Biała księga

Bitdefender®

ŚWIATOWEJ KLASY OCHRONA UDOSKONALONA O ANALITYKĘ RYZYKA PUNKTÓW KOŃCOWYCH

Spis treści

Przestrzeganie przepisów nie oznacza bezpieczeństwa

W dzisiejszych czasach media są przepełnione doniesieniami o naruszeniach cyberbezpieczeństwa i masowych wyciekach danych. Statystyki branżowe pokazują, że liczba rekordów danych ujawnionych w wyniku tych naruszeń wzrosła ponad dwukrotnie w 2018 r. w porównaniu z 2017 r. Wiele głośnych ataków, które wystąpiły w ostatnim czasie, dotyczyło firm podlegających rygorystycznym wymogom w zakresie przestrzegania przepisów, takich jak Target i Equifax. Wniosek jest taki, że samo spełnienie wymogów prawnych nie wystarczy, aby zapobiec cyberatakom, a przestrzeganie przepisów nie gwarantuje bezpieczeństwa. Cyberprzestępców nie interesują wymogi czy standardy cyberbezpieczeństwa organizacji. Chcą po prostu znaleźć i wykorzystać słabe strony lub luki punktów końcowych w Twoim środowisku. Analiza ekspertów wskazuje, że wiele z tych naruszeń miało wspólny element: dostęp uzyskiwano poprzez „zagrożony punkt końcowy" w środowisku firmy.

Na środowisko przedsiębiorstwa składa się zdumiewająca różnorodność zasobów. Każdy jego element połączony z internetem może być atakowany na setki sposobów. Słabe hasła, luki oprogramowania, błędne konfiguracje i wiele innych wektorów może posłużyć do przejęcia kontroli nad zasobami przedsiębiorstwa i zdobycia punktu zaczepienia w Twojej sieci. Po włamaniu się do sieci, napastnik może szybko poruszać się po całym przedsiębiorstwie, aby zlokalizować i zaatakować istotny zasób – wówczas mamy do czynienia z poważnym naruszeniem. Napastnik może zaatakować i zagrozić bezpieczeństwu Twojego środowiska na milion sposobów i ich połączeń.

Do większości naruszeń danych dochodzi, ponieważ organizacje nie mają pełnej i jasnej wiedzy na temat powierzchni ataku i występowania zagrożonych punktów końcowych. Trudno jest wtedy określić całkowite ryzyko włamania – działa się po omacku.

Uniwersalne wyzwania

W miarę jak organizacje, niezależnie od ich wielkości, przechodzą transformację cyfrową i przestawiają się na chmurę i aplikacje mobilne, ich infrastruktura IT rozrasta się i staje się coraz bardziej złożona. De facto 68% respondentów w badaniu przeprowadzonym przez firmę ESG stwierdziło, że ich środowisko IT stało się bardziej złożone w ostatnich dwóch latach.

Rys. 1.

Stale rosnąca powierzchnia ataku

Minęły już czasy, kiedy cyberbezpieczeństwo polegało jedynie na ochronie punktów końcowych i monitorowaniu sieci wewnętrznych zza zapory sieciowej. Wraz z rozwojem firm w sieci i w chmurze, ich powierzchnia ataku eksplodowała. Szersza powierzchnia ataku i większa złożoność dają innowacyjnym hakerom duże pole manewru.
Środowisko cyfrowe współczesnego przedsiębiorstwa musi mieć łączność z usługami zewnętrznymi, np. w formie wewnętrznych aplikacji w chmurze, lub z zewnętrznymi aplikacjami federacyjnymi. Kluczowym wyzwaniem, które stoi przed administratorami IT i bezpieczeństwa, jest uzyskanie przejrzystego i dokładnego wglądu w powierzchnię ataku przedsiębiorstwa w celu identyfikacji ryzyk i błędnych konfiguracji występujących w punktach końcowych w środowisku.

Aby chronić przed wrogimi działaniami, bezpieczeństwo przedsiębiorstwa musi ewoluować w kierunku szerszym niż tylko ochrona punktów końcowych – jego perspektywa musi się całkowicie zmienić, zważywszy na to, że środowisko punktu końcowego i zainstalowane aplikacje odgrywają większą rolę niż większość zdaje sobie sprawę. Myślenie wyłącznie przez pryzmat ochrony punktów końcowych już się nie sprawdza. Aby zrozumieć ryzyko w organizacji i kontrolować powierzchnię ataku, potrzebny jest wgląd w aktywa organizacji, konfigurację aktywów, używane aplikacje, zabezpieczenia, zachowania użytkowników i wiele więcej.

