IDC Executive Brief

# OCHRONA I ZARZĄDZANIE DANYMI W ERZE TRANSFORMACJI CYFROWEJ.

Czy model Backup as a Service (Baas) odpowiada na potrzeby organizacji segmentu Midmarket?

**Autor:** Jarek Smulski,
**Przygotowany we współpracy z:**
Netia, Commvault

*Luty 2022 r.*

IDC

# Ochrona i zarządzanie danymi w erze transformacji cyfrowej.

## Czy model Backup as a Service (Baas) odpowiada na potrzeby organizacji segmentu Midmarket?

IDC Executive Brief

February, 2022 r.

***Autor:*** *Jarek Smulski*

***Przygotowany we współpracy z:*** NETIA COMMVAULT

# I. Kluczowe znaczenie danych w transformacji cyfrowej

Transformacja cyfrowa spowodowała, że dane zostały postawione w centrum uwagi osób zarządzających firmami, stając się jednym z najważniejszych aktywów nowoczesnych organizacji ery cyfrowej. Ataki ransomware, które powodowały brak dostępności do posiadanych danych czy systemów informatycznych, wykazały jasno, że nawet firmy w doskonałej kondycji finansowej nie mogą poprawnie funkcjonować po takim ataku, co może doprowadzić do ich wyeliminowania z rynku. Ale dane to nie tylko ciągłość działania, to także, a może przede wszystkim, przewaga konkurencyjna i lepsze możliwości dostosowywania się do zmieniających okoliczności.

Hasła "transformacja cyfrowa" czy "gospodarka oparta o dane" już na dobre rozgościły się w sektorze Enterprise, czyli wśród dużych firm zatrudniających powyżej 1000 pracowników. Nawet sektor przemysłowy, mocno reprezentowany wśród największych przedsiębiorstw, coraz śmielej wdraża rozwiązania informatyczne zbierające, magazynujące i przetwarzające posiadane dane. Trend ten powoli spływa też na mniejsze organizacje, zatrudniające od 250 do 999 pracowników, często określane nazwą Midmarket. Ze względu na skalę działania, zrozumiałe jest, że ich działy czy budżety IT są mniejsze, niż u większych firm, co nie musi jednak automatycznie oznaczać, że stosowane rozwiązania IT są mnie rozwinięte czy przestarzałe.

We wrześniu 2021 roku IDC przeprowadziło badanie wśród przedstawicieli segmentu Midmarket w Polsce. Organizacje reprezentowały w całości sektor biznesowy; nie badano sektora publicznego. Celem tego badania było sprawdzenie, w jakim stopniu ta grupa respondentów jest przygotowana do funkcjonowania w cyfrowej gospodarce opartej o dane, jakie są z tym związane wyzwania oraz jaka jest świadomość i wiedza na temat zarządzania i zabezpieczania danych wśród osób za to odpowiedzialnych.

# II. Co gryzie statystycznego administratora danych?

Analizując wszystkie odpowiedzi na pytania ankiety, można wywnioskować, że poważnym wyzwaniem jest ciągle stosunkowo niska świadomość biznesu i osób zarządzających na temat istotności danych we współczesnej gospodarce. Przekłada się to na fakt, że znakomita większość badanych firm (aż 77,5%) nie ma dedykowanego budżetu na ochronę danych, najczęściej stanowi on jakąś część całego budżetu na wszystkie projekty IT. Oznacza to, że inwestycję w ochronę danych mają najczęściej incydentalny i reaktywny charakter; są odpowiedzią na to, co już się wydarzyło. Respondenci proszeni o oszacowanie rocznych wydatków na środowisko backupowe, z uwzględnieniem kosztów pracy administratora, licencji, serwerowni, sprzętu i oprogramowania, aż w 58% przypadków wybierali najniższy przedział, czyli „Mniej niż 24 000 zł". Co trzeci natomiast wybierał poziom od 24 do 48 tysięcy złotych. Potwierdza to tezę, że organizacje nie zatrudniają dedykowanych osób do zarządzania bezpieczeństwem danych a posiadana infrastruktura jest raczej skromna. Przy tak deklarowanej wysokości wydatków, model subskrypcyjny może się okazać odpowiedni rozwiązaniem, ponieważ pozwala uniknąć dużych inwestycji kapitałowych a dodatkowo rozwiązuje kwestię zatrudnienia albo wyszkolenia dedykowanego pracownika odpowiedzialnego za administrację danych.

