XOPERO
Backup&Recovery

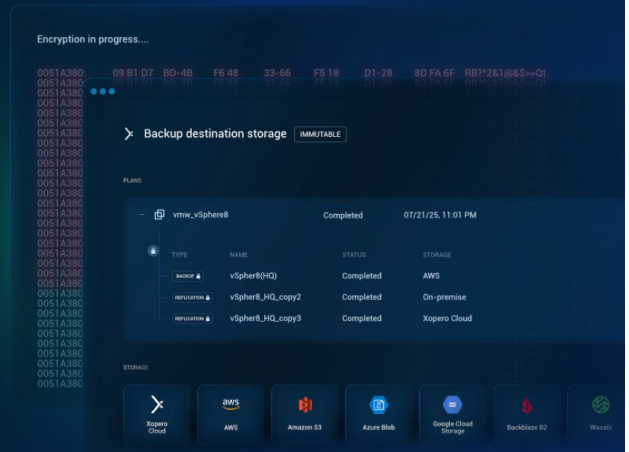
# Jak Xopero wspiera realizację wymagań DORA

## Backup, recovery i ciągłość działania dla sektora finansowego



XOPERO
Backup&Recovery

# Backup i recovery jako kluczowy element operacyjnej odporności cyfrowej




Unijne rozporządzenie DORA trwale zmieniło podejście do cyberbezpieczeństwa w sektorze finansowym.

Dziś nie chodzi już wyłącznie o ochronę danych. Kluczowa jest zdolność organizacji do utrzymania ciągłości działania mimo poważnych zakłóceń, awarii i cyberataków.

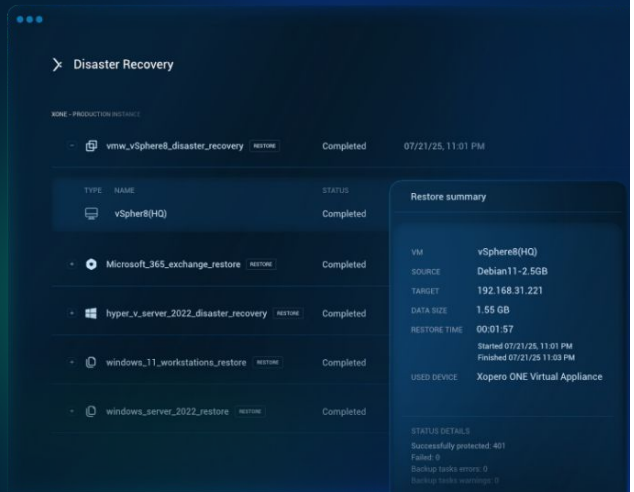
Dlatego szczególnego znaczenia nabrały obszary, które można regularnie testować i dokumentować:

- odtwarzalność kopii zapasowych,
- separacja backupu od środowiska produkcyjnego,
- integralność i dostępność danych,
- odzyskiwanie danych i usług w wymaganym czasie,
- ciągłość działania po incydencie.

To właśnie w tych punktach Xopero zapewnia organizacjom finansowym najmocniejsze wsparcie.

XOPERO
Backup&Recovery

# Atuty Xopero we wspieraniu realizacji wymagań DORA




Xopero oferuje **zaawansowane rozwiązanie klasy enterprise do backupu i disaster recovery: Xopero Unified Protection (XUP).**

**Centralne zarządzanie**
Jedna platforma zamiast wielu narzędzi upraszcza zarządzanie backupem, recovery i nadzorem operacyjnym.

**Przejście od backupu do gotowości odtworzeniowej**
Połączenie backupu z gotowym systemem BCDR wspiera ciągłość działania i ogranicza skutki incydentów.

**Integralność, izolacja i odporność kopii**
Wsparcie dla ochrony i odzyskiwania danych, także w przypadku ataku ransomware lub awarii.

**Gotowość do audytów i kontroli**
Centralny monitoring, logi i raporty dostarczają dowodów na właściwy stan zabezpieczeń i możliwość odtworzenia kopii.

# Jak Xopero wspiera wymagania związane z backupem i odzyskiwaniem danych?

| Wymaganie DORA | W czym pomaga Xopero? | Przydatne funkcjonalności XUP |
|---|---|---|
| Art. 12, polityki backupu i recovery | Wspiera spójne zarządzanie kopiami, retencją i odzyskiwaniem danych dla wielu środowisk w ramach jednej platformy łączącej sprzęt i oprogramowanie (XUP). | • backup oparty na politykach<br>• zaawansowane schematy backupu<br>• retencja i wersjonowanie |
| Art 12.2, regularne testowanie backupu i odtwarzania | Umożliwia regularne sprawdzanie nie tylko, czy kopie są przechowywane, lecz czy można je rzeczywiście odtworzyć. | • testowe przywracanie<br>• raporty<br>• zaawansowany monitoring z powiadomieniami |
| Art 12.3, fizyczna i logiczna separacja backupu od produkcji | Zapewnia izolację kopii od środowiska produkcyjnego i ogranicza ryzyko wspólnej awarii lub propagacji ataku. | • Air Gap<br>• multi-storage (nieograniczona liczba magazynów)<br>• replikacja<br>• niezależne magazyny |
| Art 12.6, odzyskiwanie danych i usług w odpowiednim czasie | Zapewnia szybkie odzyskiwanie danych i środowisk po awarii lub ataku ransomware. | • Instant Disaster Recovery<br>• Any2Any Restore<br>• Bare Metal Restore<br>• granularne przywracanie |
| Art 12.7, integralność i poufność danych przy odtwarzaniu | Chroni kopie przed zmianą, usunięciem i nieuprawnionym dostępem. | • immutable storage/WORM<br>• szyfrowanie AES kluczem prywatnym<br>• ograniczenia dostępu<br>• podejście Zero Trust |