Niedobór umiejętności w zakresie cyberbezpieczeństwa

W ostatnim badaniu ESG poświęconym największym wyzwaniom stojącym przed organizacjami IT respondenci zostali poproszeni o wskazanie obszarów, w których ich organizacja doświadcza problemu niedoboru umiejętności. W latach 2018-2019 na szczycie listy znalazły się umiejętności z zakresu cyberbezpieczeństwa, które wskazało 53% respondentów. Umiejętności w zakresie architektury/planowania IT znalazły się na drugim miejscu (38%). Niepokojące jest to, że w obu latach deficyt umiejętności z zakresu cyberbezpieczeństwa utrzymywał się na pierwszym miejscu w corocznym badaniu ESG. Tymczasem odsetek organizacji zgłaszających problem niedoboru umiejętności z zakresu cyberbezpieczeństwa wciąż rośnie.

Dotkliwy niedobór umiejętności w skali globalnej sprawia, że organizacje są narażone na większe ryzyko cyberataków. Jak wynika z raportów, do 2020 r. globalny roczny koszt cyberprzestępczości miał przekroczyć 2 biliony dolarów. W miarę pogłębiania się luki kompetencyjnej firmy będą bardziej narażone na cyberprzestępczość i zwiększone ryzyko dotyczące ich infrastruktury i klientów. Czas poszukiwania wykwalifikowanych kandydatów może wydłużać się do 6-9 miesięcy. Rodzi to poważne konsekwencje, zmuszając organizacje do działania w środowisku, w którym występują krytyczne niedobory kadrowe. W rezultacie wielu zespołom bezpieczeństwa IT brakuje zaawansowanych umiejętności w zakresie analityki, badania incydentów i przetwarzania w chmurze. Ponadto presja na posiadane zasoby siły roboczej prowadzi do tego, że mało czasu poświęca się na doskonalenie zawodowe w zakresie cyberbezpieczeństwa, co może wpływać ujemnie na satysfakcję z pracy pracowników zatrudnionych w tym obszarze.

Nadmiar narzędzi

Społeczność cyberbezpieczeństwa nie jest odporna na „syndrom błyszczącego obiektu" (ang. Shiny Object Syndrome), a na rynku aż roi się od dostępnych i nowo powstających atrakcyjnych rozwiązań najróżniejszych problemów z zakresu cyberbezpieczeństwa. Czy Twój zespół bezpieczeństwa nie jest zmęczony nadmiarem narzędzi bezpieczeństwa? Czy nie jest przeciążony ogromem niezarządzanych narzędzi? Czy ma trudności z nadążeniem za napływem informacji, procedur i aktualizacji?

Najnowsze badanie ESG wykazało, że 40% zespołów administratorów bezpieczeństwa IT używa 10-25 narzędzi bezpieczeństwa, podczas gdy 30% używa 26-50 narzędzi. Liczby te są znacznie wyższe w sektorze finansowym, gdzie 73% organizacji używa 35 lub więcej narzędzi. Jednak sedno problemu stanowi nie tyle sama liczba narzędzi, co brak integracji pomiędzy narzędziami i rozproszenie oferowanych przez nie funkcji. (https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf)

Współczesne cyberataki

Atak ransomware WannaCrypt (WannaCry) z 2017 r. siał spustoszenie na całym świecie. WannaCry to robak ransomware, który szybko rozprzestrzenia się w wielu sieciach komputerowych. Po zainfekowaniu komputera z systemem Windows szyfruje on pliki na dysku twardym, uniemożliwiając użytkownikom dostęp do nich. Następnie za ich odszyfrowanie atakujący żądają okupu w bitcoinach.

Oprogramowanie ransomware WannaCry składa się z wielu komponentów. Dostaje się na infekowany komputer w postaci droppera, komponentu ransomware szyfrującego pliki w punkcie końcowym oraz komponentu robaka, który infekuje inne połączone systemy poprzez wykorzystanie niezałatanej luki SMB w systemach MS Windows.

