

Bitdefender®

Jak
Bitdefender
wspiera
zgodność z
DORA

Przewodnik po tym, jak
produkty i usługi Bitdefender
pomagają organizacjom
spełniać wymagania regulacji
Digital Operational
Resilience Act
(DORA)

Spis treści

- 03 Czym jest **DORA**
- 04 Wymagania **DORA** obejmujące 5 kluczowych obszarów
- 05 Jak Bitdefender wspiera zgodność z wymaganiami **DORA**
- 10 Dlaczego warto wybrać Bitdefender dla zgodności z **DORA** i odporności cybernetycznej



Czym jest DORA

Digital Operational Resilience ACT (DORA) to ramy regulacyjne wprowadzone przez Unię Europejską w celu wzmocnienia cyberbezpieczeństwa i odporności cyfrowej w sektorze finansowym

Regulacja weszła w życie 16 stycznia 2023 roku, a zacznie obowiązywać od 17 stycznia 2025 roku. DORA uzupełnia inne akty europejskie mające na celu zwiększenie odporności cybernetycznej i ochrony prywatności, takie jak Dyrektywa o Bezpieczeństwie Sieci i Informacji (NIS2) oraz Ogólne Rozporządzenie o Ochronie Danych (RODO).

Kto powinien spełniać wymagania DORA

DORA dotyczy podmiotów finansowych z państw członkowskich Unii Europejskiej (UE) oraz ich dostawców usług ICT, niezależnie od miejsca, w którym się znajdują. Kluczowe podmioty, które powinny spełniać wymagania DORA, to:



Banki i inne instytucje kredytowe



Infrastruktury rynków finansowych



Firmy inwestycyjne i zarządzające funduszami



Firmy ubezpieczeniowe



Instytucje płatnicze i pieniądza elektronicznego



Dostawcy usług związanych z kryptowalutami



Zewnętrzni dostawcy usług ICT



Inne kluczowe podmioty (np. agencje ratingowe, instytucje emerytalne, dostawcy usług crowdfundingowych)

DORA

5 kluczowych wymagań



- 1 Zarządzanie ryzykiem ICT – Ramy zarządzania i minimalizowania ryzyka ICT
- 2 Zarządzanie incydentami ICT – Procesy raportowania i obsługi zakłóceń ICT
- 3 Testowanie odporności operacyjnej – Ciągłe testowanie, w tym testy penetracyjne
- 4 Zarządzanie ryzykiem stron trzecich – Nadzór i zarządzanie dostawcami ICT
- 5 Wymiana informacji – Współpraca na rzecz wzmocnienia odporności na cyberzagrożenia

Jak Bitdefender wspiera zgodność z wymaganiami DORA

Poniższa tabela przedstawia kluczowe artykuły i paragrafy z DORA, Rozporządzenia (UE) 2022/2554, w których rozwiązania Bitdefender mogą pomóc organizacjom w spełnieniu wymagań, przynajmniej częściowo. Przepisy wykonawcze i akty delegowane do Rozporządzenia (UE) 2022/2554 określają normy techniczne i regulacyjne, które dostarczają specyfikacji i wskazówek dotyczących wdrażania wymagań DORA. Jednym z nich jest Rozporządzenie Delegowane Komisji (UE) 2024/1774, które określa normy techniczne dotyczące narzędzi, metod, procesów i polityk zarządzania ICT oraz uproszczonych ram zarządzania ryzykiem ICT.

Rozporządzenie DORA (UE) 2022/2554 – Wymagania

Bitdefender
Rozwiązanie

Rozdział 2, Sekcja 2, Art. 8 – Identyfikacja

1. W ramach systemu zarządzania ryzykiem ICT, podmioty finansowe muszą identyfikować, klasyfikować i odpowiednio dokumentować wszystkie funkcje biznesowe wspierane przez ICT, role i odpowiedzialności, zasoby informacyjne oraz zasoby ICT wspierające te funkcje, a także ich zależności w kontekście ryzyka ICT.
4. Podmioty finansowe muszą identyfikować wszystkie zasoby informacyjne i ICT, w tym te znajdujące się w zdalnych lokalizacjach, zasoby sieciowe i sprzęt komputerowy, a także mapować te, które są uznawane za krytyczne.
6. W odniesieniu do ustępów 1,3,4 i 5, podmioty finansowe muszą prowadzić odpowiednie rejestry i aktualizować je okresowo oraz za każdym razem, gdy nastąpi istotna zmiana.