Tymczasem aż w 90% przypadków firmy polegają na własnych zasobach. Kwestia bezpieczeństwa IT jest ciągle wymieniana jako największe wyzwanie dla organizacji IT, ale paradoksalnie najczęściej stosowaną metodą jest maksymalne odcięcie IT od zewnętrznych czynników, w tym również od usługodawców. Rodzi się jednak pytanie, czy firmy są w stanie same zapewnić ochronę danych; obszar IT dynamicznie zmieniający się, wymagający od administratorów ciągłych szkoleń i rozwoju?

> Kwestia bezpieczeństwa IT jest największym wyzwaniem dla organizacji IT, a najczęściej stosowana metoda ochrony danych, przechowywanie kopii bezpieczeństwa w swojej serwerowni, jest niewystarczająca. Ponadto ciągłe aktualizowanie kompetencji w obszarze bezpieczeństwa przy tak rosnącej skali zagrożeń jest dla wielu firm niemożliwe. Współpraca z usługodawcą pozwala natomiast przenieść ciężar zarządzania platformą backup na barki firmy zewnętrznej.

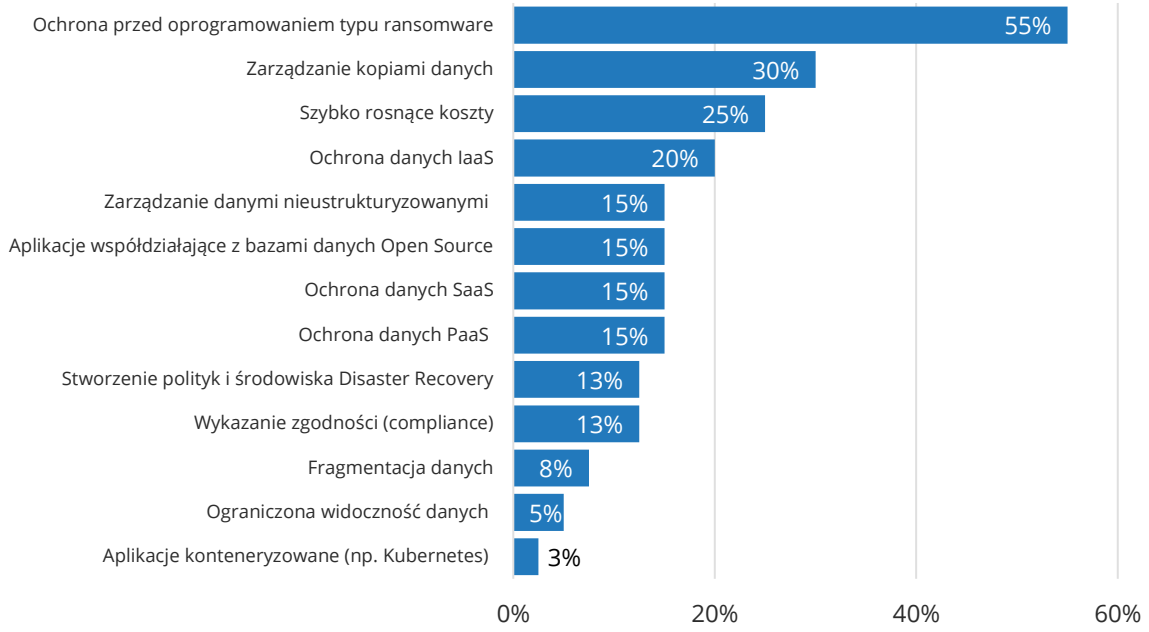
Liczba danych objętych polityką backupu i archiwizacji jest też stosunkowo niewielka. 59% respondentów wybrało przedział 10-19,9TB, a tylko blisko 13% – powyżej 20TB. Dane są więc często rozproszone, nieujednolicone, przypisane do różnych aplikacji. Ich lista natomiast szybko wydłuża się, podobnie jak obciążeń (workloadów). Ten proces nabrał tempa w czasie pandemii oraz wraz z upowszechnieniem się modelu pracy zdalnej. Oznacza to, że poziom komplikacji polityk backupu uległ zwielokrotnieniu. To nie tylko ogromne wyzwanie w administracji danych, ale utrudnia także ich analizę, ponieważ brakuje nam całościowych repozytoriów wszystkich informacji posiadanych przez daną organizację.

Wyzwania związane z zarządzaniem danymi należą do najbardziej istotnych w segmencie Midmarket, mimo tego, że wolumeny danych odbiegają znacząco od tych wymienianych przez administratorów w dużych organizacjach. Blisko 1/3 respondentów boryka się z problemami związanymi z kopiami danych, a po 15% badanych wskazało na zarządzanie danymi nieustrukturyzowanymi i aplikacje współdziałające z bazami danych Open Source.