Po zainfekowaniu punktu końcowego WannaCry próbuje uzyskać dostęp do twardo zakodowanego adresu URL (wyłącznika). Jeśli URL jest nieosiągalny, komponent ransomware wyszukuje i szyfruje pliki w wielu popularnych formatach, np. pliki Microsoft Office, JPEG, MP3 i MKV, co uniemożliwia użytkownikowi dostęp do nich. Następnie wyświetla notatkę z żądaniem okupu, domagając się 300 dolarów w bitcoinach za odszyfrowanie i przywrócenie plików.

WannaCry można było powstrzymać

Komponent robaka odpowiedzialny za rozprzestrzenianie się jest oparty na wykorzystującym lukę w SMB exploicie o nazwie EternalBlue, który prawdopodobnie był opracowany przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA). Exploit ten był wykradziony i udostępniony w dark webie przez grupę hakerską zwaną Shadow Brokers. Po przedostaniu się do sieci Windows WannaCry rozprzestrzeniał się sam i bez ludzkiej ingerencji zainfekował inne niezałatane komputery. Ten samonapędzający się mechanizm przyczynił się do jego szybkiego rozpowszechnienia.

Jak na ironię, sam Microsoft odkrył tę lukę i wydał poprawkę zapobiegającą WannaCry jeszcze przed rozpoczęciem ataku. Biuletyn Bezpieczeństwa Microsoftu **MS17-010** wydany 14 marca 2017 r. zaktualizował implementację protokołu SMB w systemie Windows, aby zapobiec infekcji z wykorzystaniem EternalBlue. Mimo że Microsoft oznaczył tę poprawkę jako krytyczną, wiele systemów nadal nie posiadało poprawek w maju 2017 r., kiedy WannaCry zaczął się szybko rozprzestrzeniać. Dla niezałatanych systemów, które zostały zainfekowane, jest niewiele działań naprawczych poza przywróceniem plików z bezpiecznej kopii zapasowej – to pokazuje, jak ważne jest aktualizowanie systemu do najnowszych poprawek bezpieczeństwa.

Pomimo nagłośnienia sprawy – nie wspominając już o poprawkach i najlepszych praktykach zapobiegania zagrożeniu – WannaCry wciąż infekuje systemy. I to nie z powodu braku dostępności środka zaradczego, lecz w konsekwencji niewdrażania poprawek – wyjaśnia to, dlaczego malware taki jak WannaCry może wyrządzać szkody nawet długo po upublicznieniu środka naprawczego. Pokazuje to, jak ważne jest uzyskanie wglądu w ryzyka generowane przez punkty końcowe w środowisku i reagowanie na nie zawczasu.

Aktualnie większym zagrożeniem są warianty WannaCry, a konkretnie nowy malware oparty na tym samym kodzie robaka EternalBlue, co WannaCry. Wszystkie warianty exploitów opartych na EternalBlue wykorzystują tę samą lukę w systemie Windows, zatem fakt rosnącej liczby tych ataków sugeruje, że wiele systemów Windows wciąż nie zostało załatanych. Ich odnalezienie przez atakujących jest kwestią czasu.

Kluczowe zadania ochrony punktów końcowych

Analityka ryzyka i wzmacnianie punktów końcowych

Kompleksowe podejście do bezpieczeństwa środowiska przedsiębiorstwa zaczyna się od zrozumienia jego powierzchni ataku, poprzez identyfikację ryzykownych punktów końcowych, a następnie wzmocnienie ich, aby zminimalizować ich podatność na cyberataki. W Bitdefender traktujemy to jako pierwszy krok do kompleksowej ochrony.

Wzmacnianie punktów końcowych to proces zmniejszania ich powierzchni ataku poprzez:

Hardening systemu operacyjnego – aktualizowanie na bieżąco systemu operacyjnego o najnowsze funkcjonalności, usuwanie zbędnych programów, zabezpieczeń, konfiguracji itp.

Wzmacnianie bezpieczeństwa usług – wyłączanie niepotrzebnych i niepożądanych usług, procesów, opcji i funkcjonalności.

Analityka błędnych konfiguracji punktów końcowych – stałe monitorowanie punktów końcowych pod kątem błędnych konfiguracji, raportowanie i naprawa błędów.

Wzmacnianie bezpieczeństwa aplikacji – aktualizowanie na bieżąco aplikacji o najnowsze łatki i poprawki błędów.