GravityZone Endpoint Security oraz **Extended Detection and Response** pomagają w identyfikacji zasobów poprzez tworzenie i utrzymywanie inwentarza systemów zarządzanych i niezarządzanych.

GravityZone CSPM+ inwentaryzuje zasoby chmurowe na różnych platformach, wykrywa błędne konfiguracje i mapuje wyniki do szerokiego zestawu regulacji i standardów.

Rozporządzenie DORA (UE) 2022/2554 – Wymagania

Bitdefender
Rozwiązanie

Rozdział 2, Sekcja 2, Art. 8 – Identyfikacja

2. Podmioty finansowe muszą na bieżąco identyfikować wszystkie źródła ryzyka ICT, w szczególności ekspozycję na ryzyko w relacjach z innymi podmiotami finansowymi, oraz oceniać zagrożenia cybernetyczne i podatności ICT istotne dla ich funkcji biznesowych wspieranych przez ICT, zasobów informacyjnych oraz zasobów ICT.

GravityZone Risk Management wykrywa podatności aplikacji, błędne konfiguracje urządzeń końcowych i ryzykowne zachowania użytkowników, priorytetyzuje je według stopnia zagrożenia i umożliwia proste środki zaradcze.

GravityZone CSPM+ identyfikuje i priorytetyzuje ryzyko wynikające z błędnych konfiguracji i podatności w zasobach chmurowych.

Usługi Offensive Security (testy penetracyjne, red teaming) pomagają wykrywać podatności i oceniać ryzyko.

Rozdział 2, Sekcja 2, Art. 8 – Identyfikacja

3. Podmioty finansowe (inne niż mikroprzedsiębiorstwa) muszą przeprowadzać ocenę ryzyka przy każdej istotnej zmianie w infrastrukturze sieciowej i systemów informacyjnych, a także w procesach lub procedurach wpływających na ich funkcje biznesowe wspierane przez ICT, zasoby informacyjne lub zasoby ICT.
7. Podmioty finansowe (inne niż mikroprzedsiębiorstwa) muszą przeprowadzać ocenę ryzyka po każdej istotnej zmianie w infrastrukturze sieciowej i systemach ICT. Muszą także przeprowadzać coroczne oceny ryzyka wszystkich starszych systemów ICT.

GravityZone Risk Management oraz **GravityZone CSPM+** generują wyniki oceny ryzyka, które ułatwiają identyfikację zagrożeń i ocenę prawdopodobieństwa skutecznych cyberataków.

Rozdział 2, Sekcja 2, Art. 9 –
Ochrona i zapobieganie

1. Aby zapewnić odpowiednią ochronę systemów ICT i organizację środków reakcji, podmioty finansowe muszą stale monitorować i kontrolować bezpieczeństwo systemów ICT oraz **minimalizować wpływ ryzyka ICT poprzez wdrażanie odpowiednich narzędzi, polityk i procedur.**
2. Podmioty finansowe powinny projektować, nabywać i wdrażać zasady, procedury, protokoły oraz narzędzia bezpieczeństwa ICT, które mają na celu zapewnienie odporności, ciągłości i dostępności systemów ICT, w szczególności tych wspierających funkcje krytyczne lub istotne, oraz utrzymanie wysokich standardów dostępności, autentyczności, integralności i poufności danych, zarówno w stanie spoczynku, w użyciu, jak i podczas transmisji.
3. W celu osiągnięcia celów, o których mowa w ustępie 2, podmioty finansowe powinny wykorzystywać rozwiązania i procesy ICT odpowiednie zgodnie z artykułem 4. Te rozwiązania i procesy ICT powinny:
(b) **minimalizować ryzyko uszkodzenia lub utraty danych, nieautoryzowanego dostępu oraz usterek technicznych, które mogą zakłócać działalność biznesową;**
(c) **zapobiegać brakom dostępności, naruszeniom autentyczności i integralności, naruszeniom poufności oraz utracie danych;**
(d) **zapewniać ochronę danych przed ryzykiem związanym z ich zarządzaniem, w tym niewłaściwą administracją, ryzykami związanymi z przetwarzaniem oraz błędami ludzkimi.**

Produkty zabezpieczające **platformy GravityZone** dla punktów końcowych, poczty e-mail, urządzeń mobilnych, chmury, kontenerów, CSPM+, pełnego szyfrowania dysków, zarządzania poprawkami, wykrywania i reagowania zapewniają kompleksową, wielowarstwową ochronę w celu minimalizacji wpływu ryzyka ICT.

