SOPHOS

Najlepsze praktyki ochrony punktów końcowych przed oprogramowaniem Ransomware, na bazie rozwiązań producenta Sophos

Rafał Gałka
Security Product Manager

06.03.2025

Wpływ ataków ransomware

Częstotliwość ataków

59%

organizacji zostało zaatakowanych przez oprogramowanie ransomware w 2023 roku

Poziom zaszyfrowania

70%

ataków doprowadziło do zaszyfrowania danych

Koszt przywrócenia działania

$2.73M

średni koszt przywrócenia sprawności po ataku

Czas przywrócenia działania

34%

organizacji potrzebowało ponad miesiąca, aby odzyskać sprawność po atakach

Źródło: The State of Ransomware 2024 – Sophos, Addressing the cybersecurity skills shortage in SMBs - Sophos

SOPHOS

Jak przeprowadzane są ataki ransomware?

Root cause

32%

ataków rozpoczęło się od wykorzystania **luki w zabezpieczeniach**

"You had an old critical **Log4j vulnerability** not fixed on Horizon, this is how we were able to get in initially.

It was a bulk scanning; not like we were targeting you intentionally."

Gang ransomware atakujący kanadyjską organizację edukacyjną

Źródło: The State of Ransomware 2024 – Sophos

SOPHOS

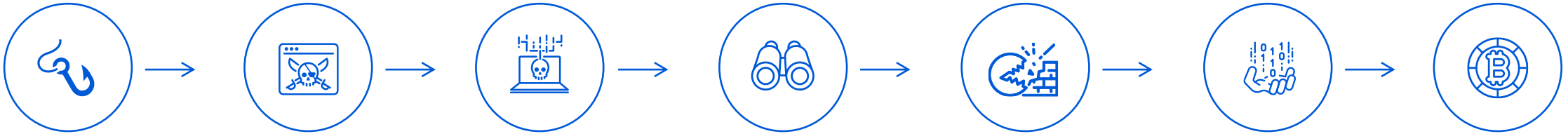
Przykładowy atak ransomware

59% organizacji zostało **zaatakowanych przez ransomware** w 2023 r.

94% ofiar stwierdziło, że ich **kopie zapasowe** były celem

32% ataków na zaszyfrowane dane wiązało się również z ich **kradzieżą**

$2.0M Mediana **zapłaconego okupu**



91% ataków rozpoczęło się **poza normalnymi godzinami pracy**

57% prób infekcji zakończyło się powodzeniem

70% ataków doprowadziły do **zaszyfrowania danych**

56% ofiar **zapłaciło okup**

Źródło: The State of Ransomware 2024 – Sophos, Stopping Active Adversaries: Lessons From The Cyber Frontline- Sophos

SOPHOS

Podstawowe procedury IT chroniące przed oprogramowaniem ransomware

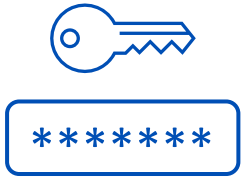
SOPHOS

Podstawowe procedury IT chroniące przed oprogramowaniem ransomware

Patch early, patch often

Wykorzystane luki w oprogramowaniu są **główną** przyczyną ataków ransomware.
Im wcześniej wprowadzisz poprawki, **tym mniej luk** będą mogli wykorzystać przeciwnicy.

Używaj menadżerów haseł i twórz silne hasła



Menedżer haseł ułatwiający zarządzanie hasłami

Hasła powinny być **unikalne** i składać się z co najmniej **12 znaków.**

Enable MFA

MFA dodaje **kluczową warstwę** zabezpieczeń poza pierwszym kluczem, aby **zablokować nieautoryzowany dostęp**.

Używaj odpornych na **phishing passkeys**, jeśli są dostępne.

Regulate network access

Zabezpiecz porty sieciowe, **blokując RDP** i inne protokoły zdalnego zarządzania.

Używaj **ZTNA** lub **VPN** do zdalnego dostępu dla użytkowników

CERT - Kompleksowo o hasłach

CERT - Rekomendacje techniczne CERT Polska dla systemów uwierzytelniania

SOPHOS

Podstawowe procedury IT chroniące przed oprogramowaniem ransomware

Monitoruj uprawnienia administratorów

Stale sprawdzaj uprawnienia administratorów i usuwaj **zbędne dostępy.**

Nie pozostawaj zalogowany jako administrator dłużej niż to konieczne.

