Od sieci po sterowniki PLC — ochrona infrastruktury krytycznej z wykorzystaniem ekosystemu WatchGuard

Damian Gołuch

Business Unit Manager, Bakotech

damian.goluch@bakotech.com

Jakie procedury zwiększają bezpieczeństwo systemów IT/OT

🔐 **1. Segmentacja sieci**

👤 **2. Zarządzanie dostępem**

🧱 **3. Zabezpieczenie punktów końcowych i urządzeń przemysłowych**

🔄 **4. Zarządzanie aktualizacjami i poprawkami**

🔎 **5. Monitorowanie i detekcja zagrożeń**

🧪 **6. Testy bezpieczeństwa i analiza ryzyka**

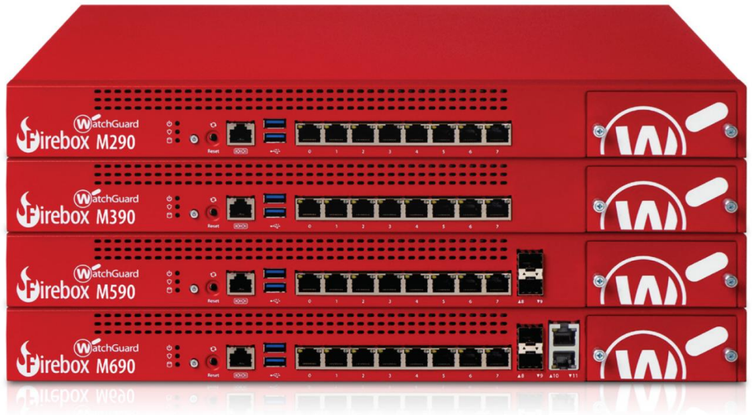
🧯 **7. Plany reagowania na incydenty**

📚 **8. Szkolenie personelu OT**

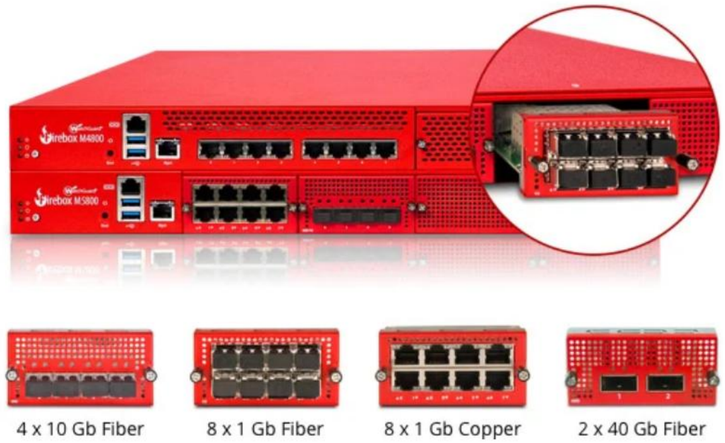
🧩 **9. Zarządzanie cyklem życia urządzeń OT**

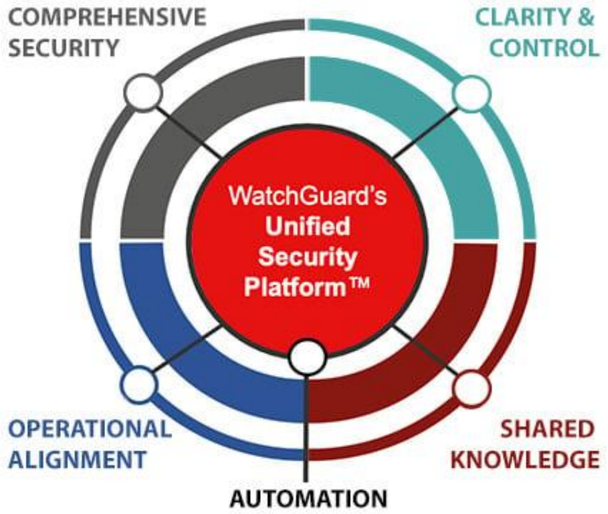
🔐 **10. Kontrola fizycznego dostępu**

Zapora sieciowa UTM/Firewall



Każda sieć potrzebuje pełnego pakietu silników skanujących do ochrony przed ransomware, wirusami, złośliwymi aplikacjami, botnetami i innymi zagrożeniami.





