# Większa dojrzałość w zakresie cyberbezpieczeństwa i odporności

## Dojrzałość w zakresie cyberbezpieczeństwa to strategiczna dźwignia dla każdej nowoczesnej firmy

Obecny krajobraz zagrożeń cybernetycznych jest bardziej dynamiczny i bezwzględny niż kiedykolwiek, a ataki oparte na sztucznej inteligencji stają się coraz częstsze, szybsze i bardziej wyrafinowane. Organizacje nie mogą już polegać na fragmentarycznych środkach ochrony ani na stopniowych aktualizacjach.

Jako lider biznesowy, musisz działać tak, jakby wyciek danych był nieunikniony, jeśli nie nieuchronny. W Dell Technologies pomagamy klientom zwiększyć ich dojrzałość w zakresie bezpieczeństwa, czyli poziom pewności, z jakim prowadzą działalność w obliczu ryzyka cybernetycznego. Robimy to, rozwijając kompleksowe, warstwowe podejście do cyberbezpieczeństwa i odporności oparte na trzech kluczowych obszarach praktyki.

Firmy muszą dysponować następującymi możliwościami:

- **Zmniejszenie obszaru narażonego na ataki**
- **Wykrywanie cyberzagrożeń i reagowanie na nie**
- **Usuwanie skutków cyberataków**

Skuteczne cyberbezpieczeństwo zaczyna się od uczciwej oceny obecnego stanu bezpieczeństwa i dojrzałości. Ta wyrazistość pozwala nadać priorytet odpowiednim ulepszeniom i inwestować w bezpieczniejsze jutro.

# Zmniejszenie obszaru narażonego na ataki

Obszar narażony na ataki w organizacji jest dynamiczny i szybko ewoluuje, a sztuczna inteligencja wprowadza nowe wektory ataków. Wraz z pracą zdalną i korzystaniem ze starszych systemów powiększają one obszar narażony na ataki, tworząc więcej punktów dostępu dla cyberprzestępców. W efekcie zmniejszanie obszaru narażonego na ataki jest strategiczną koniecznością w celu ograniczenia ryzyka, spełnienia zobowiązań w zakresie zgodności z przepisami, ochrony odporności organizacyjnej i budowania podstawowego zaufania.

# Większa dojrzałość w zakresie cyberbezpieczeństwa i odporności

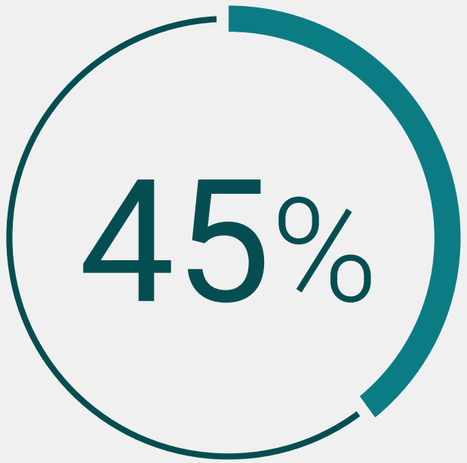
Zmniejszanie obszaru narażonego na ataki pomaga ograniczyć ogólne ryzyko, minimalizując liczbę punktów dostępu, które atakujący mogą wykorzystać. Zwiększa to dojrzałość w zakresie bezpieczeństwa i usprawnia działania w zakresie zgodności z przepisami. Rezultatem jest większa odporność, niższe koszty dzięki unikaniu incydentów oraz zdolność do szybszego działania, swobodniejszego wprowadzania innowacji i pewnego wchodzenia na nowe rynki ze świadomością, że zabezpieczenia są wbudowane od samego początku. Zaczyna się od przyjęcia zasad modelu „zero trust" — nigdy nie ufaj, zawsze weryfikuj — i egzekwowania zasady „najmniejszych uprawnień" między użytkownikami, urządzeniami i aplikacjami.

W Dell Technologies stosujemy mentalność „wprowadzania zabezpieczeń na etapie projektowania". Cyberbezpieczeństwo jest wbudowane we wszystko, co robimy, począwszy od naszego bezpiecznego globalnego łańcucha dostaw, aż po wbudowane zabezpieczenia naszych podstawowych produktów. Te zabezpieczenia zaczynają się na poziomie sprzętowym, aby zapewnić, że urządzenia uruchamiają się i działają tylko z zaufanym oprogramowaniem. Dostosowujemy nasze rozwiązania do zasad modelu „zero trust", pomagając eliminować luki w zabezpieczeniach, zanim atakujący będą mogli je wykorzystać. Na przykład nasze najbezpieczniejsze na świecie komercyjne komputery AI PC[1] zapewniają podstawowe zabezpieczenia nowoczesnej przestrzeni roboczej.