Jednak hasłem powodującym zapalenie wszystkich czerwonych lampek ostrzegawczych aż u 55% badanych jest ransomware. Stosunkowo liczna jest też grupa respondentów zmagających się z zabezpieczaniem danych w chmurze. IDC szacuje, że ten odsetek będzie rósł w Polsce, w miarę jak będzie rósł odsetek użytkowników modeli aaS.

## Wykres 1: Ochrona przed ransomware jest największym wyzwaniem polskich organizacji Midmarket.

*W jakich obszarach w zakresie ochrony danych Państwa organizacja ma najwięcej wyzwań? Proszę wybrać maksymalnie 3 odpowiedzi.*




*Źródło: Badanie IDC "Backup as a Service – Data Protection w Polsce w 2021 r.", N = 40, wrzesień 2021 r.*

Ochrona danych jest nierozerwalnie związana z planowaniem ciągłości działania (Business Continuity Planning – BCP). Jakie zdarzenia stanowią największe zagrożenie dla realizacji procesów IT? Respondenci aż w 65% przypadków obawiają się działania siły wyższej – pożaru, powodzi czy huraganu, który zniszczy ich serwerownie. Połowa badanych przedstawicieli segmentu Midmarket wskazało także cyberatak; czy to w postaci ransomware czy też ataku hackerskiego typu DDoS, wirusa czy sabotażu pracowniczego. Także co drugi pytany wybrał awarię sprzętu lub oprogramowania. W dalszym ciągu spory odsetek wskazywał na awarię telekomunikacyjną czy brak zasilania – odpowiednio 43% i 40% odpowiedzi, mimo tego, że poziom usług firm telekomunikacyjnych czy dystrybutorów energii elektrycznych uległ znacznej poprawie. Nasuwa się więc pytanie, czy poleganie na jednym centrum przetwarzania danych jest racjonalną strategią? Oraz jaki jest najbardziej racjonalny model działania firm segmentu Midmarket, które z reguły nie mają środków na budowę ośrodka zapasowego?

Respondenci aż w 65% przypadków obawiają się działania siły wyższej – pożaru, powodzi czy huraganu, który zniszczy ich serwerownie. Nasuwa się więc pytanie, czy poleganie na jednym centrum przetwarzania danych jest racjonalną strategią?

## Wykres 2: Klęski żywiołowe i zdarzenia losowe stanowią największe zagrożenie dla realizacji podstawowych procesów IT

*Proszę wybrać trzy zdarzenia stanowiące największe zagrożenie dla realizacji podstawowych procesów IT Państwa firmy*


*Źródło: Badanie IDC "Backup as a Service – Data Protection w Polsce w 2021 r.", N = 40, wrzesień 2021 r.*

Ciekawe wyniki daje również analiza istotności systemów i procesów dla biznesu. Poczta korporacyjna, którą wskazało 60% respondentów, to zasób o znaczeniu krytycznym dla ciągłości biznesu. To nie tylko narzędzie do komunikacji, ale także repozytorium najważniejszych, osobistych informacji biznesowych (kontakty, kalendarz, pliki załączników, workflow). Połowa pytanych wybrało systemy ERP, co potwierdza trend, że są one niezbędne do funkcjonowania nowoczesnej organizacji w erze cyfrowej.

Badanie IDC rzuca też więcej światła na świadomość zagrożeń, posiadaną wiedzę oraz stosowane procedury. Co piąty respondent ignoruje podstawowe zasady polityki backupu i odtwarzania po awarii nie posiadając żadnego ośrodka zapasowego. Zasada 3-2-1 backupu, mówiąca m.in. o przechowywaniu danych w jednej lokalizacji zdalnej, jest stosowana przez 65% respondentów. Natomiast 15% organizacji stosuje backup w 3 fizycznych lokalizacjach (w tym w co najmniej jednej znajdują się systemy produkcyjne). Można więc zakładać, że znaczny odsetek tych organizacji stosuje backup w chmurze albo szerzej, w opcji usługi.

Osoby zajmujące się administracją danych, dużą wagę przywiązują do informacji, gdzie znajdują się ich dane. Z jednej strony 48% respondentów trzyma je wyłącznie we własnych serwerowniach, ale z drugiej aż 53% dopuszcza, aby dane były przechowywane w zdalnej lokalizacji, pod warunkiem jednak, że będzie znana fizyczna lokalizacja tej serwerowni. Te wyniki pokazują, że ta grupa badanych bardzo ostrożnie podchodzi do usług dużych, międzynarodowych dostawców chmury, dla których umiejscowienie danych ma zdecydowanie drugorzędne znaczenie.