Regularnie twórz kopie zapasowe danych i ćwicz ich przywracanie

Regularnie twórz kopie zapasowe danych w wielu lokalizacjach

Przeprowadzaj **testy przywracania** w celu płynnego odzyskiwania danych.

Usuwaj zbędne aplikacje

Cyberprzestępcy **wykorzystują popularne aplikacje** w taktyce zwanej living-off-the-land

Instaluj tylko aplikacje niezbędne do pracy użytkownika; **w razie wątpliwości pomiń je.**

Znajdź niezabezpieczone urządzenia w sieci

Cyberprzestępcy atakują niezabezpieczone urządzenia, **aby pozostać niezauważonymi.**

Te niezabezpieczone urządzenia mogą zostać wykorzystane do **przeprowadzenia szerszego ataku**

SOPHOS

Najlepsze praktyki w zakresie ochrony punktów końcowych

SOPHOS

1. Włącz wszystkie zalecane polityki i funkcje

Włącz zalecane polityki i funkcje

Regularnie sprawdzaj, czy wszystkie **opcje ochrony** są **włączone.**

Włącz funkcje wykrywające ataki **„bezplikowe”** i **nietypowe zachowania.**

Rekomendacje

Włącz ochrona przed manipulacją (temper Protection)

Zapobiega dokonaniu nieautoryzowanej modyfikacji lub usunięciu oprogramowania do ochrony punktów końcowych

Włącz rejestrowanie danych logowania (do chmury)

Zachowuj zapisy aktywności, aby zrozumieć ataki i zapobiegać ich ponownemu wystąpieniu, nawet jeśli przeciwnicy wyczyszczą dzienniki.

Zadbaj o regularne aktualizacje produktów

Aktualizuj produkty zabezpieczające, aby chronić się przed ewoluującymi zagrożeniami. Wyłączenie aktualizacji z czasem osłabia ochronę.

2. Regularnie sprawdzaj wykluczenia

Regularnie sprawdzaj wykluczenia

Wykluczenia ograniczają skanowanie zaufanych plików, zmniejszając opóźnienia i fałszywe alarmy, ale mogą stwarzać **zagrożenie dla bezpieczeństwa**, umożliwiając złośliwemu oprogramowaniu **wykorzystywanie niezabezpieczonych obszarów**.

Rekomendacje

Usuń jak najwięcej wykluczeń, jak to tylko możliwe

Regularnie sprawdzaj listę wykluczeń w ustawieniach polityk, usuwając wszelkie niepotrzebne wykluczenia w celu zwiększenia bezpieczeństwa..

Upewnij się, że zachowane wyłączenia są jak najbardziej szczegółowe

Unikaj wykluczania całych dysków lub katalogów; zamiast tego celuj w pojedyncze pliki według ich pełnych ścieżek.

3. Włącz MFA dla konsoli zarządzania zabezpieczeniami

Włącz MFA dla konsoli zarządzania zabezpieczeniami

Zapewnia to bezpieczny dostęp do platformy, która zarządza ochroną punktów końcowych i innymi kontrolami bezpieczeństwa. Uniemożliwia to atakującym zmianę lub wyłączenie ustawień ochrony.

4. Utrzymywanie dobrych praktyk i higieny IT

Utrzymywanie dobrych praktyk i higieny IT

Ocena stanu infrastruktury IT gwarantuje, że punkty końcowe i zainstalowane oprogramowanie działają efektywnie.

Zmniejsza to ryzyko związane z cyberbezpieczeństwem.

Rekomendacje

Wdrożenie programu utrzymania i zarządzania higieną IT

Na przykład upewnij się, że protokół RDP **działa tylko tam, gdzie jest potrzebny** i oczekiwany, **regularnie sprawdzaj problemy z konfiguracją**, monitoruj **wydajność urządzeń** i usuwaj **niechciane lub niepotrzebne** programy.