Funkcja **ograniczania skutków oprogramowania ransomware** zmniejsza wpływ potencjalnych incydentów związanych z ransomware.

Kompleksowe, warstwowe zabezpieczenia dostępne w produktach platformy GravityZone pomagają zapobiegać naruszeniom i utracie danych, zmniejszając prawdopodobieństwo incydentów wpływających na dostępność, autentyczność lub integralność danych.

Usługi ofensywnego bezpieczeństwa, w tym testy penetracyjne i red teaming, pomagają wykrywać błędne konfiguracje i podatności, które mogą prowadzić do nieautoryzowanego dostępu, utraty danych lub usterek zakłócających działalność biznesową.



Rozdział 2, Sekcja 2, Art. 10 –
Wykrywanie

1. Podmioty finansowe powinny wdrożyć Mechanizmy umożliwiające szybkie wykrywanie nietypowych działań, zgodnie z Artykułem 17, w tym problemów z wydajnością sieci ICT oraz incydentów związanych z ICT, a także identyfikowanie potencjalnych istotnych pojedynczych punktów awarii.
2. **Mechanizmy wykrywania, o których mowa w ustępie 1, powinny umożliwiać wielowarstwową kontrolę, określać proggi alertów oraz kryteria uruchamiania i inicjowania procesów reagowania na incydenty związane z ICT, w tym automatyczne mechanizmy powiadamiania odpowiednich pracowników odpowiedzialnych za reagowanie na takie incydenty.**
3. Instytucje finansowe powinny **przeznaczać wystarczające zasoby i możliwości na monitorowanie aktywności użytkowników, występowania anomalii ICT oraz incydentów związanych z ICT, w szczególności cyberataków.**



Rozwiązania GravityZone Endpoint Detection and Response oraz Extended Detection and Response zostały zaprojektowane do szybkiego wykrywania anomalnej aktywności oraz oznak potencjalnych ataków lub incydentów bezpieczeństwa. Po wykryciu, rozwiązania te dostarczają czytelne podsumowania incydentów oraz umożliwiają łatwe prowadzenie dochodzenia i reagowanie.

Usługi Bitdefender Managed Detection and Response zapewniają całodobowe monitorowanie zagrożeń, ich analizę oraz reakcję na incydenty. Usługi te rozszerzają wewnętrzne możliwości organizacji i gwarantują odpowiednie zasoby do monitorowania cyberataków oraz incydentów ICT.



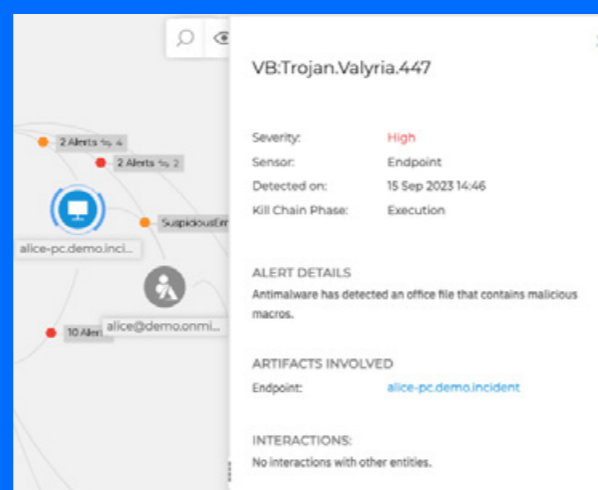
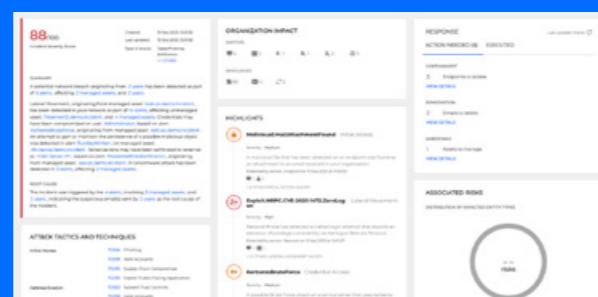
Rozdział 2, Sekcja 2, Art. 11 – Reagowanie i Odzyskiwanie