53% respondentów dopuszcza, aby dane były przechowywane w zdalnej lokalizacji, pod warunkiem jednak, że będzie znana fizyczna lokalizacja tej serwerowni.

# III. Netia Data Protection – usługa BaaS łącząca globalne rozwiązania technologiczne i krajową lokalizację

Respondenci pytani o najważniejsze kryteria wyboru dostawcy usług BaaS czy DRaaS, aż w 78% przypadków wskazali, że oczekują bogatego portfolio usług. Bardzo istotne jest też dla nich jakość wsparcia oraz możliwość wskazania lokalizacji danych (odpowiednio 68% i 43% wskazań). Dopiero za tymi czynnikami jest elastyczność cenowa (wybrana przez 40% respondentów). Badane organizacje rozumieją, że budowa systemu backup wewnątrz organizacji-jest dużym wyzwaniem,-gdyż wiąże się z wytworzeniem trudnych do pozyskania kompetencji. Wybór modelu aaS pozwala zlikwidować tę lukę kompetencyjną. Co więcej uzyskują także dostęp do sprawdzonej technologii, platformy sprzętowej oraz odpowiedni poziom wsparcia. W ten sposób mogą znacząco zmniejszyć swój dług technologiczny i nadrobić zaległości w rozwoju systemów IT.

Wybór modelu aaS pozwala zlikwidować lukę kompetencyjną. Co więcej, klienci takich usług uzyskują także dostęp do sprawdzonej technologii, platformy sprzętowej oraz odpowiedni poziom wsparcia. W ten sposób mogą znacząco zmniejszyć swój dług technologiczny i nadrobić zaległości w rozwoju systemów IT.

Netia Data Protection to rozwiązanie typu Backup as a Service, oparte na technologii zarządzania i ochrony danych firmy Commvault. Zapewnia firmom utrzymanie ciągłości działania oraz odtworzenie danych z aplikacji, baz danych, środowisk wirtualnych, systemów plików po awarii czy ataku hackerskim. Łączy dobrze znaną i sprawdzoną technologię, z lokalnością, czyli umiejscowieniem serwerowni w Polsce, wsparciem przez wysokiej klasy administratorów danych posługujących się językiem polskim oraz z gwarancją wysokiej dostępności.

W chwili obecnej dostępne są cztery opcje usługi:

- **Backup.APP** – umożliwia wykonanie kopii zapasowej aplikacji, w tym baz danych,
- **Backup.vServer** – to kopia zapasowa środowiska wirtualnego i fizycznego
- **Backup.PLIK** – dedykowane rozwiązanie dla backupu systemu plików,
- **Backup.USER** – usługa zabezpieczająca dane użytkowników Microsoft 365, będąca odpowiedzią, na rosnące problemy pracowników zdalnych.

Standardowa polityka backupowa zakłada wykonywanie pełnej kopii danych raz w tygodniu a kopii przyrostowej raz dziennie oraz 30-dniową retencję danych. Użytkownicy mogą również zdefiniować indywidualną politykę poprzez intuicyjny panel użytkownika lub z pomocą inżynierów Netii[1].

Umiejscowienie usługi w Polsce dobrze odpowiada na sygnalizowaną w badaniu potrzebę identyfikacji miejsca przechowywania danych; jest też niezbędnym elementem wszystkich polityk backupu, w których

[1] Wszystkie informacje techniczne pochodzą ze strony *https://www.netia.pl/pl/srednie-i-duze-firmy/produkty/bezpieczenstwo/netia-data-protection* Dostęp: 2022.01.12

zasady narzucone przez regulatorów rynkowych wymagają, aby np. dane klientów nie opuszczały granic kraju.

Co jeszcze przemawia za usługowym modelem backupu? Przede wszystkim brak kosztownych inwestycji kapitałowych w celu stworzenia oraz utrzymania lokalnego systemu backupu i disaster recovery. Zgodnie z zasadą 3-2-1 usługa Netia Data Protection może być także właśnie tą trzecią lokalizacją danych, ostatnią, "złotą" kopią, która pozwoli odbudować organizację sparaliżowaną atakiem ransomware.