Wiele organizacji w celu bieżącej aktualizacji systemów operacyjnych korzysta z wbudowanych narzędzi systemowych lub narzędzi dostarczanych przez producentów systemów operacyjnych, np. Microsoft SCCM. Inne do zarządzania aktualizacjami używają rozwiązań firm trzecich, które potrafią aktualizować system operacyjny i większość popularnych aplikacji. Niewiele jest narzędzi, które mogą być użyte do identyfikacji i naprawy błędów konfiguracji punktów końcowych. Jednym z takich narzędzi jest niedawno ogłoszony Microsoft Defender ATP Threat & Vulnerability Management, który skanuje punkt końcowy pod kątem błędnych konfiguracji systemu operacyjnego i aplikacji oraz brakujących aktualizacji/łatek w celu sporządzenia wskaźnika podatności na zagrożenia.

Istnieją nieliczne narzędzia umożliwiające wykonanie niektórych lub wszystkich powyższych działań z zakresu wzmacniania bezpieczeństwa. Są one jednak oderwane od siebie, mają osobne konsole zarządzania i często są zarządzane przez odrębne zespoły. Powoduje to zamieszanie i opóźnienia oraz pozostawia luki w ochronie. Niewątpliwie potrzebne jest zintegrowane rozwiązanie zapewniające kompleksową ochronę.

Zintegrowane zapobieganie naruszeniom oparte na analizie ryzyka

Wymagania w zakresie bezpieczeństwa organizacji wynikają z wielu różnych czynników. Wymagania dotyczące cyberbezpieczeństwa niektórych organizacji, np. z sektora finansowego i opieki zdrowotnej, wynikają z konieczności spełnienia wymogów prawnych. Z kolei inne organizacje uznają, że ich wymagania wynikają z wcześniejszych naruszeń lub proaktywnego podejścia do kwestii zapobiegania.

Podejścia te są pomocne, ale nie zapewniają kompleksowego bezpieczeństwa ze względu na ich wąski zakres i wymagania. Skuteczniejszym sposobem na zapewnienie kompleksowej ochrony jest podejście holistyczne obejmujące identyfikację zagrożonych zasobów w środowisku oraz ciągłą ocenę wszystkich punktów końcowych pod kątem podatności, ustawień zabezpieczeń i zapewnienia zautomatyzowanych lub wspomaganych działań naprawczych połączonych z zapobieganiem i monitorowaniem.

Rys. 2.

Jak działa Analityka Ryzyka w Bitdefender

Analityka Ryzyka w GravityZone stale monitoruje wszystkie chronione punkty końcowe pod kątem ponad 200 wskaźników ryzyka (IoR) i oblicza łączne wyniki ryzyka, jak również indywidualne wyniki poszczególnych punktów końcowych. Rezultaty są wyświetlane

na Pulpicie ryzyka z oznaczeniem stopnia nasileniem ryzyka. Jak dotąd, kryteria wykorzystywane w analizie ryzyka opierają się głównie na identyfikacji błędnych konfiguracji punktów końcowych, ponieważ jest to najczęstszy powód naruszeń bezpieczeństwa organizacji.

Błędy konfiguracji punktów końcowych

Błędna konfiguracja systemu jest jednym z częstych powodów naruszeń bezpieczeństwa punktów końcowych - ponad 90% dotychczasowych cyberataków było możliwych, ponieważ punkt końcowy w środowisku był źle skonfigurowany lub brakowało mu odpowiednich ustawień, co umożliwiało atakującemu dostęp do systemu.

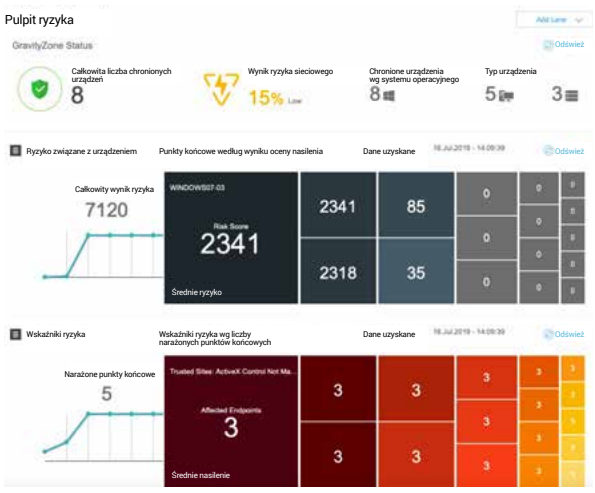
Błędy w konfiguracji systemu, które mogą być wykorzystane przez atakujących, obejmują m.in:

