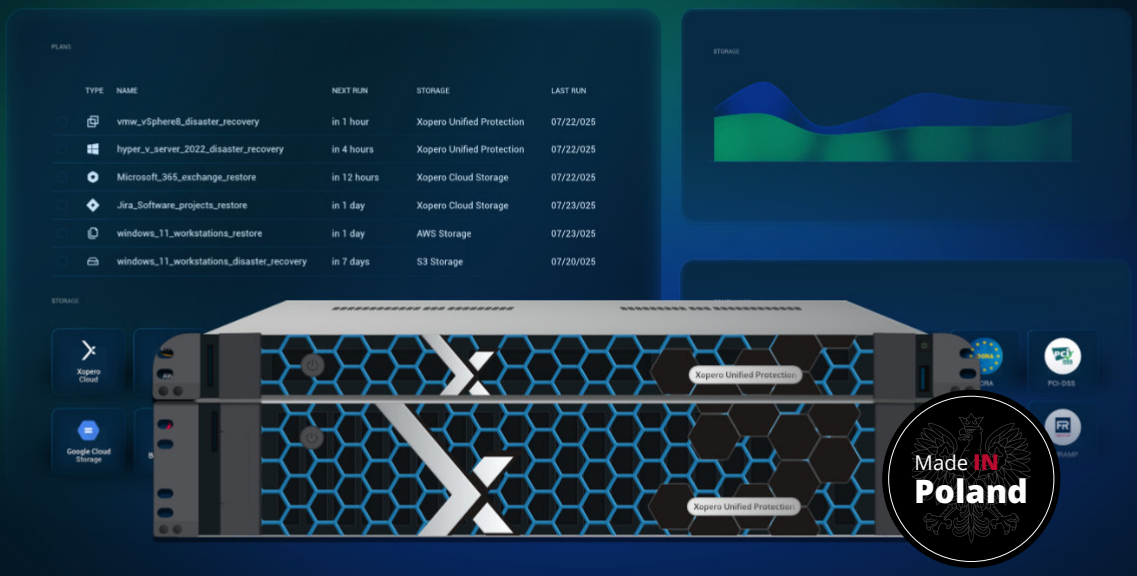
XOPERO
Unified Protection



Xopero Unified Protection dla sektora obronnego

Zintegrowany system ochrony danych z funkcjami zachowania ciągłości działania i odzyskiwania po cyberincydencie (BCDR). Stworzony z myślą o krytycznych infrastrukturach i sektorze militarnym.

Backup Appliance All-In-ONE

Model Plug&Play

Backup odporny na ransomware

Zabezpieczenie krytycznej infrastruktury IT

Najważniejsze korzyści

Wielofunkcyjne rozwiązanie

W Xopero Unified Protection kopie są kompresowane i szyfrowane, a na magazynie zapisywane w formie niewykonywalnej. Oznacza to, że nawet jeśli ransomware trafi w pliki znajdujące się w kopii zapasowej, dane te nie będą mogły zostać wykonane w pamięci masowej, a ransomware nie rozprzestrzeni się na magazynie.

Model Plug&play

W Xopero Unified Protection możesz dodać dowolną ilość magazynów danych - chmurowych, lokalnych, czy kolejnych urządzeń XUP, w tym w innej lokalizacji. Zapewnij zgodność z wytycznymi dzięki georedundancji i replikacji do dowolnych magazynów. W przypadku awarii lub ataku na jeden z magazynów, przywrócisz aktualną kopię z kolejnego.

Ciągłość działania i odzyskiwanie po awarii

Air gap backup to najbezpieczniejsza forma przechowywania danych, gdzie fizyczne odcięcie od sieci tworzy barierę niemożliwą do złamania. To rozwiązanie zostało zaprojektowane w celu neutralizacji zagrożeń klasy APT czy wyrafinowanych ataków cybernetycznych na krytyczną infrastrukturę.

Centralne zarządzanie

Dane uwierzytelniające są wysyłane agentowi tylko w momencie wykonywania kopii zapasowej. Nawet jeśli maszyna źródłowa zostanie zainfekowana, przestępcy nie będę mieli możliwości uzyskania dostępu do magazynu.