- Instytucje finansowe powinny wdrożyć politykę ciągłości działania ICT poprzez dedykowane, odpowiednie i udokumentowane rozwiązania, plany, procedury i mechanizmy mające na celu:
 - zapewnienie ciągłości krytycznych lub istotnych funkcji instytucji finansowej;
 - szybkie, odpowiednie i skuteczne reagowanie na wszystkie incydenty związane z ICT oraz ich rozwiązywanie w sposób ograniczający szkody i priorytetowo traktujący wznowienie działalności oraz działania naprawcze;**
 - natychmiastowe uruchomienie dedykowanych planów umożliwiających zastosowanie środków ograniczających, procesów i technologii dostosowanych do każdego rodzaju incydentu związanego z ICT, a także zapobieganie dalszym szkodom oraz wdrożenie dostosowanych procedur reagowania i odzyskiwania zgodnie z artykułem 12;
 - oszacowanie wstępnych skutków, strat i szkód.

- W ramach kompleksowego zarządzania ryzykiem ICT, podmioty finansowe powinny:
 - testować plany ciągłości działania ICT oraz plany reagowania i odzyskiwania ICT w odniesieniu do systemów ICT wspierających wszystkie funkcje, co najmniej raz w roku, a także w przypadku jakichkolwiek istotnych zmian w systemach ICT wspierających funkcje krytyczne lub ważne;**

Produkty GravityZone EDR, XDR oraz usługi Bitdefender MDR umożliwiają organizacjom skuteczne reagowanie na incydenty ICT oraz powstrzymywanie ataków, zapobiegając ich dalszemu rozprzestrzenianiu się.

Funkcje raportowania kryminalistycznego i wizualizacje dostępne w produktach GravityZone EDR i XDR ułatwiają ocenę wpływu incydentów ICT.



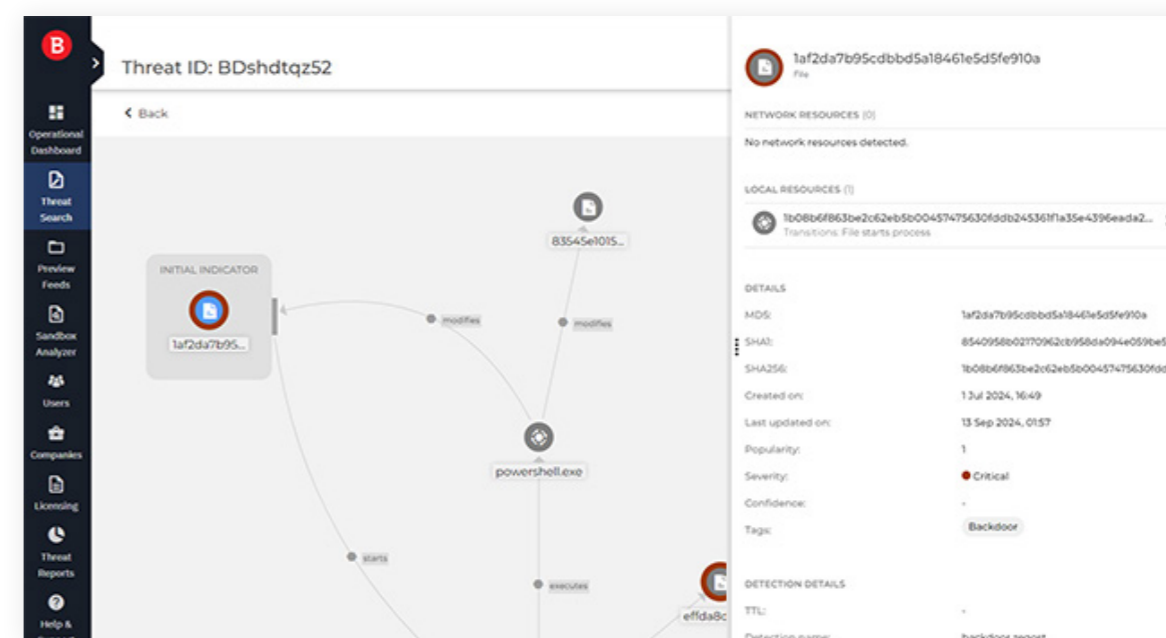
Rozdział 2, Sekcja 2, Art. 13 – Nauka i Rozwój

- Instytucje finansowe muszą **posiadać odpowiednie zasoby i personel do gromadzenia informacji o podatnościach oraz zagrożeniach cybernetycznych, incydentach związanych z ICT, w szczególności cyberatakach, oraz do analizy ich potencjalnego wpływu na cyfrową odporność operacyjną.**

GravityZone EDR, XDR i CSPM+ zapewniają kompleksowe i łatwe do wygenerowania raporty dotyczące podatności, ryzyk oraz cyberataków lub innych incydentów wpływających na organizację.