Zmniejszanie obszaru narażonego na ataki zwiększa dojrzałość zabezpieczeń przez eliminację niepewności — mniej niewiadomych, mniej punktów dostępu i mniej niespodzianek.

**Najważniejsze rezultaty u klientów:**

- **Minimalizowanie podatności:** dzięki proaktywnemu wzmacnianiu punktów końcowych, infrastruktury i aplikacji możesz znacznie zmniejszyć możliwości atakujących.
- **Uproszczone zarządzanie zabezpieczeniami:** mniejsza liczba narażonych zasobów oznacza mniej kontroli do zarządzania, co prowadzi do bardziej usprawnionego i wydajnego stanu bezpieczeństwa.
- **Silniejsza podstawa innowacji:** dzięki zaufanym punktom końcowym i chronionym danym możesz z większą pewnością wdrażać nowe technologie, takie jak sztuczna inteligencja i przetwarzanie brzegowe.




Organizacje, które koncentrują się na zmniejszaniu obszaru narażonego na ataki, osiągają redukcję o 45% ryzyka cybernaruszeń podczas zarządzania zagrożeniami zewnętrznymi[2].

# Wykrywanie cyberzagrożeń i reagowanie na nie

W dziedzinie cyberbezpieczeństwa szybkość i inteligencja idą ze sobą w parze. Skuteczne wykrywanie i reagowanie pozwalają szybko identyfikować i eliminować zagrożenia, skracając czas przestojów i ograniczając szkody spowodowane atakiem. Rezultatem są niższe koszty, mniej przestojów i większa pewność operacyjna, że Twoja firma może bezpiecznie działać nawet wtedy, gdy jest stale zagrożona.

# Większa dojrzałość w zakresie cyberbezpieczeństwa i odporności

Jednak wiele organizacji boryka się z ograniczoną widocznością w środowiskach hybrydowych i przytłaczającą liczbą alertów. Atakujący przebywają w sieciach średnio 11 dni, zanim zostaną wykryci. Aby temu przeciwdziałać, potrzebna jest widoczność punktów końcowych, sieci i systemów w czasie rzeczywistym poprzez ciągłe monitorowanie, analizę zagrożeń i automatyzację.

Odpowiedni partnerzy w zakresie bezpieczeństwa zapewniają specjalistyczną wiedzę ekspercką w zakresie analizy zagrożeń i reagowania na incydenty. Dell łączy zaawansowaną analitykę, wykrywanie zagrożeń oparte na sztucznej inteligencji i uczeniu maszynowym oraz usługi zarządzane 24x7 z bezpiecznym fundamentem sprzętowym, aby identyfikować i eliminować zagrożenia, zanim spowodują zakłócenia. Opcjonalne usługi, takie jak Managed Detection and Response (MDR), zapewniają specjalistyczną wiedzę w zakresie bezpieczeństwa, która pozwala na zwiększenie widoczności i szybkie reagowanie na zagrożenia oraz ich eliminację.

Solidne możliwości wykrywania i reagowania zwiększają dojrzałość zabezpieczeń, skracając czas przestojów i dając zespołom pewność, że mogą podejmować zdecydowane działania w przypadku pojawienia się zagrożeń.

**Najważniejsze rezultaty u klientów:**

- **Szybsze wykrywanie i krótszy czas reakcji:** Managed Detection and Response (MDR) może skrócić średni czas wykrywania i reagowania o 25-49%, zmniejszając prawdopodobieństwo, że atak stanie się poważniejszy.
- **Mniejsze obciążenie operacyjne:** współpraca z ekspertami w zakresie proaktywnego wykrywania zagrożeń i ciągłego monitorowania pozwala na przeniesienie obciążenia z wewnętrznych zespołów, umożliwiając im skupienie się na pracy strategicznej.
- **Zwiększona odporność:** dojrzałe funkcje wykrywania i reagowania prowadzą do mniejszej liczby incydentów związanych z bezpieczeństwem i pomagają uniknąć wyższych kosztów związanych z naruszeniami.

**4,44 mln USD**

Średni koszt naruszenia danych wyniósł 4,44 mln USD w 2025 r.[3]

# Usuwanie skutków cyberataku

W przypadku najgorszego scenariusza głównym celem jest jak najszybszy powrót do normalnej działalności przy minimalnych zakłóceniach. Odzyskiwanie danych po cyberataku gwarantuje szybkie przywrócenie czystych danych i systemów, co ogranicza szkody wizerunkowe i daje pewność, że odzyskiwanie jest niezawodne i nie grozi ponownym zainfekowaniem.