Firmy segmentu Midmarket mogą także dzięki takiej usłudze rozwiązać problem braku dedykowanej osoby do administracji danymi. Szacunki podparte m.in. zestawieniami przygotowanymi przez Komisję Europejską pokazują, że w Polsce brakuje blisko 50 tysięcy specjalistów IT. Dzieje się tak pomimo tego, że każdego roku studia informatyczne i pokrewne kończy prawie 14 tysięcy osób. Model usługowy pozwala więc, by to wyzwanie budowy własnych kompetencji administracji danych, chociaż częściowo przenieść na zewnętrzny podmiot.

Rosnąca popularność modeli usługowych w Polsce, przekłada się na popyt na rozwiązania Backup as a Service. Niedoinwestowane działy IT mogą dzięki temu lepiej reagować na istniejące zagrożenia oraz pokonać lukę kompetencyjną. Firmy reprezentujące rynek Midmarket oczekują jednak hybrydowego podejścia, są otwarte na chmurę, ale w dalszym ciągu przywiązują dużą wagę do własnej, posiadanej infrastruktury, kompetencji i zasobów. Chętnie szukają też lokalnych partnerów.

# IV. Podsumowanie

- Większość organizacji działających na rynku Midmarket, ciągle nie jest gotowa do konkurowania w realiach gospodarki cyfrowej. Działy IT są niedoinwestowane, nie posiadają odpowiednich narzędzi do zarządzania i analizowania danych. Ich strategia opiera się przede wszystkim na ochronie danych zgodnie z regulacjami, a nie pełnym ich wykorzystaniu do celów biznesowych.
- Zdając sobie sprawę z istotności danych, podmioty Midmarket starają się w pełni kontrolować proces backupu i archiwizacji danych, nie posiadają jednak wystarczających kompetencji i zasobów, by do minimum zmniejszyć ryzyko utraty danych. Zaufanie zewnętrznemu dostawcy ma duże znaczenie w budowie organizacji opartej na danych, pozwalając znacząco przyspieszyć tę transformację.
- Zdecydowana większość podmiotów rynku Midmarket nie posiada dedykowanego budżetu oraz administratorów skoncentrowanych na ochronie danych. Rynek pracy specjalistów IT jest bardzo konkurencyjny, popyt na nim zdecydowanie przewyższa podaż. Mniejsze organizacje najczęściej nie są tak atrakcyjne dla pracowników IT, jak duże korporacje, a koszty budowy i rozwoju własnych kompetencji są wysokie i ciągle rosną.
- Analizując najbardziej istotne kryteria wyboru dostawcy usług BaaS czy DRaaS, organizacje Midmarket w szczególności zwracają uwagę na listę oferowanych usług, jakość wsparcia czy zapewniają one zgodność z odpowiednimi regulacjami oraz czy można zlokalizować miejsce przechowywania tych danych. Cena została wskazana na dalszym miejscu, co oznacza, że zamawiający są skłonni zapłacić więcej, jeśli będą mieli dostęp do dodatkowych funkcji.
- W zakresie ochrony danych, administratorzy najbardziej obawiają się ataków typu ransomware. Sporym wyzwaniem jest także zapanowanie nad kopiami danych oraz szybko rosnącymi kosztami. Stosunkowo nowym wyzwaniem, ale nabierającym dużego znaczenia, jest ochrona danych w chmurze.

- Mimo tych obaw, aż co piąty respondent ignoruje podstawowe zasady polityki backupu i odtwarzania po awarii nie posiadając żadnego, odseparowanego fizycznie ośrodka zapasowego.
- Obawa dotycząca ciągłości działania po ataku ransomware, powinna zwrócić uwagę szefów działów IT firm Midmarket na usługi BaaS i DRaaS. Istnienie trzeciej, "złotej" kopii danych w chmurze, umożliwiająca odtworzenie cyfrowego stanu posiadania, może gwarantować przetrwanie danej organizacji na rynku. I to za nieporównywalnie niższą cenę, niż tworzenie cyfrowego archiwum odseparowanego od własnych systemów IT.


## IDC Polska

ul. Gotarda 9
02-683 Warszawa
Poland

+48 225 484 050
Twitter: @IDC
idc-community.com

www.idc.com


## O tej publikacji

Niniejsza publikacja została opracowana przez IDC Custom Solutions. Przedstawiona opinia, analiza i wyniki badań pochodzą z innych bardziej szczegółowych badań i analiz niezależnie przeprowadzonych i opublikowanych przez IDC, o ile nie wskazano na konkretne badanie sponsorowane. IDC Custom Solutions udostępnia treści IDC w szerokiej gamie formatów do dystrybucji przez różne firmy. Licencja na dystrybucję treści IDC nie oznacza poparcia ani wyrażenia opinii o licencjobiorcy.