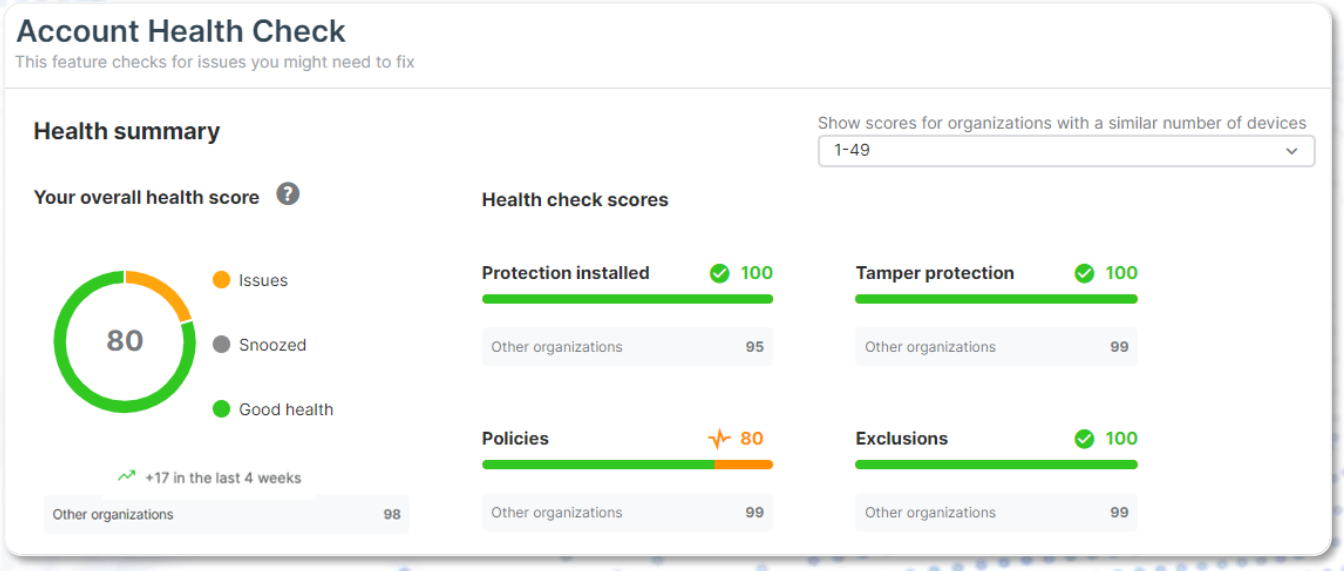
Kontrola stanu infrastruktury IT może wykazać potrzebę aktualizacji oprogramowania. Jest to również niezawodny sposób na zapewnienie regularnego tworzenia kopii zapasowych danych.

4. Utrzymywanie dobrych praktyk i higieny IT

Utrzymywanie dobrych praktyk i higieny IT

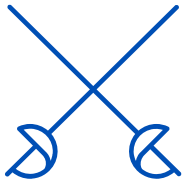
Ocena stanu infrastruktury IT gwarantuje, że punkty końcowe i zainstalowane oprogramowanie działają efektywnie.

Zmniejsza to ryzyko związane z cyberbezpieczeństwem.



5. Proaktywne wyszukiwanie aktywnych zagrożeń

Proaktywne wyszukiwanie aktywnych zagrożeń



Dzisiejsi cyberprzestępcy stosują taktykę ukrywania się, co sprawia, że **proaktywne wykrywanie zagrożeń** i szybkie działanie są niezbędne do ich powstrzymania.