- **Wyłączenie zaawansowanej ochrony**
- **Włączenie usługi Windows Telnet** dla nieszyfrowanych połączeń przychodzących zamiast korzystania z serwerów SSH umożliwia nieautoryzowany dostęp do komputera niepowołanym osobom.
- **Włączone automatyczne logowanie** zmniejsza ochronę konta, umożliwiając dostęp każdemu.
- **Niezabezpieczona lub wyłączona Kontrola konta użytkownika (UAC)** nie będzie informować użytkownika o próbach instalacji nowego oprogramowania lub zmiany ustawień komputera przez niepowołane osoby.
- **Włączony LM Hash**, gdy powinien być domyślnie wyłączony, aby uniknąć ryzyka nieprawidłowego działania mechanizmów szyfrowania i uwierzytelniania haseł.
- **Wyłączony ASLR (Address Space Layout Randomization)** – zmniejsza bezpieczeństwo systemu i powinien być zawsze włączony.
- **Wyłączony tryb ochrony menedżera sesji**
- **Włączone niezabezpieczone logowanie gościa Niezabezpieczone logowanie gościa** obniża bezpieczeństwo klientów Windows. Tej opcji nie należy nigdy włączać, ponieważ konta gościa są bardziej narażone na ataki typu man-in-the-middle.
- **Niewyłączone automatyczne uruchamianie** – powinno być wyłączone (zablokowane), gdyż w przeciwnym razie umożliwia atakującemu wykonanie złośliwego kodu bez wiedzy i zgody użytkownika.

Gdy którykolwiek warunek z powyższych lub pozostałych 206 predefiniowanych warunków zostanie wykryty w punkcie końcowym, wynik ryzyka punktu końcowego wzrasta o wartość zależną od stopnia istotności danego warunku.
Teraz dzięki Analityce Ryzyka administratorzy IT zyskują wszechstronny obraz poziomu cyberbezpieczeństwa firmy. Ogólny wynik ryzyka widoczny w głównym panelu nawigacyjnym jest pochodną indywidualnych wyników ryzyka punktów końcowych. Interfejs użytkownika Analityki Ryzyka Punktu Końcowego (ERA) umożliwia administratorowi przejście od ogólnego wyniku ryzyka do indywidualnego wyniku ryzyka każdego punktu końcowego.

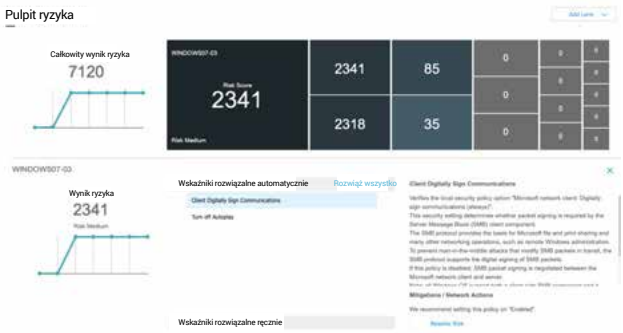
Panel ryzyka GravityZone przedstawiony poniżej (Rys. 3) daje administratorom IT wgląd w profil ryzyka wszystkich punktów końcowych chronionych przy użyciu GravityZone. Główny Panel ryzyka pokazuje ogólny profil ryzyka. Górny rząd pokazuje całkowitą liczbę chronionych urządzeń, wyniku ryzyka: aktualny stan i trend, urządzenia wg OS i rodzaje urządzeń (punkt końcowy lub serwer), itd.

Rys. 3.



Rys. 4.

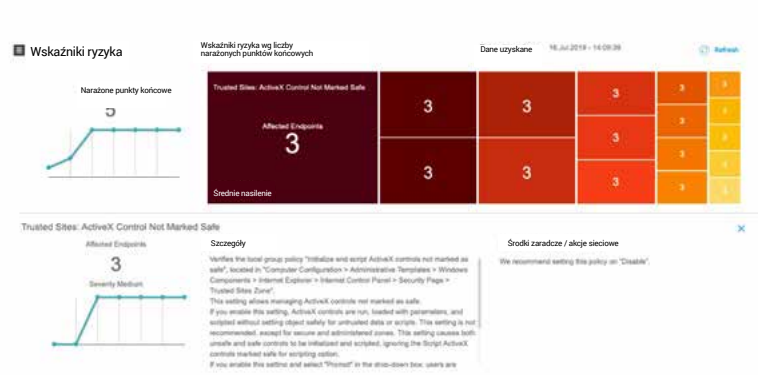
Rys. 5.