# Jak Xopero wspiera realizację wymagań związanych z ciągłością działania?

| Wymaganie DORA | W czym pomaga Xopero? | Przydatne funkcjonalności XUP |
|---|---|---|
| Art. 11.4, utrzymywanie i okresowe testowanie planów ciągłości ICT | Wspiera techniczną warstwę planów ciągłości i recovery przez odtwarzanie środowisk, testy i centralne zarządzanie procesem odtworzeniowym. | • gotowy system BCDR<br>• centralna konsola<br>• testowe przywracanie |
| Art 11.5, redundancja dla komponentów krytycznych | Wspiera redundancję i odporność środowiska dzięki replikacji danych między niezależnymi magazynami oraz georedundancji. | • replikacja i georedundancja<br>• Xopero Cloud Storage<br>• multi-storage<br>• brak pojedynczego punktu awarii (SPOF) |
| Art 11.6, testy ciągłości działania, reagowania i przywracania sprawności | Ułatwia testowanie odtworzenia i pomiar gotowości odtworzeniowej. | • testowe przywracanie<br>• raporty z testów<br>• pomiar RTO i RPO |
| Art 11.6, scenariusze przełączenia na kopie i zasoby redundantne | Wspiera scenariusze awaryjne oparte na kopiach, magazynach zapasowych i szybkim odtworzeniu po incydencie. | • backup na wielu storage'ach<br>• replikacja<br>• Disaster Recovery<br>• odtworzenie do nowego środowiska |

# Jak Xopero wspiera realizację wymagań w zakresie ochrony i zapobiegania?

| Wymóg DORA | W czym pomaga Xopero? | Przydatne funkcjonalności XUP |
|---|---|---|
| Art. 9.3b, minimalizacja ryzyka utraty danych | Chroni przed utratą danych dzięki wersjonowaniu, retencji, replikacji i wielu niezależnym kopiom. | • długoterminowa retencja<br>• przywracanie z konkretnego momentu w czasie<br>• multi-storage<br>• replikacja |
| Art. 9.3c, ochrona integralności i poufności danych | Chroni dane backupowe przed nieuprawnioną zmianą, usunięciem i dostępem. | • immutable storage/WORM<br>• role i uprawnienia<br>• Bezpieczny Manager Haseł<br>• wzmocnione mechanizmy autoryzacji |
| Art. 9.4b, ograniczanie rozprzestrzeniania się zagrożeń i izolacja | Wzmacnia separację warstwy backupowej i ogranicza skutki ataku ransomware dla magazynu kopii. | • Air Gap<br>• niewykonywalne pliki w kopii<br>• podejście Zero Trust<br>• ograniczony dostęp do danych uwierzytelniających magazynu |
| Art 9, ochrona i zapobieganie | Wzmacnia prewencyjną ochronę warstwy danych przez połączenie szyfrowania, niezmienności kopii i kontroli dostępu. | • szyfrowanie AES w spoczynku i w trakcie transmisji<br>• immutable storage/WORM<br>• gotowy system RBAC<br>• centralne zarządzanie |

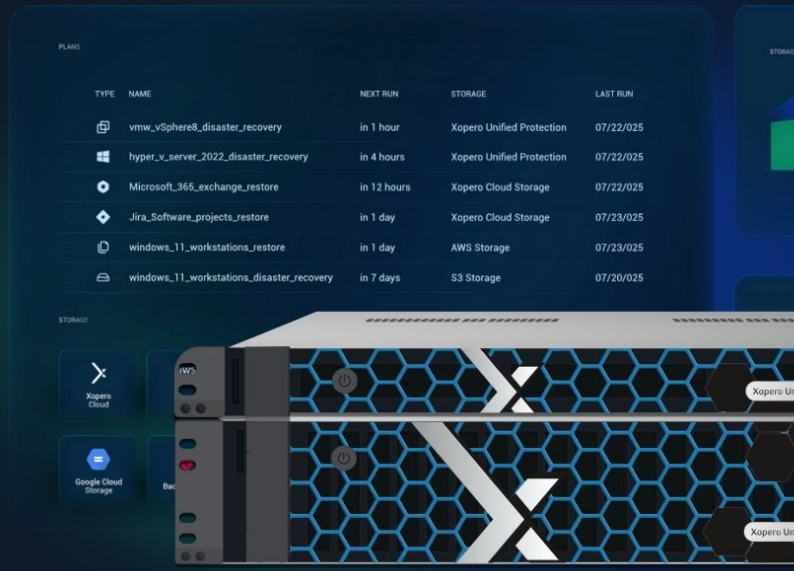
# Porozmawiajmy o architekturze backupu i recovery w kontekście DORA

Xopero Software S.A. to polska firma współpracująca z instytucjami publicznymi.

Nasze rozwiązania projektujemy z myślą o spełnieniu wymagań regulacyjnych UE, w tym DORA, NIS2 i RODO. Firma posiada certyfikaty ISO 27001 oraz SOC 2 Type II.

**Sprawdź, jak Xopero ułatwi Twojej organizacji dostosowanie do wymogów DORA.**

Umów demo




*Materiał ten ma charakter ogólny i informacyjny. Nie stanowi analizy prawnej ani potwierdzenia pełnej zgodności z DORA. Ocena zgodności wymaga uwzględnienia specyfiki organizacji, procesów, środowiska ICT oraz obowiązków regulacyjnych.*