WatchGuard Threat Hunting

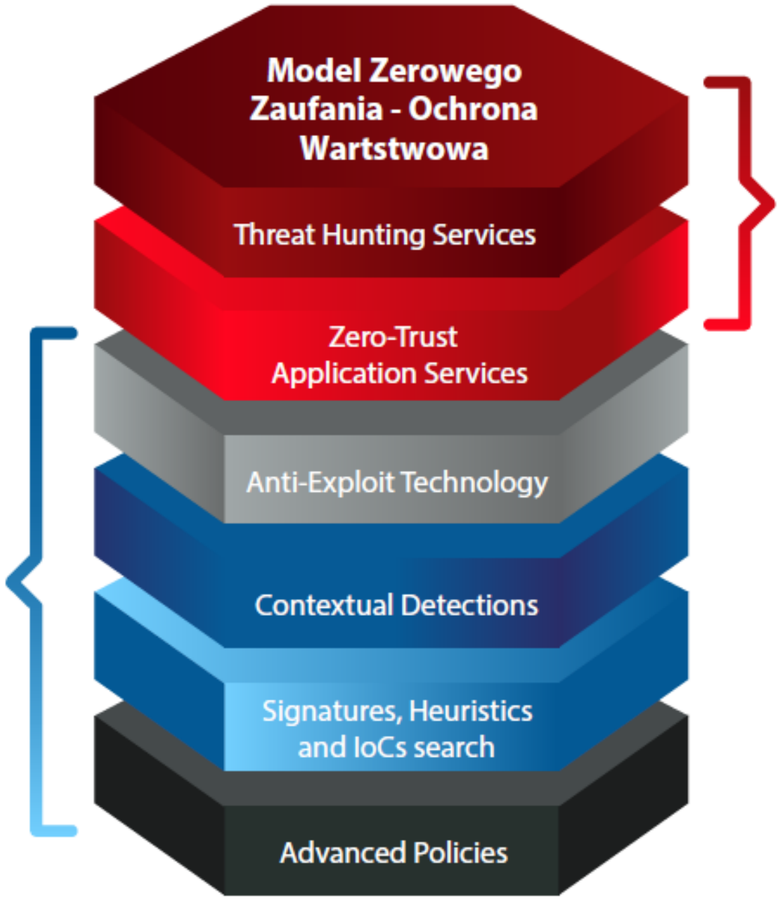
ENDPOINT LAYERS:

Layer 1/ / Enhanced Security Policies
Wykrywanie lub blokowanie wykonywania powszechnych technik ataku.

Layer 2 / Signature Files, Heuristic Technologies and IoC Search
Skuteczna, zoptymalizowana technologia do wykrywania ataków

Layer 3 / Contextual Detections
Umożliwiają one wykrywanie bez złośliwego oprogramowania i bez plików

Layer 4 / Anti-Exploit Technology
Umożliwia wykrywanie ataków bezplikowych, które mają na celu wykorzystanie podatności.



