SafeDR | Backup & Disaster Recovery

I-BS.PL

Ciągłość działania systemów IT.

Backup, który przywraca środowiska — nie tylko dane.

Linux | Windows | Proxmox | PostgreSQL

SafeDR to platforma *Disaster Recovery*, która nie zatrzymuje się na poziomie kopii danych. Backup jest tu częścią większego procesu — prowadzącego do uruchomienia środowiska gotowego do pracy.

System działa w modelu hybrydowym. Dane z Linuxa, udziałów sieciowych czy baz danych pobierane są bezpośrednio — bez instalacji oprogramowania. W środowiskach Windows lekki agent wykorzystujący VSS wykonuje pełne obrazy dysków i zabezpiecza je jeszcze przed wysyłką.

Całość tworzy jeden, spójny mechanizm — od pobrania danych po ich odtworzenie. Bez ręcznych działań, bez improwizacji, bez rozproszonych narzędzi.

W efekcie backup przestaje być celem samym w sobie. Staje się elementem procesu, który przywraca dostęp do systemów, aplikacji i pracy operacyjnej.

W praktyce oznacza to:

- → dane pozostają odseparowane od środowiska produkcyjnego,
- → kopie są zabezpieczone przed modyfikacją,
- → środowisko może zostać uruchomione bez odbudowy infrastruktury,
- → użytkownicy odzyskują dostęp do systemów i procesów,
- → proces odtworzenia jest cyklicznie testowany — automatyczne testy DR potwierdzają, że kopie działają, a klient otrzymuje certyfikat PDF dla audytora.

Szybki powrót do działania

Awaria nie kończy się na utracie danych. Zatrzymują się procesy, użytkownicy tracą dostęp do systemów, a organizacja traci kontrolę nad środowiskiem.

Dotyczy to różnych sytuacji — od ataku ransomware, przez awarię sprzętu, aż po zdarzenia fizyczne, które wyłączają całą infrastrukturę.

W każdej z nich kluczowe staje się nie tylko odzyskanie danych, ale szybkie przywrócenie działania całego środowiska.

SafeDR odpowiada na te scenariusze w sposób systemowy:

- → odtwarzanie danych bez ryzyka ich nadpisania lub utraty,
- → przywrócenie działania usług bez ręcznej odbudowy,
- → dostęp do środowiska niezależnie od stanu infrastruktury lokalnej,
- → kontrolowany i przewidywalny proces przywracania — bez improwizacji i ręcznych decyzji.

Scenariusze zastosowania SafeDR

Ransomware
Dane zostają zaszyfrowane, a systemy przestają działać. **SafeDR** umożliwia odtworzenie środowiska z niezmienialnych kopii, bez ryzyka nadpisania lub utraty danych.

Awaria sprzętu
Uszkodzenie serwera lub macierzy powoduje przerwę w dostępie do systemów.
SafeDR przywraca dane i usługi bez konieczności ręcznej odbudowy infrastruktury.

Katastrofa fizyczna
Utrata dostępu do lokalnej infrastruktury (np. pożar, zalanie, brak zasilania).
SafeDR zapewnia dostęp do kopii offsite i możliwość odtworzenia środowiska niezależnie od lokalizacji.

Błąd ludzki
Przypadkowe usunięcie danych, nadpisanie plików lub błędna zmiana konfiguracji.
SafeDR pozwala przywrócić wcześniejszy stan danych lub systemu bez ingerencji w pozostałe środowisko.

SafeDR | Backup & Disaster Recovery

Źródła danych i ich pozyskiwanie

SafeDR zbiera dane z różnych źródeł i przetwarza je w jednym, spójnym procesie — niezależnie od typu systemu czy technologii, co eliminuje konieczność stosowania różnych narzędzi, wyjątków konfiguracyjnych i ręcznych obejść.

Serwery Linux
Dostęp do plików i katalogów przez SSH — obsługa kopii pełnych i przyrostowych (rsync).

