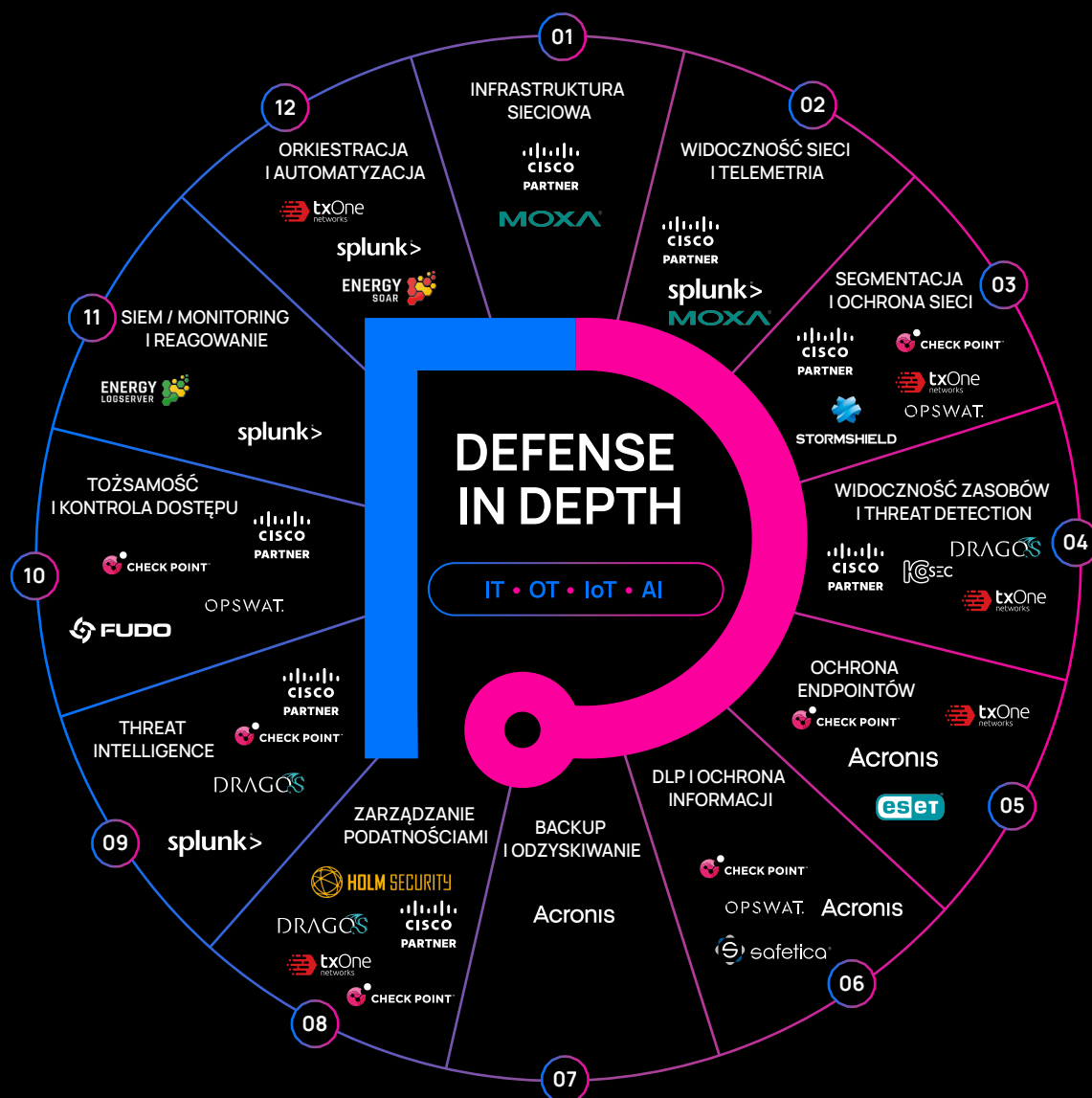


Budujemy cyberodporność operacji krytycznych, przemysłowych i biznesowych od IT do OT.



