EMEA

# Ochrona danych w środowiskach multicloud

Środowiska multicloud – cyber odporność w złożonych środowiskach

Rosnąca popularność wykorzystania chmur publicznych zaowocowała wzrostem wyzwań w obszarze ochrony danych przed cyberatakami. Organizacje, które stale modernizują proces ochrony danych, znacznie minimalizują ryzyko związane z ich utratą, a tym samym zwiększają swoją gwarancję bezpieczeństwa.

## Obawy czy system ochrony danych jest skuteczny – są niestety bardzo powszechne

**64%** badanych obawia się, że doświadczy incydentu naruszenia bezpieczeństwa w ciągu kolejnych 12 miesięcy

**$1.24m** to średni koszt utraty danych w ciągu ostatnich 12 miesięcy

**63%** badanych obawia się, że istniejące metody ochrony danych w ich organizacjach są niewystarczające do ochrony przed malware i ransomware

**72%** badanych uważa, że brak rozwiązań do ochrony nowych technologii takich jak konteneryzacja, aplikacje cloud-native, IoT, to jedno z pięciu najważniejszych wyzwań, jakie pojawią się przed ich organizacjami w najbliższym czasie

## Wraz ze wzrostem adopcji chmury publicznej rosną obawy związane z odpowiednią ochroną danych

**76%** respondentów korzystających z chmury hybrydowej lub publicznej podczas aktualizacji lub wdrażania aplikacji nie jest pewna czy ich organizacja może skutecznie chronić wszystkie swoje dane w chmurach publicznych

**57%** respondentów postrzega możliwość ochrony wielu workloadów (maszyny wirtualne, kontenery, aplikacje cloud-native) zdeponowanych na platformach on premise i w chmurach publicznych jako najważniejszą cechę środowisk hybrydowych

## Cyber zagrożenia pozostają na pierwszym miejscu priorytetów w organizacjach każdej wielkości

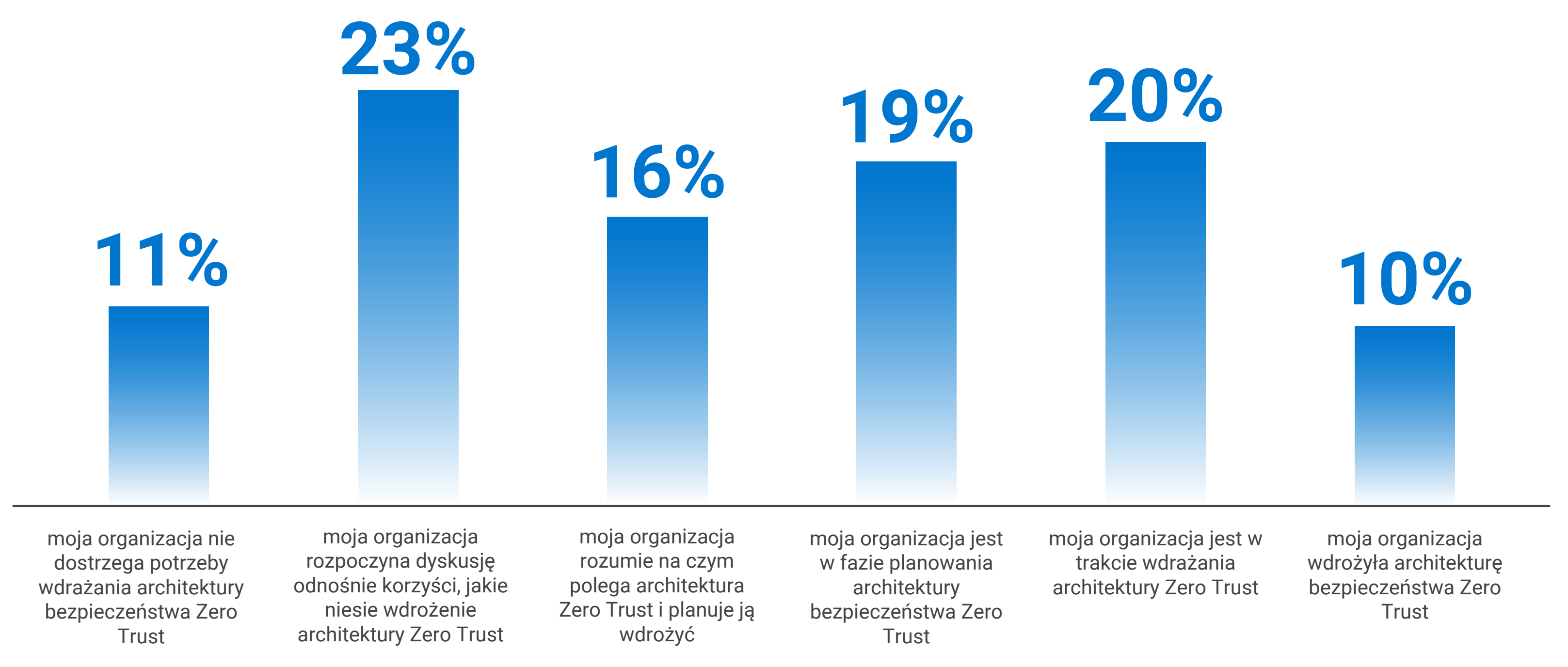
**67%** badanych nie jest pewna czy wszystkie krytyczne dla biznesu dane można skutecznie odzyskać po ewentualnym cyberataku

**48%** respondentów zgłosiło, że padło celem cyberataku lub innego incydentu naruszenia bezpieczeństwa, który uniemożliwił dostęp do danych firmowych w ciągu ostatnich 12 miesięcy

**60%** respondentów twierdzi, że atak miał miejsce spoza sieci organizacji

**69%** badanych przyznaje, że ich organizacja jest narażona na większą utratę danych wraz ze wzrostem liczby pracowników pracujących z domu

## Chociaż wiele organizacji rozumie potrzebę i wdraża lub planuje wdrażać architekturę Zero Trust, wciąż niewiele przedsiębiorstw może się pochwalić działającymi rozwiązaniami



## Rozwiązania as-a-service to często najprostsza operacyjnie opcja w obszarze wdrażania rozwiązań zabezpieczania danych

3 priorytety rozwiązań as-a-service:

- Storage
- Cyber bezpieczeństwo
- Disaster recovery

## Mniejsza liczba dostawców w obszarze rozwiązań ochrony danych to uproszczenie procesu ich wdrażania

**90%** badanych zabezpieczających swoje dane za pomocą rozwiązań kilku dostawców uważa, że obniżyłoby koszty i uprościło działalność operacyjną redukując liczbę wykorzystywanych rozwiązań

## Jak organizacje mogą zoptymalizować proces ochrony danych w czasie transformacji cyfrowej?

- Zmodernizuj swój system ochrony danych
- Zredukuj nakład pracy związany z wdrożeniem i utrzymaniem systemu
- Zwiększ odporność organizacji na cyber ataki

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

**Metodologia**

Badanie przeprowadzone przez Vanson Bourne między sierpniem a październikiem 2022 r. Respondentami byli decydenci IT zarówno z firm prywatnych, jak i organizacji rządowych zatrudniających ponad 250 pracowników. W badaniu wzięło udział łącznie 1000 respondentów z czterech regionów – 200 z obu Ameryk (USA, Meksyk i Brazylia), 450 z EMEA (Wielka Brytania, Francja, Niemcy, Włochy, RPA i Zjednoczone Emiraty Arabskie), 250 z APJ (Australia, Indie, Japonia, Singapur i Korei Południowej) oraz 100 z Chin.

Commissioned by Dell Technologies

DELL Technologies

VansonBourne