Udziały Windows
Dane z udziałów SMB/CIFS pliki, katalogi i dokumenty w środowisku Windows.

PostgreSQL
Spójne kopie baz danych z użyciem pg_dump — gotowe do odtworzenia.

Windows VSS
Pełna kopia systemu Windows w trakcie jego pracy — bez zatrzymywania usług.

Proxmox Backup Server
Maszyny wirtualne Proxmox VE — snapshoty wykonywane natywnie przez PBS, bez przestojów.

FortiGate
Konfiguracja firewalla (FortiOS) pobierana przez REST API globalnie lub per-VDOM.

MikroTik RouterOS
Eksport konfiguracji urządzeń RouterOS przez połączenie SSH pełne dane i parametry.

Cisco IOS / ASA
Kopie konfiguracji urządzeń (running i startup) przez SSH gotowe do odtworzenia.

Jeden spójny model odzyskiwania danych i systemów

SafeDR oddziela proces backupu od środowiska produkcyjnego i przenosi do kontrolowanego modelu, w którym dane są zabezpieczone już na etapie ich pobierania. Każdy etap — od pozyskania danych po ich zapis — odbywa się w jednym, spójnym procesie.

Dane są pobierane bez ingerencji w działanie systemów produkcyjnych, następnie zabezpieczane i zapisywane w odseparowanym repozytorium. W razie potrzeby mogą zostać odtworzone w sposób kontrolowany, bez konieczności ręcznej odbudowy infrastruktury.

Automatyzacja backupu i odtwarzania

Harmonogramowanie
Automatyczne planowanie zadań backupu z wizualnym podglądem. Codziennie, co tydzień lub według własnych reguł.

Testy odtworzeniowe
Automatyczne uruchamianie kopii w izolacji + weryfikacja boot. Certyfikat PDF dla audytora — DORA, NIS2, KNF.

Zarządzanie przestrzenią
Podgląd wykorzystania magazynu i kontrola retencji danych. Łatwe zarządzanie polityką przechowywania kopii.

Monitoring i logi
Status zadań w czasie rzeczywistym oraz szczegółowe logi każdego uruchomienia.

Przechowywanie danych — DyskDR

Dane są przechowywane w DyskDR — silniku backupu opartym na sprawdzonej technologii *Proxmox Backup Server*. Zapewnia to wysoką niezawodność, integralność danych oraz skalowalność rozwiązania. Wbudowane mechanizmy dbają o bezpieczeństwo i spójność danych, a także efektywne wykorzystanie przestrzeni.

Takie podejście upraszcza architekturę i zapewnia spójny sposób pracy z backupem i odtwarzaniem danych.

Efektywność

- → **Deduplikacja chunk-level**
  Powtarzalne fragmenty danych zapisywane są tylko raz.
- → **Kompresja zstd**
  Zmniejsza rozmiar danych bez wpływu na możliwość odtworzenia.

Spójność

- → **Weryfikacja integralności**
  System kontroluje poprawność danych w repozytorium.
- → **Niezmienialność snapshotów**
  Kopie nie mogą zostać nadpisane ani zmodyfikowane.

Dostępność

- → **Replikacja PBS → PBS**
  Możliwość utrzymania kopii w wielu lokalizacjach.
- → **Dostępność kopii**
  Kopie pozostają dostępne niezależnie od stanu środowiska produkcyjnego.

Bezpieczeństwo danych

SafeDR zabezpiecza dane na każdym etapie — od pobrania po przechowywanie i odtworzenie. Dostęp do kopii jest kontrolowany, a ich treść pozostaje niedostępna bez odpowiednich kluczy.