Sprawne działanie w sieciach DMZ

Xopero Unified Protection zapewnia maksymalne bezpieczeństwo danych poprzez izolowanie ich w strefie zdemilitaryzowanej (DMZ) w modelu “air-gapped”. Replikuj dane do strefy replikacji fizycznie odciętej od sieci i niedostępnej dla ransomware i innych zagrożeń.

Zgodność z regulacjami prawnymi i standardami

Xopero Unified Protection zostało zaprojektowane z myślą o wymaganiach UE/US i spełnia wymogi regulacyjne, takie jak NIS2, znowelizowana ustawa o Krajowym Systemie Cyberbezpieczeństwa czy RODO. Firma posiada także certyfikaty ISO 27001 oraz SOC 2 Type II.

Cyberbezpieczeństwo jako priorytet

Szyfrowanie AES kluczem prywatnym, który wykorzystywany jest wyłącznie na czas wykonywania kopii i uniemożliwia jej odszyfrowanie osobom trzecim.

Xopero Zero Trust Approach - chroniony dostęp do kopii i magazynów. Eliminuje ryzyko nieautoryzowanego dostępu i eskalacji uprawnień.

Role-based access control, czyli możliwość przypisywania ról i nadawania uprawnień - pełna kontrola i elastyczność zarządzania.

Nielimitowana retencja (długoterminowe przechowywanie kopii zapasowych, możliwość odtworzenia kopii z dowolnego momentu w czasie, nawet sprzed lat).

Bezpieczna autoryzacja oraz **manager haseł** ograniczają ryzyko przejęcia dostępu do kopii czy magazynu.

Architektura No single point of failure minimalizuje ryzyko pojedynczego punktu awarii.

Zabezpieczane środowiska



XOPERO UNIFIED PROTECTION DLA SEKTORA OBRONNEGO

Ransomware protection - gotowe na każdy scenariusz

Polska jest jednym z najczęściej atakowanych państw w sieci. W 2025 roku Wojska Obrony Cyberprzestrzeni odparły ponad 5 tysięcy incydentów w sieciach wojskowych.

Neutralizacja ataków ransomware

W Xopero Unified Protection kopie są kompresowane i szyfrowane, a na magazynie zapisywane w formie niewykonywalnej. Oznacza to, że nawet jeśli ransomware trafi w pliki znajdujące się w kopii zapasowej, dane te nie będą mogły zostać wykonane w pamięci masowej, a ransomware nie rozprzestrzeni się na magazynie.

Multi-storage, replikacja, skalowalność

W Xopero Unified Protection możesz dodać dowolną ilość magazynów danych - chmurowych, lokalnych, czy kolejnych urządzeń XUP, w tym w innej lokalizacji. Zapewnij zgodność z wytycznymi dzięki georedundancji i replikacji do dowolnych magazynów. W przypadku awarii lub ataku na jeden z magazynów, przywrócisz aktualną kopię z kolejnego.

Technologia Air Grap Backup

Air gap backup to najbezpieczniejsza forma przechowywania danych, gdzie fizyczne odcięcie od sieci tworzy barierę niemożliwą do złamania. To rozwiązanie zostało zaprojektowane w celu neutralizacji zagrożeń klasy APT czy wyrafinowanych ataków cybernetycznych na krytyczną infrastrukturę.

Chroniony dostęp z Zero Trust Approach

Dane uwierzytelniające są wysyłane agentowi tylko w momencie wykonywania kopii zapasowej. Nawet jeśli maszyna źródłowa zostanie zainfekowana, przestępcy nie będę mieli możliwości uzyskania dostępu do magazynu.

Zachowaj ciągłość działania operacyjnego

Wróć do działania po awarii lub ataku ransomware bez konieczności odbudowy od zera.

- Odtwarzaj systemy i dane na inny sprzęt i do innego środowiska, także zdalnie w trybie Bare Metal, aby odzyskać sprawność mimo zmian w infrastrukturze.
- Przywracaj tylko potrzebne pliki i foldery, kiedy liczy się czas i nie chcesz odzyskiwać całej maszyny (z dowolnego momentu w czasie, nawet sprzed lat).
- Planuj testowe odtworzenia i otrzymuj raporty, żeby mieć dowód odtwarzalności i znać realny czas przywrócenia oraz dopuszczalną utratę danych (RTO/RPO).