Drugi rząd (Rys. 5) ukazuje całkowity wynik ryzyka, a kafelki obrazują wyniki ryzyka poszczególnych punktów końcowych, przy czym punkt końcowy z najwyższym wynikiem ryzyka znajduje się po lewej stronie. Po najechaniu myszką na dane kafelek wyświetlą się dodatkowe szczegóły, takie jak nazwa punktu końcowego, jego rodzaj, kategoria ryzyka, itd. Jeśli klikniemy przycisk „Szczegóły" na kafelku, pojawi się szczegółowe omówienie ryzyka wraz z opcją „Rozwiąż ryzyko" (jeśli ma zastosowanie) lub opisem rozwiązania krok po kroku. Umożliwia to administratorom IT głębsze zrozumienie zakresu ryzyka, na jakie narażone są punkty końcowe. Dostarcza też szczegółowych informacji na temat środków zaradczych, a w niektórych przypadkach udostępnia automatyczną redukcję ryzyka.

Trzeci rząd na Panelu ryzyka (Rys. 6) prezentuje wskaźniki ryzyka (IoR), czyli rodzaje ryzyka występujące w środowisku przedsiębiorstwa. Kolor kafelka sygnalizuje nasilenie ryzyka, a cyfry na środku wskazują liczbę dotkniętych nim punktów końcowych. Po kliknięciu przycisku „Szczegóły" pojawia się szczegółowy opis tych zagrożeń w szerszym widoku, wraz z działaniami zaradczymi, jeśli mają zastosowanie.

Rys. 6.



Podsumowanie

Skuteczne podejście do cyberbezpieczeństwa nie kończy się na wdrożeniu rozwiązań EPP i EDR. Aby nie dać się zaskoczyć ewoluującym zagrożeniom, ważne jest posiadanie wglądu w analitykę ryzyka punktów końcowych. Jej rolą jest stałe monitorowanie punktów końcowych pod kątem różnych kryteriów ryzyka, w tym analiza błędnej konfiguracji punktów końcowych w oparciu o zalecenia *Security baseline* firmy Microsoft oraz kryteriów oceny podatności podanych przez inne firmy. Kompleksowa analityka ryzyka daje administratorom wgląd w poziom zabezpieczeń całej organizacji oraz jej poszczególnych punktów końcowych. Analityka Ryzyka Punktu Końcowego (ERA) umożliwia automatyczną eliminację wielu rodzajów ryzyka za pomocą jednego kliknięcia i podaje zalecane działania naprawcze w przypadku złożonych zagrożeń (wspomagana eliminacja ryzyka). Identyfikacja narażonych punktów końcowych w środowisku IT przedsiębiorstwa i jak najszybsze usuwanie luk bezpieczeństwa znacząco zmniejszy ryzyko wystąpienia naruszenia bezpieczeństwa na dużą skalę. Zarządzanie ryzykiem IT odgrywa kluczową rolę w przedsiębiorstwie, a działania podejmowane przez administratorów już dziś mogą uchronić firmę przed zagrożeniami, które niesie jutro.

Więcej informacji jest dostępnych na stronie: https://bitdefender.pl/gravityzone-enterprise-security

Bitdefender jest globalnym producentem technologii bezpieczeństwa, który dostarcza rozwiązań bezpieczeństwa odbiorcom w ponad 100 krajach przy współpracy z siecią partnerów, dystrybutorów i resellerów. Od 2001 roku Bitdefender konsekwentnie produkuje wielokrotnie nagradzane technologie bezpieczeństwa dla przedsiębiorstw i konsumentów oraz jest wiodącym producentem rozwiązania z zakresu technologii wirtualizacji i chmury. Działania Bitdefender z zakresu badań i rozwoju, sojuszy i partnerstwa wytyczają najwyższe standardy bezpieczeństwa w aspekcie wielokrotnie nagradzanej technologii oraz strategicznych sojuszy z czołowymi światowymi producentami technologii wirtualizacji i chmury.

Więcej informacji jest dostępnych na stronie http://www.bitdefender.com/

Bitdefender-Bialaksiega-WCPERA-CREAT3790-pLPL