Szyfrowanie danych	Dane są szyfrowane przed transferem i przechowywane wyłącznie w formie zaszyfrowanej. Chroni dane niezależnie od miejsca ich przechowywania.
Integralność danych	Każda kopia podlega weryfikacji integralności na poziomie repozytorium. Zapewnia spójność i możliwość odtworzenia.
Klucz RSA po stronie klienta	Klucz prywatny pozostaje wyłącznie po stronie klienta i nie jest przechowywany w systemie. Zapewnia pełną kontrolę nad dostępem do kopii.
Izolacja klientów	Dane klientów są logicznie odseparowane w repozytorium. Zapewnia bezpieczeństwo w środowisku współdzielonym.
Zero-knowledge	Dane są szyfrowane po stronie klienta i trafiają do repozytorium już jako zaszyfrowane. Brak dostępu do danych po stronie dostawcy.

Nadzór i kontrola dostępu

Powiadomienia e-mail
Alerty o błędach, sukcesach i dostępnej przestrzeni. Konfigurowalne progi powiadomień.

Raporty PDF
Automatyczne raporty (tygodniowe lub miesięczne) z załącznikiem PDF.

LDAP / Active Directory
Integracja logowania z katalogiem firmowym (LDAP / Active Directory).

Role i uprawnienia
Dostęp do funkcji przypisywany według ról — kontrola, kto może wykonywać operacje backupu, odtwarzania i konfiguracji.

SafeDR vs. klasyczny backup

Obszar	Klasyczny backup	SafeDR
model działania	agenty na serwerach	model hybrydowy
złożoność wdrożenia i utrzymania	konfiguracja i aktualizacje na wielu hostach	jedna centralna konfiguracja, brak agentów
wpływ na systemy produkcyjne	obciążenie serwerów produkcyjnych	brak ingerencji w systemy produkcyjne
zarządzanie	rozproszone	centralne w jednym panelu
zakres backupu	pliki lub wybrane systemy	pliki, bazy danych, VM, systemy Windows
odtwarzanie	ręczne, wieloetapowe	szybkie przywrócenie
disaster recovery	ograniczone lub dodatkowe narzędzia	wbudowane + cykliczne testy odtwarzania z certyfikatem PDF dla audytora
integralność danych	brak gwarancji niezmienialności kopii	niezmienialność snapshotów + weryfikacja integralności
skalowalność	rozbudowa wymaga dodatkowej konfiguracji	łatwe skalowanie wraz ze wzrostem danych
efekt biznesowy	zabezpieczenie danych	zabezpieczenie danych + ciągłość działania

Decyzja o backupie to również decyzja biznesowa

SafeDR może działać lokalnie, w modelu hybrydowym lub w pełni offsite — w zależności od wymagań i poziomu kontroli nad danymi. Pozwala to dopasować wariant do tych wymagań — bez kompromisów między bezpieczeństwem, czasem przywrócenia i kosztami.

Najważniejsze pytania, które warto zadać

- → Jak szybko musimy przywrócić działanie po awarii?
- → Czy dane mogą być przechowywane poza organizacją?
- → Jaki poziom kontroli nad infrastrukturą i miejscem przechowywania danych jest wymagany?
- → Kiedy ostatnio testowaliśmy odtwarzanie kopii i czy mamy dokument dla audytora?

Co zmienia SafeDR

- → Przewidywalny i krótszy czas odtworzenia.
- → Dane pozostają pod kontrolą organizacji.
- → Kontrola nad danymi i środowiskiem dopasowana do wymagań regulacyjnych.
- → Potwierdzona skuteczność kopii dzięki automatycznym testom odtwarzania.

Poznaj pozostałe rozwiązania z rodziny Safe

SafeConnect

Dostęp uprzywilejowany pod pełną kontrolą.
www.i-bs.pl/safeconnect

SafeGuard

Kontrola dostępu do sieci i komunikacji między zasobami.
www.i-bs.pl/safeguard

I-BS.PL

www.i-bs.pl/safedr

Chcesz dowiedzieć się więcej o rozwiązaniu?
Skontaktuj się z nami — odpowiemy na pytania i przedstawimy szczegóły oferty.

Joanna Stępień
tel.: 788 679 946
j.stepien@i-bs.pl

Bartłomiej Skoczylas
tel.: 728 403 586
b.skoczylas@i-bs.pl