OCHRONA
I WIDOCZNOŚĆ OT



BEZPIECZEŃSTWO
IoT



CYBERODPORNOŚĆ
IT



PRZEGLĄDY
TECHNICZNE



WSPARCIE
INŻYNIERYJNE IT I OT

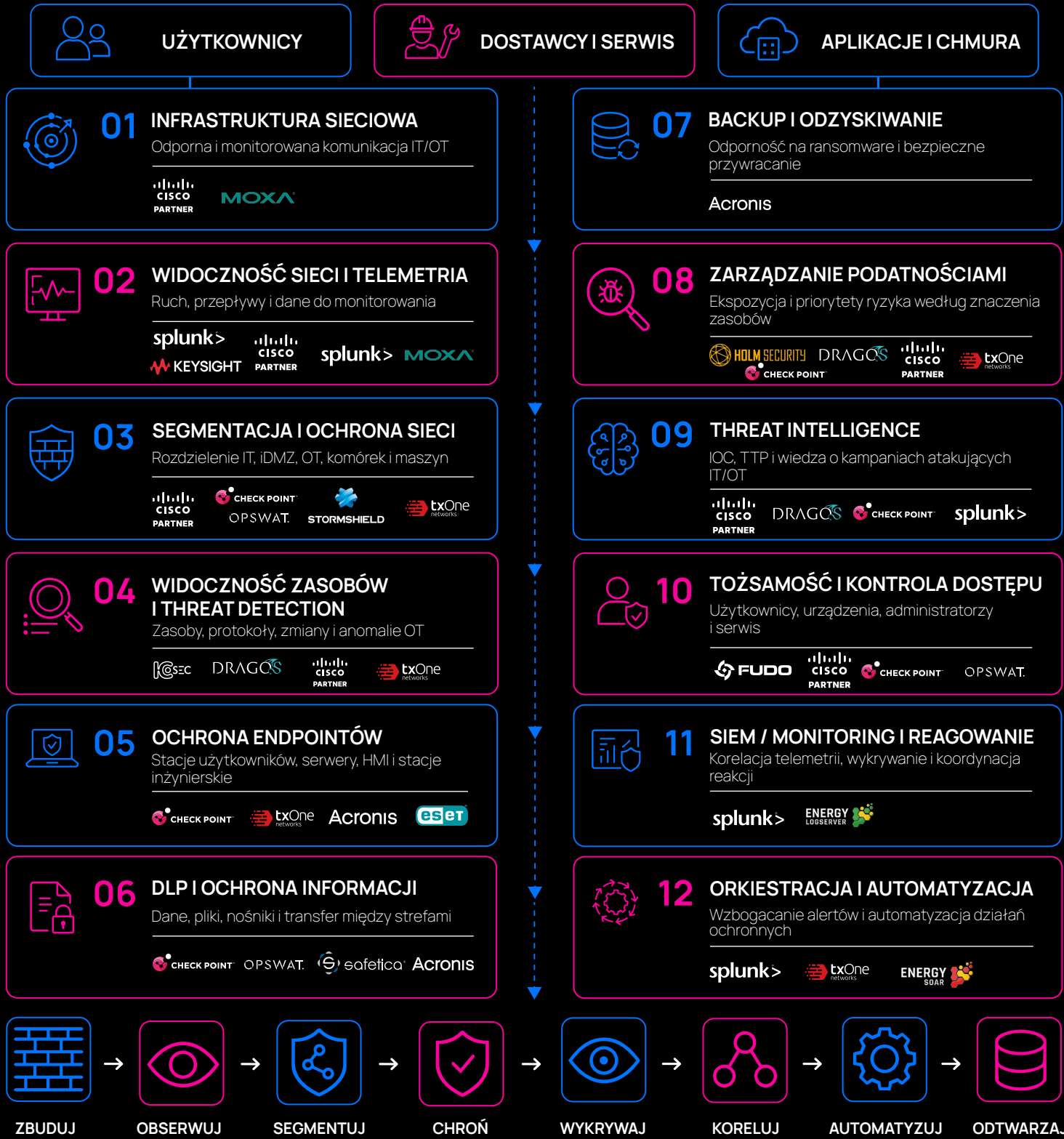


SZKOLENIA
I ĆWICZENIA

Spokojne podejście. • Praktyczne bezpieczeństwo. • Partnerska współpraca.