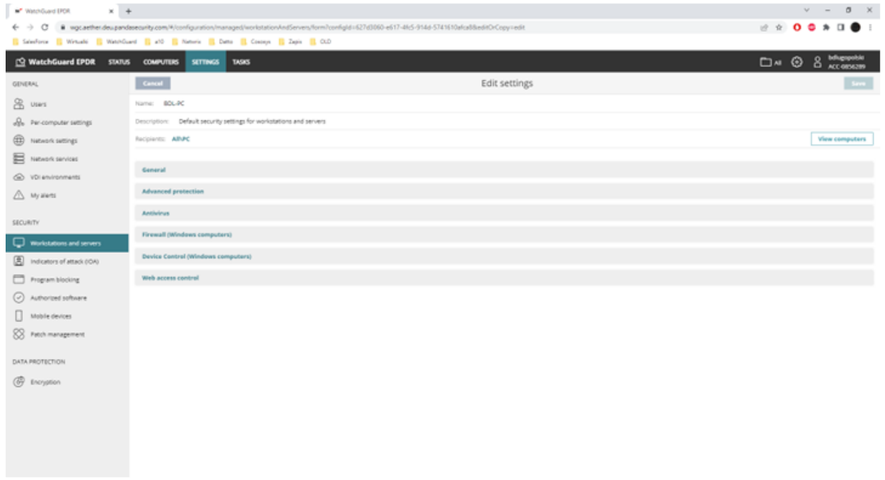
CLOUD-NATIVE LAYERS

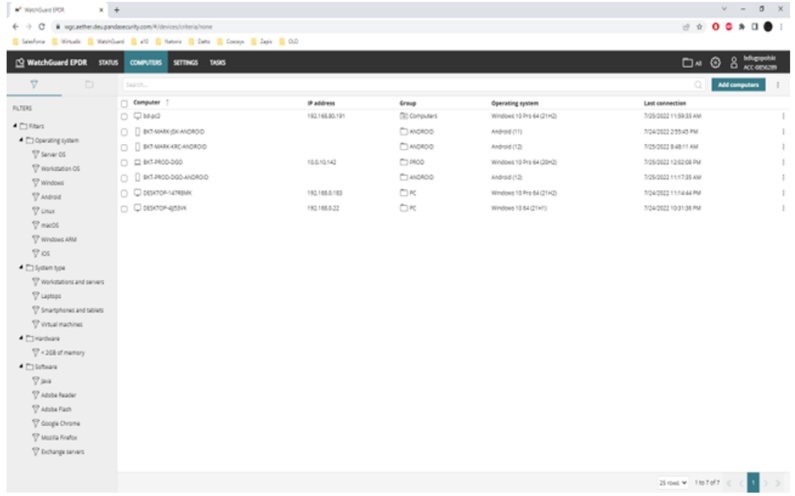
Layer 5 / Zero-Trust Application Service

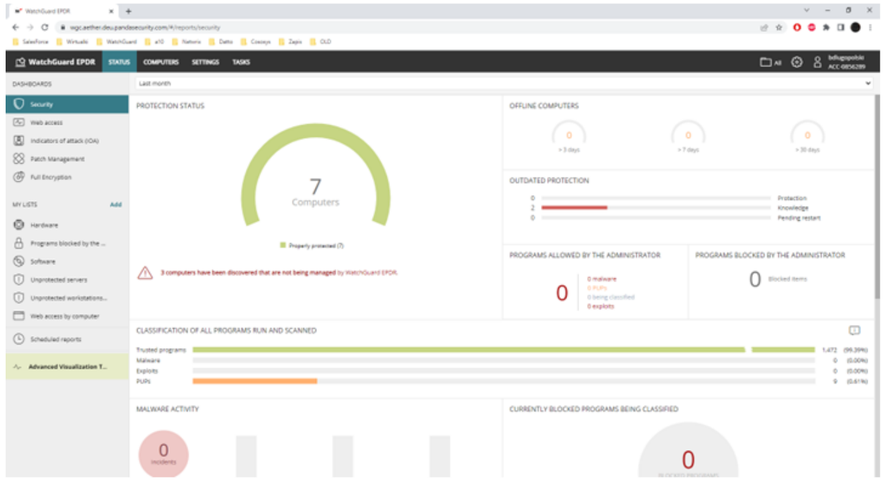
Klasyfikuje 100% procesów przed ich uruchomieniem, odmawiając wykonania, dopóki nie zostaną one uznane za zaufane.