Bitdefender Advanced Threat Intelligence dostarcza kluczowych informacji na temat najistotniejszych zagrożeń dla konkretnych branż oraz oferuje zaawansowane funkcje wyszukiwania, które pomagają organizacjom zrozumieć i ocenić wpływ potencjalnych zagrożeń na ich odporność cyfrową.

Usługi ofensywnego bezpieczeństwa, w tym testy penetracyjne i red teaming, pomagają wykrywać błędne konfiguracje, podatności oraz analizować ich wpływ na organizację.



Bitdefender
Advanced
Threat
Intelligence

**Rozdział 4 – Testowanie odporności cyfrowej,
Art. 24 – Ogólne wymagania dotyczące
przeprowadzania testów odporności cyfrowej**

1. W celu oceny gotowości do reagowania na incydenty związane z ICT, identyfikacji słabych punktów, niedociągnięć i luk w odporności cyfrowej oraz szybkiego wdrażania działań naprawczych, instytucje finansowe, inne niż mikroprzedsiębiorstwa, biorąc pod uwagę kryteria określone w art. 4(2), muszą ustanowić, utrzymywać i regularnie przeglądać solidny i kompleksowy program testowania odporności cyfrowej jako integralną część zarządzania ryzykiem ICT, o którym mowa w art. 6.
2. Program testowania odporności cyfrowej musi obejmować szereg ocen, testów, metodologii, praktyk i narzędzi stosowanych zgodnie z art. 25 i 26.

**Rozdział 4 – Testowanie odporności cyfrowej,
Art. 25 – Testowanie narzędzi i systemów ICT**

1. Program testowania odporności cyfrowej, o którym mowa w art. 24, musi obejmować, zgodnie z kryteriami określonymi w art. 4(2), realizację odpowiednich testów, takich jak: **oceny podatności i skanowania**, analizy źródeł otwartych, oceny bezpieczeństwa sieci, analizy luk, przeglądy bezpieczeństwa fizycznego, ankiety i rozwiązania do skanowania, przeglądy kodu źródłowego, jeśli to możliwe, testy scenariuszowe, testy kompatybilności, testy wydajności, **testy end-to-end oraz testy penetracyjne**.
2. Centralne depozyty papierów wartościowych i centralni kontrpartnerzy muszą przeprowadzać **oceny podatności przed wdrożeniem lub ponownym wdrożeniem nowych lub istniejących aplikacji**, komponentów infrastruktury oraz usług ICT wspierających krytyczne lub istotne funkcje instytucji finansowej.

Usługi ofensywnego bezpieczeństwa, w tym testy penetracyjne i red teaming, pomagają wykrywać błędne konfiguracje i podatności oraz analizować ich wpływ na organizację przed wdrożeniami i większymi zmianami w środowisku organizacji.

**Rozdział 4 – Testowanie odporności
cyfrowej, Art. 26 – Zaawansowane
testowanie narzędzi, systemów i
procesów ICT w oparciu o TLPT**

1. Instytucje finansowe, inne niż te wymienione w art. 16(1) pierwszego akapitu oraz inne niż mikroprzedsiębiorstwa, które zostały zidentyfikowane zgodnie z ust. 8 trzeciego akapitu niniejszego artykułu, muszą przeprowadzać co najmniej **raz na trzy lata zaawansowane testowanie metodą TLPT (Threat-Led Penetration Testing)**. W oparciu o profil ryzyka instytucji finansowej oraz biorąc pod uwagę okoliczności operacyjne, właściwy organ nadzorczy może, jeśli to konieczne, zażądać zmniejszenia lub zwiększenia tej częstotliwości.
3. W przypadku, gdy dostawcy usług ICT stron trzecich są objęci zakresem TLPT, instytucja finansowa musi podjąć niezbędne środki i zabezpieczenia, aby zapewnić udział tych dostawców w testowaniu oraz ponosić pełną odpowiedzialność za zgodność z niniejszym rozporządzeniem.
8. Instytucje finansowe muszą zatrudniać testerów w celu przeprowadzania TLPT zgodnie z art. 27. Jeśli instytucje korzystają z wewnętrznych testerów, co trzy testy muszą zatrudniać zewnętrznych testerów.