12 WARSTW OCHRONY IT/OT

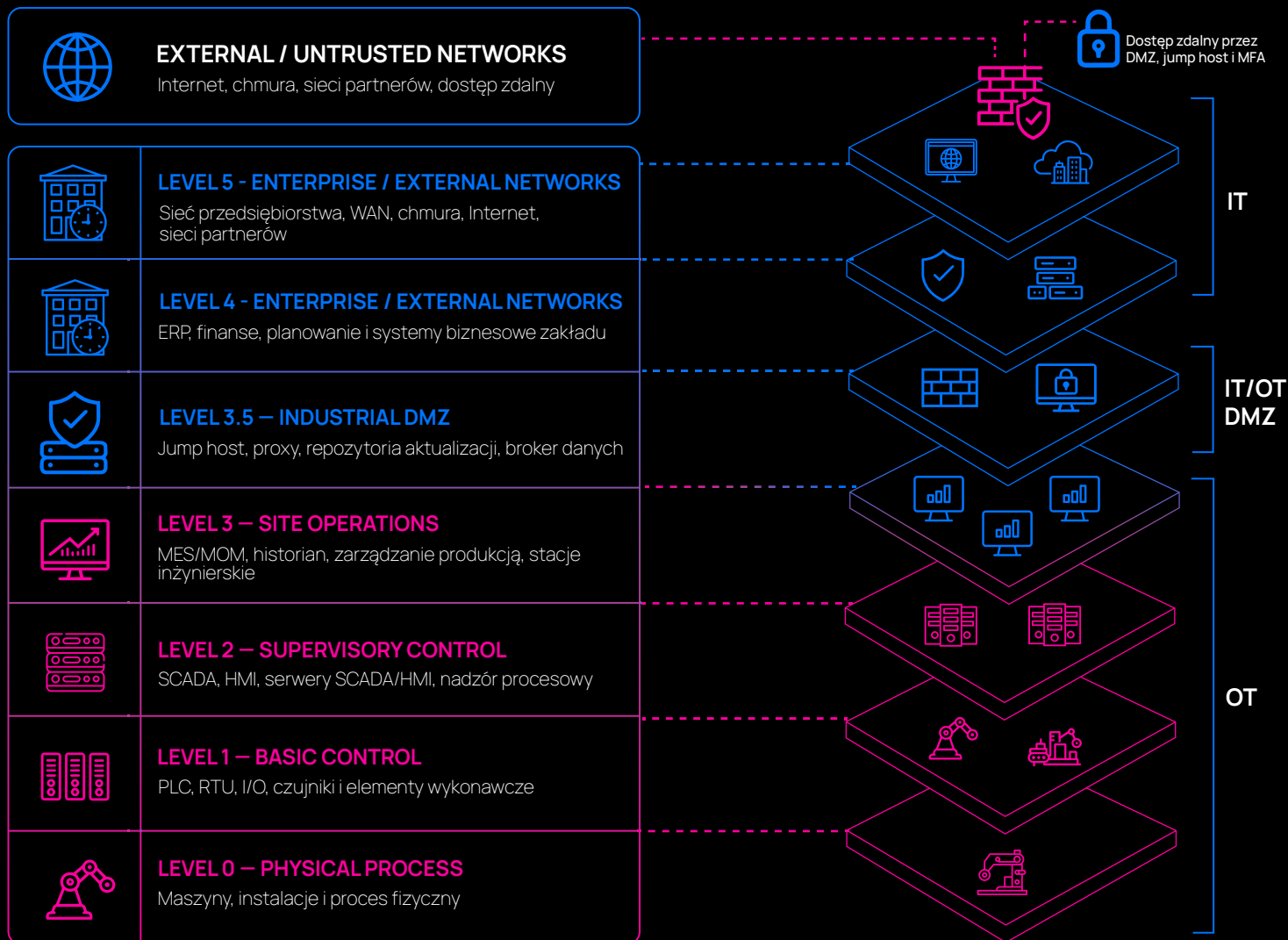
Jeden spójny system: od infrastruktury i widoczności po reakcję, automatyzację i odtwarzanie



MODEL PURDUE'A

SEGMENTACJA IT/OT, KTÓRA OGRANICZA ZASIĘG INCYDENTU

Model Purdue porządkuje środowisko przemysłowe na warstwy i pomaga kontrolować komunikację między IT i OT.