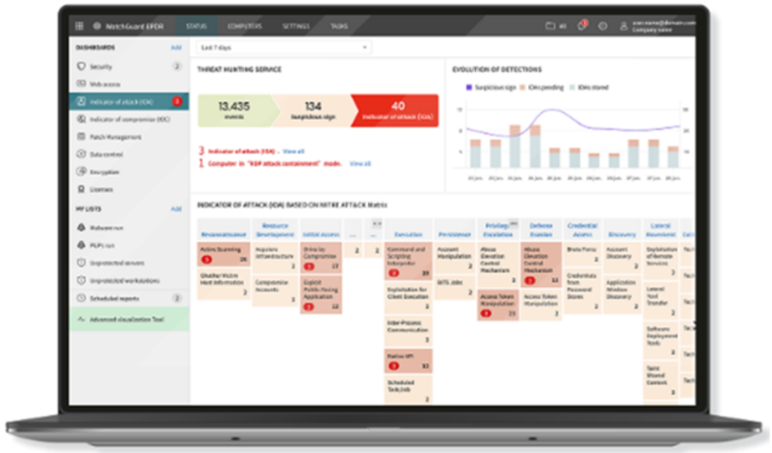
Layer 6 / Threat Hunting Service
Umożliwia on wykrywanie zagrożonych punktów końcowych, ataków we wczesnej fazie, podejrzanych działań oraz wykrywanie IoAs