Pakiet dodatkowych usług

Asysta wdrożeniowa

Producent dostarczy urządzenie i wdroży je kompleksowo we wskazanym przez Ciebie miejscu. Zapewni także późniejsze wsparcie techniczne i obsługę w języku polskim.

Dokumentacja powdrożeniowa

Po zakończeniu wdrożenia otrzymasz skróconą dokumentację na potrzeby audytów bezpieczeństwa oraz kontroli wewnętrznej.

Konsultacje techniczne

Po miesiącu produkcyjnej pracy systemu możesz skorzystać z darmowej konsultacji, a specjaliści Xopero wyjaśnią, jak optymalnie dopasować system do potrzeb Twojej organizacji.

Wymiana urządzenia

Po utrzymaniu wsparcia technicznego przez 5 lat i przy jego odnowieniu na co najmniej 1 rok, otrzymasz nowe urządzenie z możliwością zachowania poprzedniego.

Nielimitowane licencje

W cenie urządzenia chronisz dowolną liczbę maszyn, bez licencjonowania per komputer. Rozbudowujesz tylko storage i wydajność, gdy tego potrzebujesz.

Automatyczne aktualizacje

Zawsze aktualne, automatycznie aktualizowane wersje oprogramowania bez konieczności ręcznej instalacji.

Gwarancja NBD onsite

W przypadku awarii sprzętu zgłoszonej do wsparcia technicznego, technik przeprowadza zdalną diagnostykę, a serwisant przyjeżdża na miejsce w następnym dniu roboczym z potrzebnymi częściami i dokonuje naprawy.

Xopero wzmacnia cybersuwerenność Polski

Xopero Software S.A. to polski producent rozwiązań do ochrony danych i cyberbezpieczeństwa oparty w 100% na rodzimym kapitale. Jako zaufany partner instytucji państwowych uczestniczy w krajowych i europejskich inicjatywach w zakresie cyberbezpieczeństwa i suwerenności cyfrowej.

PWCyber: Program Współpracy w Cyberbezpieczeństwie realizowany przez Ministra Cyfryzacji

Współpraca obejmuje udział w projektach i doradztwo w zakresie analizy zagrożeń, reagowania na incydenty i zabezpieczeń cyfrowych wzmacniających odporność na cyberzagrożenia.

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland

Xopero Software jest jednym ze współwłaścicieli klastra integrującego przedsiębiorstwa z sektora prywatnego z nauką, administracją publiczną i partnerami międzynarodowymi.

Platforma ta tworzy warunki do budowy bezpiecznej, suwerennej i konkurencyjnej cyberprzestrzeni opartej na polskich rozwiązaniach.

Program Partnerstwo dla Cyberbezpieczeństwa NASK

Z inicjatywy NASK-PIB i Ministerstwa Cyfryzacji skupia podmioty KSC w celu rozwoju narzędzi i procedur zwiększających bezpieczeństwo strategicznych systemów IT w Polsce. Xopero Software współpracuje z organizacjami biorącymi udział w programie na rzecz wzmocnienia infrastruktury ochrony danych dla administracji publicznej i sektora prywatnego RP.

European Cyber Security Organisation (ECSO)

Xopero Software jest członkiem ECSO - ponadnarodowej, organizacji, która działa jako kluczowa platforma współpracy między sektorem prywatnym a publicznym w celu wzmocnienia cyberbezpieczeństwa w Unii Europejskiej.

Dlaczego Xopero Software?

- **Polska firma**, zaufany partner instytucji państwowych.
- **Aktywne wsparcie dla krajowych inicjatyw** w zakresie cyberbezpieczeństwa.
- Współpraca z kluczowymi podmiotami w celu **wzmocnienia odporności cyfrowej Polski**.

XOPERO Backup&Recovery PWCyber #CyberMadeInPoland PdK NASK ECS EUROPEAN CYBER SECURITY ORGANISATION

XOPERO
Unified Protection

Organizacje, które zadbały o bezpieczeństwo swoich danych z Xopero Software



























Więcej informacji na Xopero.com