KLUCZOWE ZASADY SEGMENTACJI



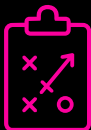
SPRAWDŹ SEGMENTACJĘ SWOJEJ SIECI IT/OT

Umów konsultację z ekspertem **BEZDRAM**



USŁUGI – ZAKRES I ZASTOSOWANIE

Szczegółowy zakres usług eksperckich i szkoleń dla środowisk ICS/OT

WARSTWA	PRODUCENT / PRODUKTY I USŁUGI	ZAKRES FUNKCJONALNY I ZASTOSOWANIE
 PRZEGLĄD ARCHITEKTURY	Dragos Architecture Review Suite	Ocena architektury OT, zabezpieczeń, konfiguracji i zgodności regulacyjnej. Identyfikuje luki oraz dostarcza priorytetyzowane rekomendacje dotyczące ochrony, detekcji i reagowania.
 TESTOWANIE ŚRODOWISK OT	Dragos Red Team Services (Network Vulnerability Assessment, Penetration Testing, Purple Team Exercises)	Testowanie zabezpieczeń środowisk OT poprzez ocenę podatności, testy penetracyjne oraz ćwiczenia Purple Team. Pozwala identyfikować ścieżki ataku i weryfikować skuteczność kontroli.
 ĆWICZENIA TABLETOP	Dragos Tabletop Exercises – CyberTop	Symulowane ćwiczenia testujące reagowanie na incydenty OT, komunikację i koordynację zespołów. Scenariusze mogą obejmować ransomware, insider threat oraz kompromitację łańcucha dostaw.
 SZKOLENIA ICS/OT	Dragos ICS/OT Cybersecurity Training • Dragos Academy	Szkolenia z architektury, technologii, protokołów i bezpieczeństwa ICS/OT. Obejmują ćwiczenia praktyczne z PLC, Modbus, analizy ruchu, skanowania, podatności, exploitation i OSINT.
 OCENA GOTOWOŚCI NA INCYDENTY OT	Dragos Threat Baseline	Warsztat identyfikujący wiarygodne scenariusze zagrożeń OT na podstawie rzeczywistych incydentów. Wspiera priorytetyzację ryzyka, inwestycji, detekcji i planów reagowania.
 PLANOWANIE REAGOWANIA NA INCYDENTY OT	Dragos IRP Workshop	Warsztat służący opracowaniu lub aktualizacji planu reagowania na incydenty OT. Obejmuje ocenę dojrzałości, scenariuszowe playbooki oraz rekomendacje rozwoju zdolności reagowania.
 WSPARCIE W REAGOWANIU NA INCYDENTY OT (24/7)	Dragos Rapid Response Retainer	Całodobowy dostęp do ekspertów reagowania na incydenty OT, uzgodnione warunki współpracy, warsztat wdrożeniowy oraz priorytetowe rozpoczęcie działań.
 REAGOWANIE NA INCYDENTY OT	Dragos OT Incident Response Services	Zdalne i realizowane na miejscu wsparcie podczas incydentów przemysłowych. Obejmuje analizę forensic, odtworzenie przebiegu ataku oraz rekomendacje dotyczące ograniczenia, usunięcia zagrożenia i przywrócenia operacji.

USŁUGI DLA BEZPIECZEŃSTWA OT

Od oceny odporności po reagowanie na incydenty i rozwój kompetencji



ZAKRES USŁUG



OCENA RYZYKA
I PODATNOŚCI



IDENTYFIKACJA
ŚCIEŻEK ATAKU



REKOMENDACJE
I PLAN DZIAŁAŃ



WERYFIKACJA KONTROLI
I SKUTECZNOŚCI



ROZWÓJ KOMPETENCJI
I DOJRZAŁOŚCI



NASZE PODEJŚCIE

Od bezpiecznej architektury po ciągłe monitorowanie i doskonalenie

BEZDRAM

CYBERBEZPIECZEŃSTWO BEZ DRAMATU

PREVENT

B

BUILD

Projektujemy bezpieczną architekturę dopasowaną do procesów i ryzyka.