Wykrywanie, reakcja i zapobieganie incydentom





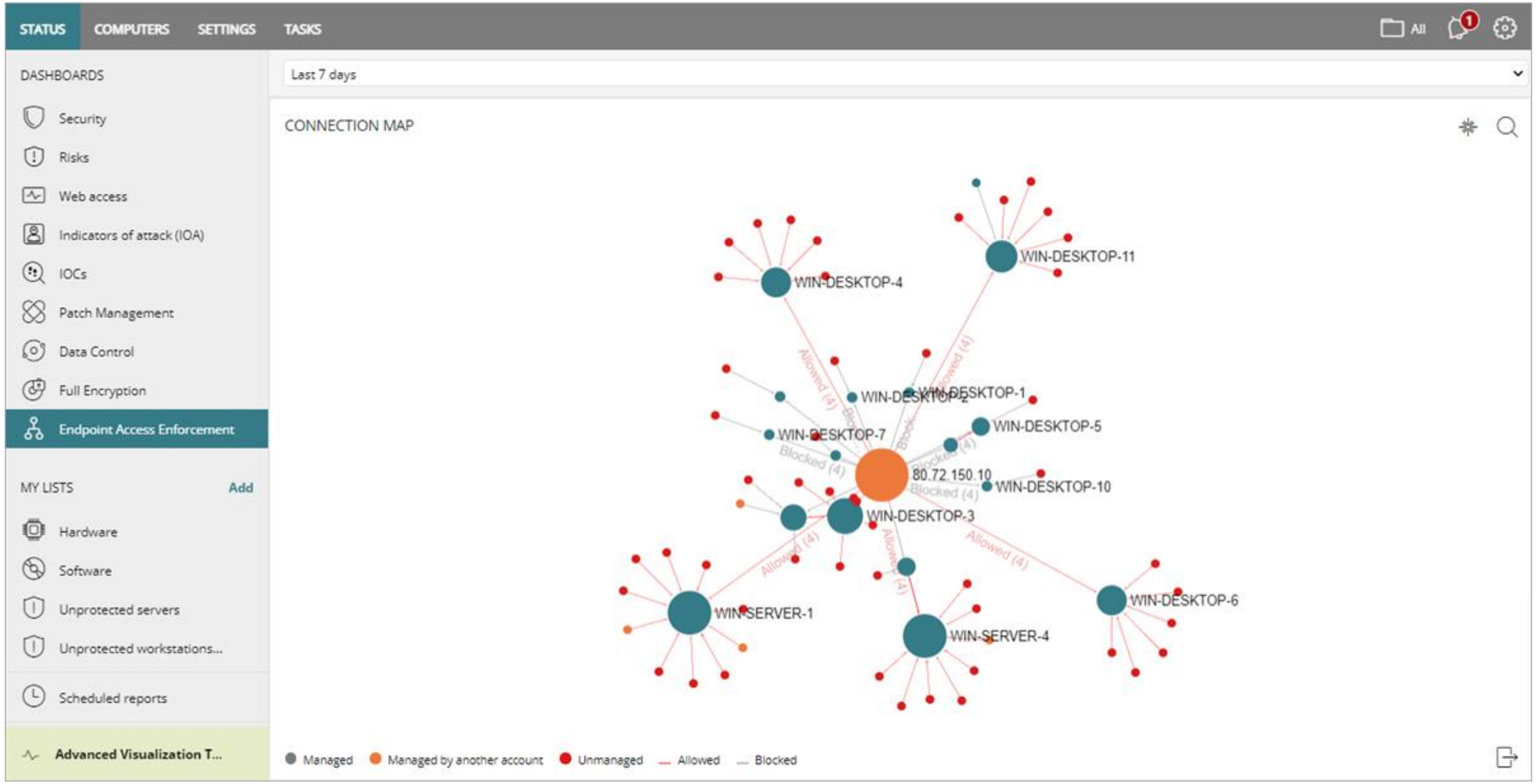




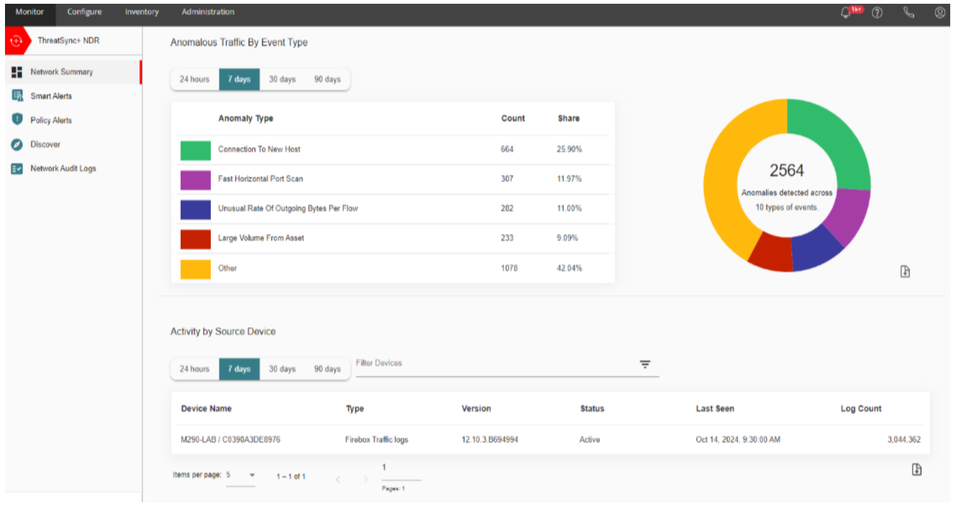
Pełna widoczność oraz zarządzanie z jednej konsoli.

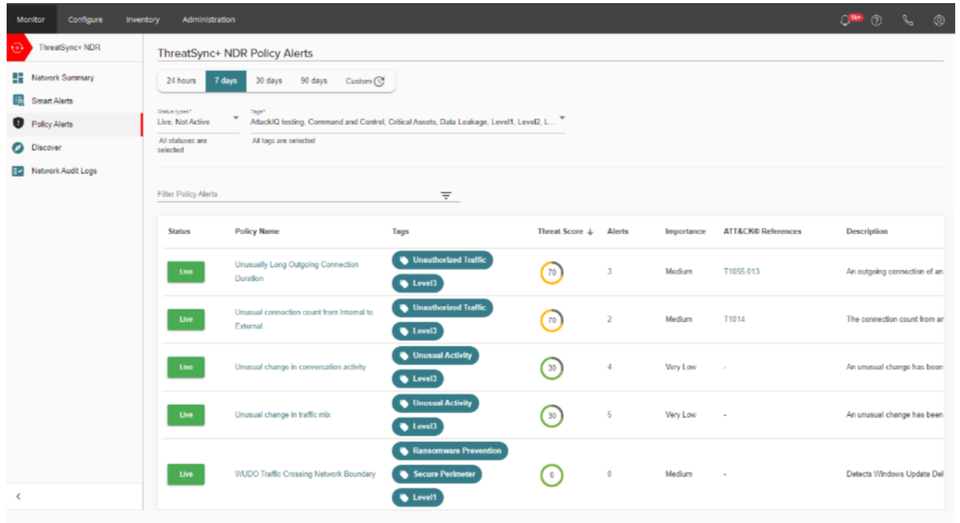
Ułatwienie pracy dla administratora IT czy szum informacyjny?