Usługi ofensywnego bezpieczeństwa, w tym testy penetracyjne prowadzone w oparciu o zagrożenia (Threat-Led Penetration Testing – TLPT) oraz red teaming, pomagają wykrywać błędne konfiguracje i podatności, aby zwiększyć odporność cybernetyczną organizacji.

Rozdział 4 – Testowanie odporności cyfrowej, Art. 27

Instytucje finansowe mogą korzystać wyłącznie z testerów do przeprowadzania TLPT (Threat-Led Penetration Testing), którzy:

- (a) wykazują najwyższą przydatność i renomę;
- (b) posiadają zdolności techniczne i organizacyjne oraz wykazują **specjalistyczną wiedzę w zakresie analizy zagrożeń, testów penetracyjnych i red teamingu**;
- (c) są certyfikowani przez organ akredytacyjny w państwie członkowskim lub przestrzegają formalnych kodeksów postępowania bądź ram etycznych;
- (d) zapewniają niezależne potwierdzenie lub raport audytowy dotyczący właściwego zarządzania ryzykiem związanym z realizacją TLPT, w tym należytej ochrony poufnych informacji instytucji finansowej oraz zabezpieczenia przed ryzykami biznesowymi instytucji finansowej;
- (e) posiadają odpowiednie ubezpieczenia od odpowiedzialności zawodowej, obejmujące ryzyko niewłaściwego postępowania oraz zaniedbań.

Usługi ofensywnego bezpieczeństwa, w tym testy penetracyjne i red teaming, wykorzystują analizę zagrożeń opartą na szeroko zakrojonych badaniach i laboratoriach Bitdefender, aby pomóc w identyfikacji błędnych konfiguracji i podatności oraz ich analizie zgodnie z metodologiami branżowymi.

Bitdefender posiada szereg ważnych certyfikacji, takich jak **ISO 27001**, wydany przez organ certyfikacyjny w UE.

Rozporządzenie delegowane Komisji (UE) 2024/1774, Tytuł 2, Rozdział 1, Sekcja 4, Art. 6

2. Instytucje finansowe opracowują politykę dotyczącą szyfrowania i kontroli kryptograficznych, o której mowa w ust. 1, na podstawie wyników zatwierdzonej klasyfikacji danych i oceny ryzyka ICT. Polityka ta zawiera zasady dotyczące wszystkich następujących aspektów:
 - (a) szyfrowania danych w spoczynku i podczas transmisji;
 - (b) szyfrowania danych w użyciu, jeśli jest to konieczne;
 - (c) szyfrowania połączeń wewnętrznych w sieci oraz ruchu z podmiotami zewnętrznymi;
 - (d) zarządzania kluczami kryptograficznymi, zgodnie z art. 7, określającego zasady dotyczące prawidłowego użycia, ochrony i cyklu życia kluczy kryptograficznych.

GravityZone Full Disk Encryption pomaga organizacjom zabezpieczać dane w spoczynku, wykorzystując natywne mechanizmy szyfrowania dla systemów Mac i Windows, zapewniając centralne zarządzanie kluczami oraz uproszczone raportowanie zgodności.

Rozporządzenie delegowane Komisji (UE) 2024/1774, Tytuł 2, Rozdział 1, Sekcja 4, Art. 10

2. Procedury zarządzania podatnościami, o których mowa w ust. 1, muszą:
 - (b) zapewniać wykonywanie zautomatyzowanych skanowań podatności i ocen aktywów ICT, przy czym częstotliwość i zakres tych działań muszą być dostosowane do klasyfikacji określonej w art. 8(1) Rozporządzenia (UE) 2022/2554 oraz ogólnego profilu ryzyka danego aktywa ICT.

GravityZone Patch Management umożliwia organizacjom przeprowadzanie zautomatyzowanego skanowania podatności na urządzeniach z systemami Windows, Mac i Linux, a także zapewnia automatyczne wdrażanie poprawek oraz funkcje raportowania wspierające zbieranie dowodów zgodności.

