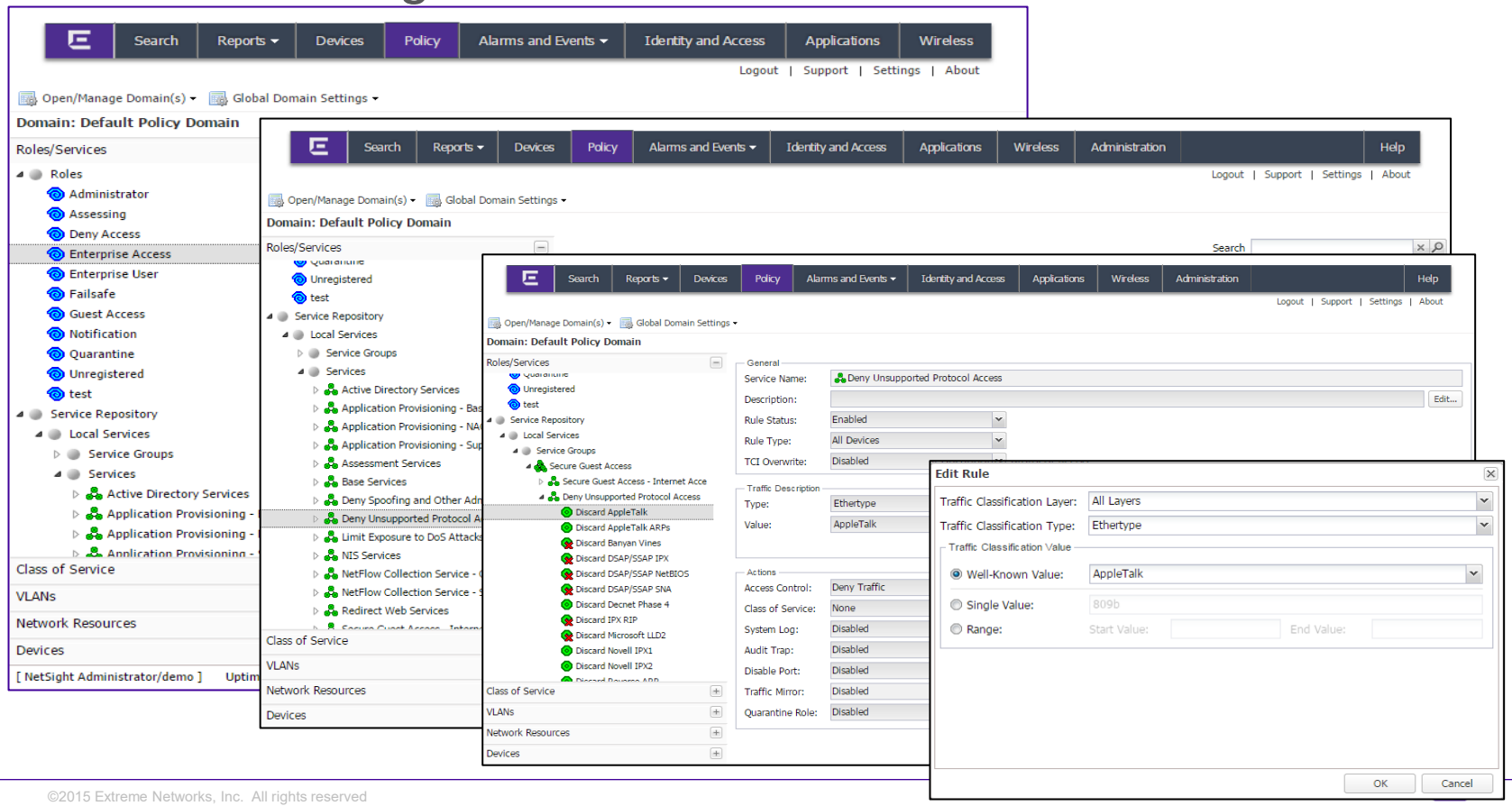


Pompa infuzyna

Haker (zarówno w sieci, jak i poza nią) próbuje złośliwie uzyskać dostęp do pompy infuzyjnej. Zostanie zablokowany na adapterze

©2016 Extreme Networks, Inc. All rights reserved

# Centralne zarządzanie politykami bezpieczeństwa – ExtremeManagement




©2015 Extreme Networks, Inc. All rights reserved

# Extreme jako “leader” wg Gartner – w technologiach LAN/WLAN


©2016 Extreme Networks, Inc. All rights reserved


# Dziękujemy za uwagę

WWW.EXTREMENETWORKS.COM