# Większa dojrzałość w zakresie cyberbezpieczeństwa i odporności

Nawet jeśli budujesz najsilniejszą możliwą obronę, musisz planować tak, jakby atak był nieunikniony. Posiadanie planu i możliwości usuwania skutków ataków ma kluczowe znaczenie. Obejmuje to utrzymywanie czystych, niezmiennych kopii zapasowych danych o znaczeniu krytycznym w odizolowanym sejfie odzyskiwania oraz korzystanie ze środowisk typu cleanroom w celu sprawdzenia, czy przywrócone systemy są wolne od złośliwego oprogramowania przed przywróceniem ich do trybu online.

Dell wykorzystuje możliwości odzyskiwania danych w swojej ofercie produktów, a przywrócenie działalności do normalności jest naszym priorytetem w przypadku wystąpienia incydentów. Rozwiązania takie jak PowerProtect Cyber Recovery Vault izolują i chronią czyste kopie krytycznych danych w celu szybkiego odzyskiwania, ograniczenia utraty danych i uniemożliwiania ich wykorzystania w atakach ransomware. Ta architektura pomaga szybko przywrócić krytyczne obciążenia robocze do trybu online, dzięki czemu możesz czuć się pewnie.

Odzyskiwanie danych jest często prawdziwym testem dojrzałości zabezpieczeń — gdy pewność siebie zależy od tego, jak szybko i sprawnie firma może powrócić do normalnej działalności.

**Najważniejsze rezultaty u klientów:**

- **Mniejszy wpływ na działalność:** organizacje z dobrze przygotowanym planem reagowania na incydenty mogą obniżyć koszty naruszenia o około 61%.
- **Szybsze wznowienie operacji:** priorytetowe traktowanie szybkiego powrotu do działalności, a nie tylko usuwania zagrożeń, pomaga przywrócić operacje przy minimalnych zakłóceniach i kosztach.
- **Lepsza integralność danych:** izolowanie danych o znaczeniu krytycznym, korzystanie z niezmiennych kopii i weryfikacja integralności przed przywróceniem buduje zaufanie do procesu odzyskiwania.


organizacji przyznało, że miałyby trudności z odzyskaniem danych po cyberataku przy jednoczesnym spełnieniu umów o poziomie usług[4].

# Wzmocnij dojrzałość swoich zabezpieczeń dzięki strategicznym partnerstwom

Doświadczeni partnerzy są niezbędni do poruszania się w dzisiejszym szybko zmieniającym się i złożonym krajobrazie cyberbezpieczeństwa. Cyberzagrożenia stają się coraz bardziej wyrafinowane i częste, co sprawia, że niemal niemożliwe jest utrzymanie przez jedną organizację wiedzy eksperckiej, zasobów i technologii niezbędnych do utrzymania przewagi nad konkurencją. Współpracując z liderami ds. bezpieczeństwa, takimi jak Dell, firmy uzyskują dostęp do specjalistycznych umiejętności, najnowocześniejszych technologii i sieci zaufanych partnerów. Współpraca ta zapewnia wsparcie i wiedzę ekspercką niezbędną do skutecznego wykrywania zagrożeń, zapobiegania im i reagowania na nie, zapewniając firmom ochronę w stale zmieniającym się środowisku cyfrowym.

Dzięki odpowiedniemu podejściu w tych trzech obszarach praktyki organizacje zwiększają swoją dojrzałość w zakresie bezpieczeństwa, budując pewność działania, wprowadzania innowacji i rozwoju pomimo ciągłej presji cybernetycznej. Dell łączy zaufane rozwiązania infrastrukturalne, bezpieczne środowisko pracy, zaawansowane usługi i ekosystem partnerów, aby pomóc Twojej organizacji zachować bezpieczeństwo, elastyczność i odporność — gotową na przyszłe wyzwania.

**Odkryj rozwiązania w zakresie bezpieczeństwa**

DELL Technologies

## Informacje o firmie Dell Technologies

Firma Dell Technologies (NYSE: DELL) pomaga klientom w rozwijaniu nowoczesnego środowiska cyfrowego oraz przekształcaniu sposobu pracy, stylu życia i korzystania z rozrywki. Firma zapewnia klientom najszersze i najbardziej innowacyjne w branży portfolio technologii i usług w dobie sztucznej inteligencji.