E

ENABLE

Łączymy bezpieczeństwo z technologią, ludźmi i procesami.



Z

ZERO TRUST

Ograniczamy dostęp zgodnie z zasadą minimalnych uprawnień.



D

DETECT

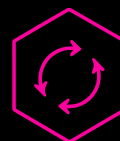
Zapewniamy widoczność i szybkie wykrywanie zagrożeń.



R

RESPOND

Ograniczamy skutki incydentów i przywracamy ciągłość działania.



A

ASSURE

Weryfikujemy zgodność z NIS2, IEC 62443, ISO 27001 i NIST CSF.



M

MAINTAIN

Monitorujemy, testujemy i stale doskonalimy zabezpieczenia.



PROTECT & IMPROVE

NASI PARTNERZY TECHNOLOGICZNI



OPSWAT



CHRONIMY ŚRODOWISKA IT, OT/ICS I INFRASTRUKTURĘ KRYTYCZNĄ

Umów konsultację bezpieczeństwa ↓

BEZDRAM

tel. +48 504 297 222

cyber@bezdrum.pl

www.bezdrum.pl

EKOSYSTEM OCHRONY PLIKÓW I POCZTY

Kontrolowana wymiana danych między Internetem, środowiskiem IT i strefą OT

STREFA 01:
INTERNET I APLIKACJE

STREFA 02
PRZETWARZANIE I TRANSFER IT

STREFA 03
CHRONIONE ŚRODOWISKO OT / ICS

01 KONTROLA PLIKU NA WEJŚCIU

ICAP SERVER + ICAP CLOUD

Kontrola przesyłania i pobierania bez przebudowy aplikacji



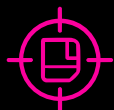
ICAP SERVER - ON-PREMISES

WAF, proxy, load balancer, SWG, SSL inspector i MFT i Multiscanning i Deep CDR™ i Proactive DLP™ i Adaptive Sandbox

ICAP CLOUD - USŁUGA ZARZĄDZANA

Skalowanie, wysoka dostępność i prywatne przetwarzanie i mTLS, RBAC i regiony wdrożeniowe wspierające suwerenność danych

02 ANALIZA, SANITYZACJA I WERDYKT



METADEFENDER CORE + SANDBOX

Zaufanie do pliku przed wykonaniem

- Metascan™: do 30+ silników AV*
- Deep CDR™: rekonstrukcja 200+ formatów*
- Proactive DLP™ oraz File-Based Vulnerability Assessment
- polityki, API, ICAP, SDK i automatyzacja



METADEFENDER EMAIL SECURITY

Ochrona poczty przed phishingiem i malware

- ON-PREM: Email Gateway Security
MTA / Transport Rules • do 30 silników AV
- CLOUD: MICROSOFT 365
ochrona poczty Microsoft 365 bez infrastruktury on-prem
- Multiscanning • Deep CDR™ • Sandbox

WIELOWARSTWOWA OCHRONA POCZTY PRZED DOSTARCZENIEM

03 TRANSFER PRZEZ GRANICE ZAUFANIA



MANAGED FILE TRANSFER

Bezpieczna wymiana plików IT / OT

- inspekcja i sanitizacja przed dostawą
- szyfrowanie w tranzycie i spoczynku
- RBAC, MFA i wieloetapowa akceptacja
- trasowanie, harmonogramy, orkiestracja i audyt



OPTICAL DIODE

Sprzętowo wymuszony jeden kierunek

- brak routowalnej ścieżki zwrotnej
- pełne zerwanie protokołu (transmisja wyłącznie danych użytkowych)
- redundancja optyczna i wysoka dostępność
- 1U: 100 Mb/s–1 Gb/s; opcja 10 Gb/s*
- DIN Rail: warianty do 50 Mb/s*

04 OSTATNI PUNKT KONTROLI PRZED OT

KIOSK + MEDIA VALIDATION

Skanowanie, sanitizacja i zatwierdzanie mediów wymiennych



KIOSK DESKTOP 4

17 000+ plików/min* i USB-A/C, SD, microSD
i wersja desktop lub montaż ścienny

KIOSK MOBILE 4

0 500+ plików/min* i utwardzony system,
obsługa w rękawicach i wzmocniona
konstrukcja, IP65