Recommendations

Wykorzystanie technologii EDR / XDR

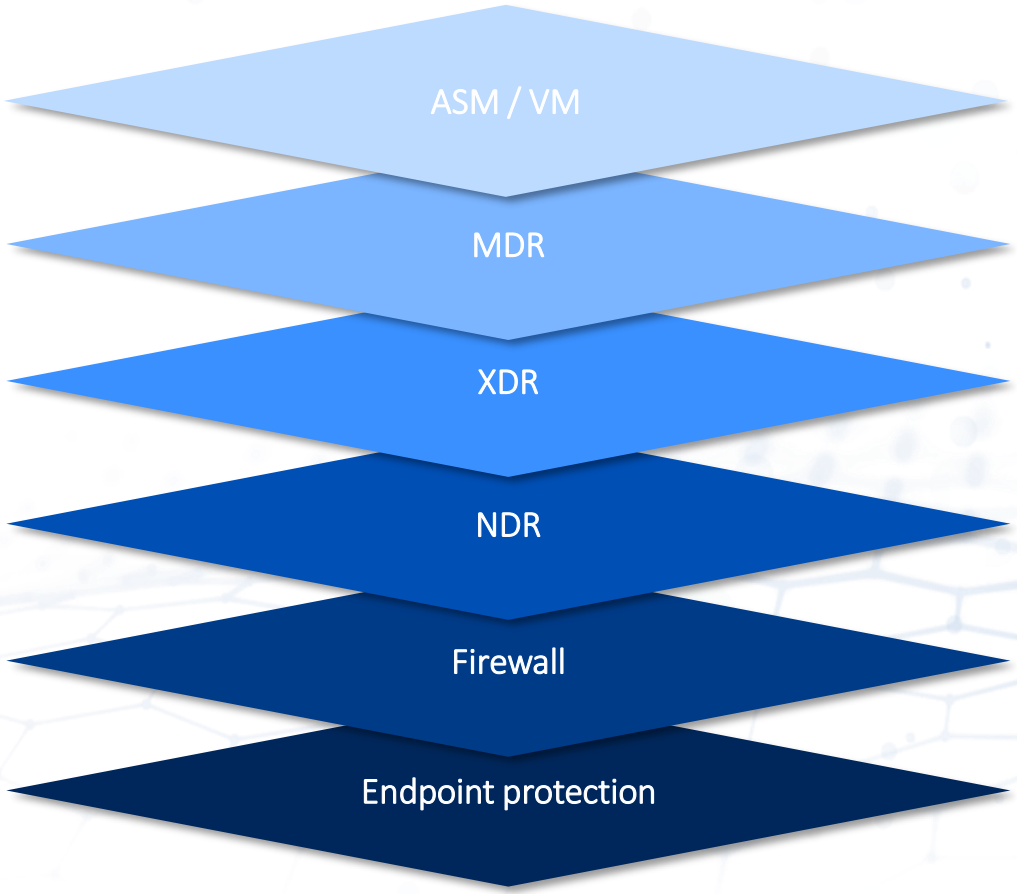
EDR i XDR zapewniają możliwości **wyszukiwania**, **badania** i **neutralizacji** zagrożeń dla **wewnętrznego** działu zajmującego się bezpieczeństwem.

Wykorzystanie usług MDR

Dostawcy usług MDR zapewniają **doświadczonych analityków bezpieczeństwa**, którzy **wyszukują** i **eliminują** zagrożenia **za Ciebie**. 24/7, 365 dni w roku.

Ochrona przed oprogramowaniem ransomware poprzez nakładanie warstw zabezpieczeń

Ochrona przed oprogramowaniem ransomware poprzez nakładanie warstw zabezpieczeń



Może być używany do identyfikacji i priorytetyzacji luk w zabezpieczeniach. Pozwala to zidentyfikować i zastosować brakujące poprawki, zanim atakujący będą mogli je wykorzystać.

Zapewnia całodobowe monitorowanie i wykrywanie zagrożeń przez ekspertów specjalizujących się w wykrywaniu i reagowaniu na cyberataki, którym same rozwiązania technologiczne nie są w stanie zapobiec.

Zapewnia wewnętrznemu zespołowi ds. bezpieczeństwa możliwości polowania na zagrożenia, prowadzenia dochodzeń i neutralizacji.