Rozporządzenie delegowane Komisji (UE) 2024/1774, Tytuł 2, Rozdział 1, Sekcja 4, Art. 11

2. Procedura bezpieczeństwa danych i systemów ICT, o której mowa w ust. 1, musi zawierać wszystkie następujące elementy związane z bezpieczeństwem danych i systemów ICT, zgodnie z klasyfikacją określoną w art. 8(1) Rozporządzenia (UE) 2022/2554:
 - (e) Identyfikację środków bezpieczeństwa, które zapewniają, że **wyłącznie autoryzowane nośniki danych**, systemy i urządzenia końcowe mogą być używane do przesyłania i przechowywania danych instytucji finansowej.

Moduł **GravityZone Device Control** dostępny w pakietach GravityZone pozwala organizacjom ograniczać dostęp do urządzeń zewnętrznych na podstawie ich typu i sposobu podłączenia, umożliwiając jednocześnie wyjątki dla urządzeń zidentyfikowanych na podstawie ID urządzenia lub ID produktu.

Dlaczego warto wybrać Bitdefender dla zgodności z DORA i odporności cybernetycznej

- 1. Przyspiesz i uprość zgodność z DORA** – Skorzystaj z innowacyjnych funkcji zarządzania ryzykiem i zgodnością, aby łatwiej spełniać wymagania DORA.
- 2. Obniż koszty i zoptymalizuj bezpieczeństwo dzięki kompleksowemu rozwiązaniu** – Bitdefender oferuje platformę do analizy ryzyka, wzmacniania zabezpieczeń, zapobiegania, ochrony, wykrywania i reagowania, a także Cloud Security Posture Management (CSPM), MDR oraz usługi testowania.
- 3. Wyjdź poza formalną zgodność z DORA – zwiększ odporność cybernetyczną i zarządzanie ryzykiem** wykorzystując najwyższą ocenianą platformę GravityZone, aby podnieść poziom cyberbezpieczeństwa.
- 4. Współpracuj z zaufanym liderem w dziedzinie cyberbezpieczeństwa** – Bitdefender to globalny lider w dziedzinie cyberbezpieczeństwa, z siedzibą główną w Unii Europejskiej.

Uprość zgodność z DORA i zwiększ odporność cybernetyczną dzięki Bitdefender

Skontaktuj się z naszymi ekspertami, aby dowiedzieć się, jak Bitdefender może pomóc w spełnieniu wymagań DORA i innych regulacji oraz zwiększyć odporność cybernetyczną przy mniejszym nakładzie pracy.

[Kontakt](#)

Zastrzeżenie prawne dotyczące korzystania z treści marketingowych Bitdefender

Treści marketingowe są własnością Bitdefender i jego podmiotów stowarzyszonych i podlegają prawom autorskim, znakom towarowym, patentom, tajemnicom handlowym oraz innym prawom własności intelektualnej zgodnie z przepisami prawa Stanów Zjednoczonych, przepisami międzynarodowymi oraz przepisami obowiązującymi w innych krajach.

Wszystkie prezentowane informacje są dostarczane "TAKIE, JAKIE SĄ", wyłącznie w celach informacyjnych. Treści marketingowe nie pociągają za sobą żadnej odpowiedzialności prawnej, gwarancji ani zapewnień. Odbiorca ma obowiązek dokonania własnej oceny.

Bitdefender i jego podmioty stowarzyszone zachowują wszelkie prawa do treści marketingowych, w tym wszelkie prawa własności intelektualnej, tytuły oraz interesy związane z dostarczonymi materiałami, włączając w to wszelkie opinie zwrotne, modyfikacje, dzieła pochodne, rozwinięcia, ulepszenia, tłumaczenia oraz inne formy przetwarzania oryginalnej treści.

Wykorzystanie treści marketingowych jest możliwe wyłącznie po uzyskaniu uprzedniej pisemnej zgody Bitdefender. Po uzyskaniu zgody, użytkownik uzyskuje następujące prawa do korzystania z treści marketingowych Bitdefender:

1.1 Jeśli treść marketingowa ma do 250 znaków (format krótki) – może być reprodukowana w oryginalnej formie;

1.2 Jeśli treść marketingowa przekracza 250 znaków (format rozszerzony) – maksymalnie 30% oryginalnej treści może być reprodukowana bez zmian, natomiast pozostała część musi zostać przekształcona w inny sposób. Zmodyfikowana treść nie może zmieniać celu oryginalnego przekazu, ani negatywnie wpływać na wizerunek oraz markę Bitdefender.