MEDIA VALIDATION AGENT

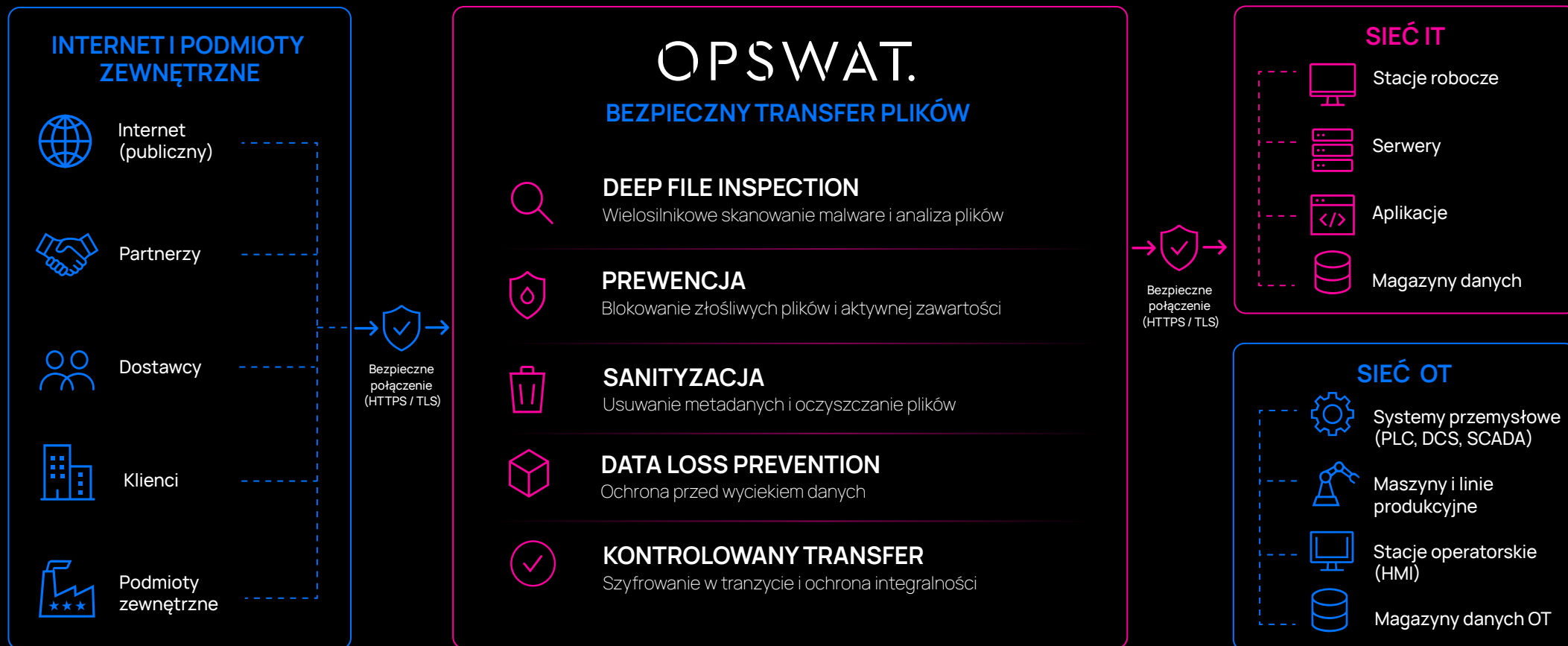
weryfikuje podpisany manifest i porównuje
hashe zatwierdzonych plików i blokuje
media zmienione lub nieskanowane

PLIK JEST WERYFIKOWANY, SANITYZOWANY I KONTROLOWANY NA KAŻDEJ GRANICY

* Parametry zależą od modelu, konfiguracji i licencji. Wartości według aktualnych kart produktowych OPSWAT.

BEZPIECZNY PRZEPŁYW PLIKÓW

Zanim przekroczą granicę Internet-IT i IT-OT.



BLOKOWANIE ZAGROZEŃ

Malware i aktywna zawartość



KONTROLOWANY TRANSFER

Granica IT/OT i pełny audyt



MONITORING I INTEGRACJA

Alerty oraz SIEM/SOAR