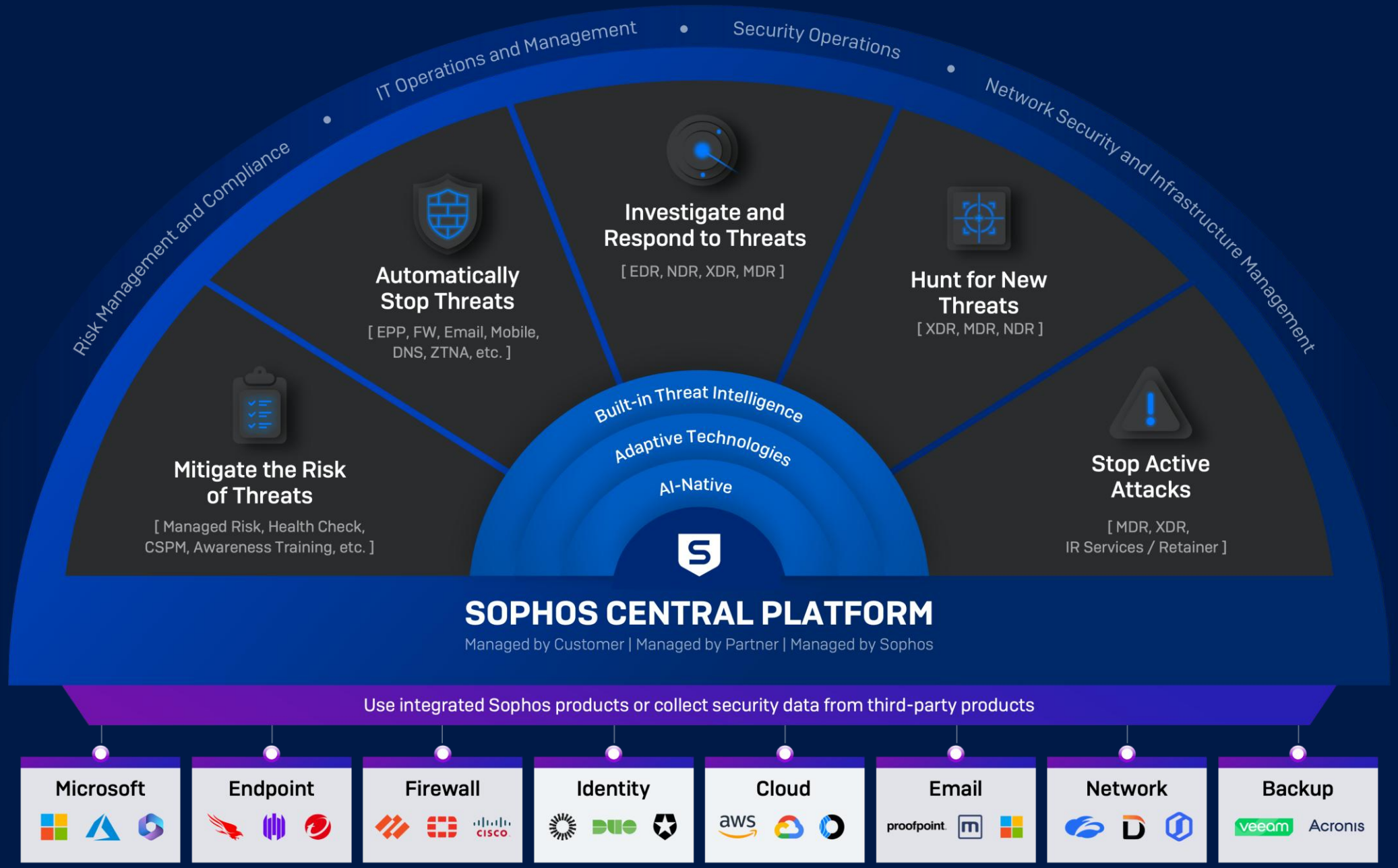
Wykrywa niezabezpieczone urządzenia i identyfikuje intruzów poruszających się w sieci.

Identyfikuje i blokuje podejrzany ruch sieciowy oraz zapobiega przedostawaniu się zagrożeń do środowiska.

SOPHOS

Jak Sophos może pomóc

SOPHOS


Risk Management and Compliance
IT Operations and Management
Security Operations
Network Security and Infrastructure Management
Mitigate the Risk of Threats
[Managed Risk, Health Check, CSPM, Awareness Training, etc.]
Automatically Stop Threats
[EPP, FW, Email, Mobile, DNS, ZTNA, etc.]
Investigate and Respond to Threats
[EDR, NDR, XDR, MDR]
Hunt for New Threats
[XDR, MDR, NDR]
Stop Active Attacks
[MDR, XDR, IR Services / Retainer]
Built-in Threat Intelligence
Adaptive Technologies
AI-Native
SOPHOS CENTRAL PLATFORM
Managed by Customer | Managed by Partner | Managed by Sophos
Use integrated Sophos products or collect security data from third-party products
Microsoft
Endpoint
Firewall
Identity
Cloud
Email
Network
Backup
aws
proofpoint
cisco
veeam
Acronis

SOPHOS

Dowiedz się więcej

Pobierz raport

Pobierz Raport
aby uzyskać głębszy wgląd w to, jak najlepiej skonfigurować rozwiązanie do ochrony urządzeń końcowych w celu zapewnienia optymalnej ochrony przed oprogramowaniem ransomware.

SOPHOS