Dowiedz się więcej na stronie Dell.com

# Często zadawane pytania

**1. Dlaczego cyberbezpieczeństwo powinno być najwyższym priorytetem dla mojej firmy?**
*Cyberbezpieczeństwo to coś więcej niż tylko ochrona; to fundament, na którym firma może opierać innowacyjność i rozwój, jednocześnie opierając się niebezpiecznym cyberatakom. Solidny stan bezpieczeństwa to nie tylko obrona — to możliwości. Firmy z dojrzałymi strukturami cyberbezpieczeństwa mogą działać szybciej, wprowadzać innowacje i bez obaw wchodzić na nowe rynki. Są lepiej przygotowane do obsługi zmian regulacyjnych, wymagań klientów i presji konkurencyjnej.*

**2. Jak zrównoważyć potrzebę ścisłego bezpieczeństwa ze swobodą wprowadzania innowacji?**
*Nie musisz wybierać między bezpieczeństwem a innowacyjnością. Uważamy, że solidne zabezpieczenia faktycznie umożliwiają innowacje. Gdy masz fundament oparty na założeniu „bezpieczeństwo już na etapie projektowania", w którym zabezpieczenia są wbudowane w urządzenia, infrastrukturę i dane od samego początku, Twoje zespoły mogą bez obaw wdrażać nowe technologie, takie jak sztuczna inteligencja i przetwarzanie na brzegu sieci.*

**3. Dlaczego bezpieczeństwo łańcucha dostaw jest tak ważne?**
*Prawdziwe zabezpieczenia zaczynają się na długo przed naciśnięciem przycisku zasilania. Wraz z rozwojem cyfrowego ekosystemu wzrasta też zagrożenie — dlatego zaufanie staje się Twoją pierwszą linią obrony. Każde ogniwo w łańcuchu dostaw musi być chronione, ponieważ pojedynczy, zagrożony element może osłabić nawet najbardziej zaawansowane oprogramowanie. Dlatego budujemy zabezpieczenia od podstaw, chroniąc każdy krok od produkcji po wdrożenie. Od hali fabrycznej pod Twoje drzwi — technologia, jaką otrzymujesz, jest zaufana, zweryfikowana i stworzona z myślą o niezawodnym działaniu.*

**4. W jaki sposób Dell pomaga nam w odzyskaniu sprawności po cyberataku?**
*Minimalizacja przestojów i zakłóceń ma kluczowe znaczenie w przypadku wystąpienia incydentów. Przygotowanie jest kluczowe. Nasze rozwiązanie PowerProtect Cyber Recovery Vault izoluje czystą, niezmienną kopię Twoich najważniejszych danych, bezpiecznie oddzieloną od Twojego środowiska podstawowego. W przypadku incydentu możesz szybko i pewnie przywrócić działanie bez kompromisów i bez konieczności płacenia okupu.*
*Dell oferuje szeroką gamę produktów i usług zaprojektowanych z myślą o wdrożeniu kompleksowej strategii odzyskiwania danych. Obejmuje usługi konsultingowe, tworzenie planu odzyskiwania i szkolenia, a także funkcje ochrony danych, które mogą zapewnić bezpieczeństwo najważniejszych danych. Dell stosuje podejście zorientowane na ludzi i technologię, zapewniając współpracę zarówno pracowników, jak i technologii, aby pomóc Ci szybko odzyskać sprawność.*

**5. Czy Dell może pomóc w wykrywaniu zagrożeń w czasie rzeczywistym?**
*Zdecydowanie. Szybkość to wszystko, jeśli chodzi o powstrzymywanie cyberzagrożeń. Łączymy wbudowane funkcje zabezpieczeń z zaawansowanymi usługami, takimi jak Managed Detection and Response (MDR), aby monitorować środowisko 24/7. Dzięki informacjom opartym na sztucznej inteligencji i uczeniu maszynowym oraz wiedzy eksperckiej, pomagamy natychmiast wykrywać anomalie i potencjalne zagrożenia, umożliwiając reagowanie i ograniczanie problemów, zanim wpłyną one na działalność.*

# Źródła

**[1] Na podstawie wewnętrznej analizy firmy Dell, październik 2024 r. (Intel) i marzec 2025 r. (AMD). Dotyczy komputerów z procesorami Intel i AMD. Nie wszystkie funkcje są dostępne na każdym komputerze. W przypadku niektórych funkcji wymagany jest dodatkowy zakup. Komputery z procesorami Intel zostały zweryfikowane przez Principled Technologies, lipiec 2025 r. Anatomia zaufanego urządzenia — infografika**
**[2] Forrester Consulting, „The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight", październik 2024 r.**
**[3] IBM i Ponemon Institute, „Raport o kosztach naruszenia danych 2025: luka w nadzorze AI", 2025.**
**[4] Dell Technologies, „Zaawansowana dojrzałość w zakresie cyberbezpieczeństwa:infrastruktura technologiczna to serce każdej nowoczesnej firmy", luty 2025 r.**