Endpoint Access Enforcement monitoruje połączenia z komputerami w sieci, aby ograniczyć infekcje z niezabezpieczonych urządzeń (Windows, Mac i Linux). Pulpit Endpoint Access Enforcement pokazuje informacje o połączeniach między komputerami w sieci, które spełniają warunki skonfigurowane w ustawieniach Endpoint Access Enforcement

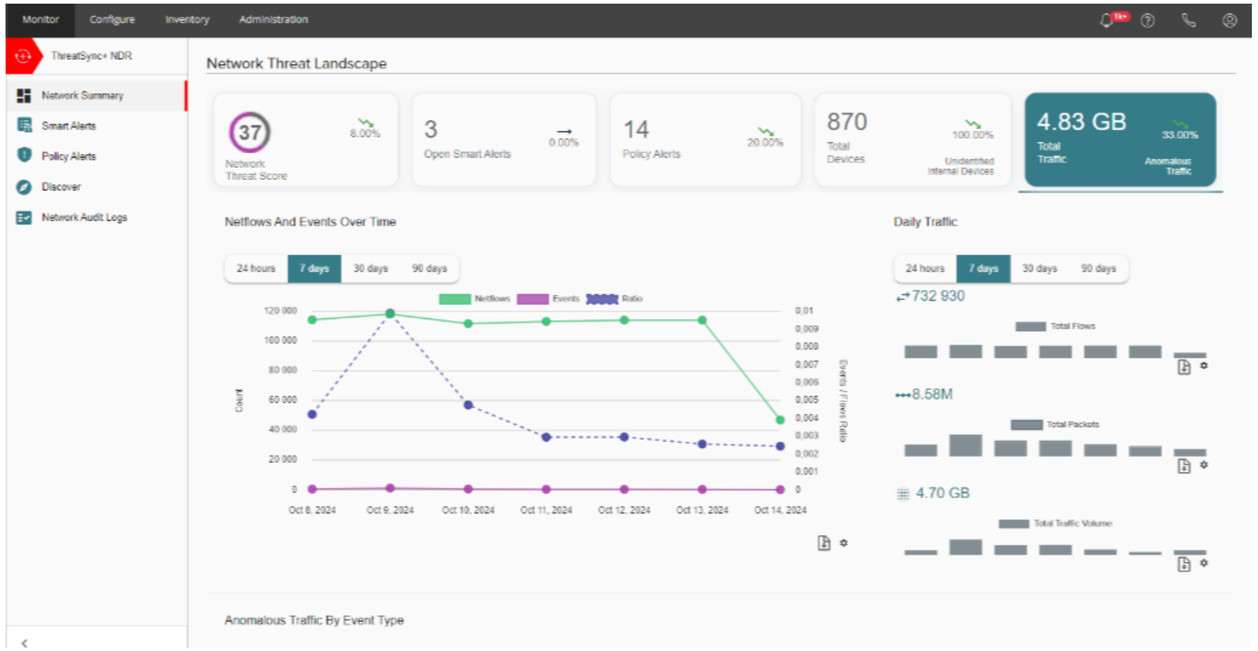


ThreatSync+ NDR



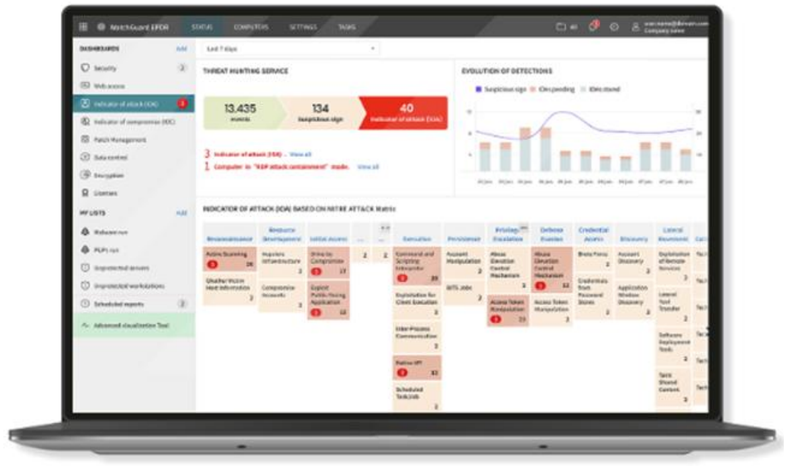


ThreatSync+ NDR pozyskuje NetFlow i szybko wykrywa ataki, które ominęły obronę obwodową i aktywnie rozwijają się w sieci. Silnik AI identyfikuje C&C, ruch boczny, nietypowy dostęp, nietypowy ruch danych, beaconing, skanowanie i inne procesy ataku oparte na ruchu.

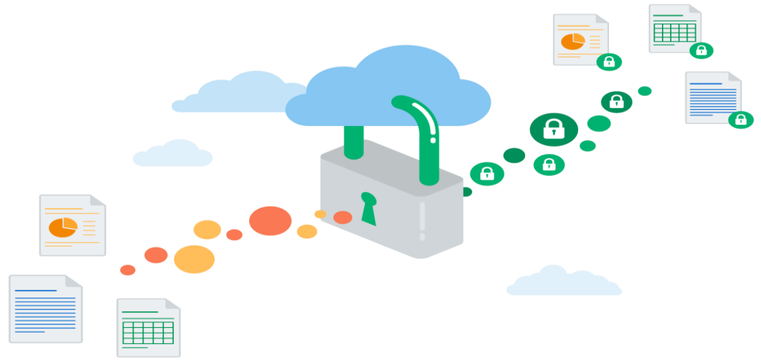


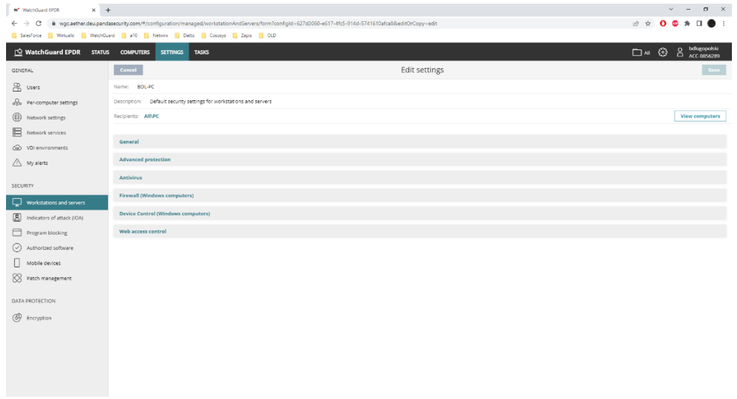
Moduły rozszerzające platformę WatchGuard Security of One

Świadomość, z jakich aplikacji korzystają użytkownicy oraz regularne aktualizacje to podstawy zapewnienia bezpieczeństwa firmy. Exploity, backdoory, End-Of-Life Software
oraz OS – hakerzy bez trudu są w stanie wykorzystać wszelkie luki w bezpieczeństwie, więc rolą administratorów jest sobie z tym poradzić.



Szyfrowanie **może pomóc chronić dane firmy przed atakami hakerów i cyberprzestępców**. Zakładając, że są one prawidłowo zaszyfrowane, dane przechowywane na serwerach i urządzeniach firmowych powinny pozostać bezpieczne, nawet jeśli urządzenie zostanie skradzione.





DZIĘKUJĘ ZA UWAGĘ!

Damian Gołuch
Business Unit Manager,Bakotech

Damian.goluch@bakotech.com

+48 664 753 900