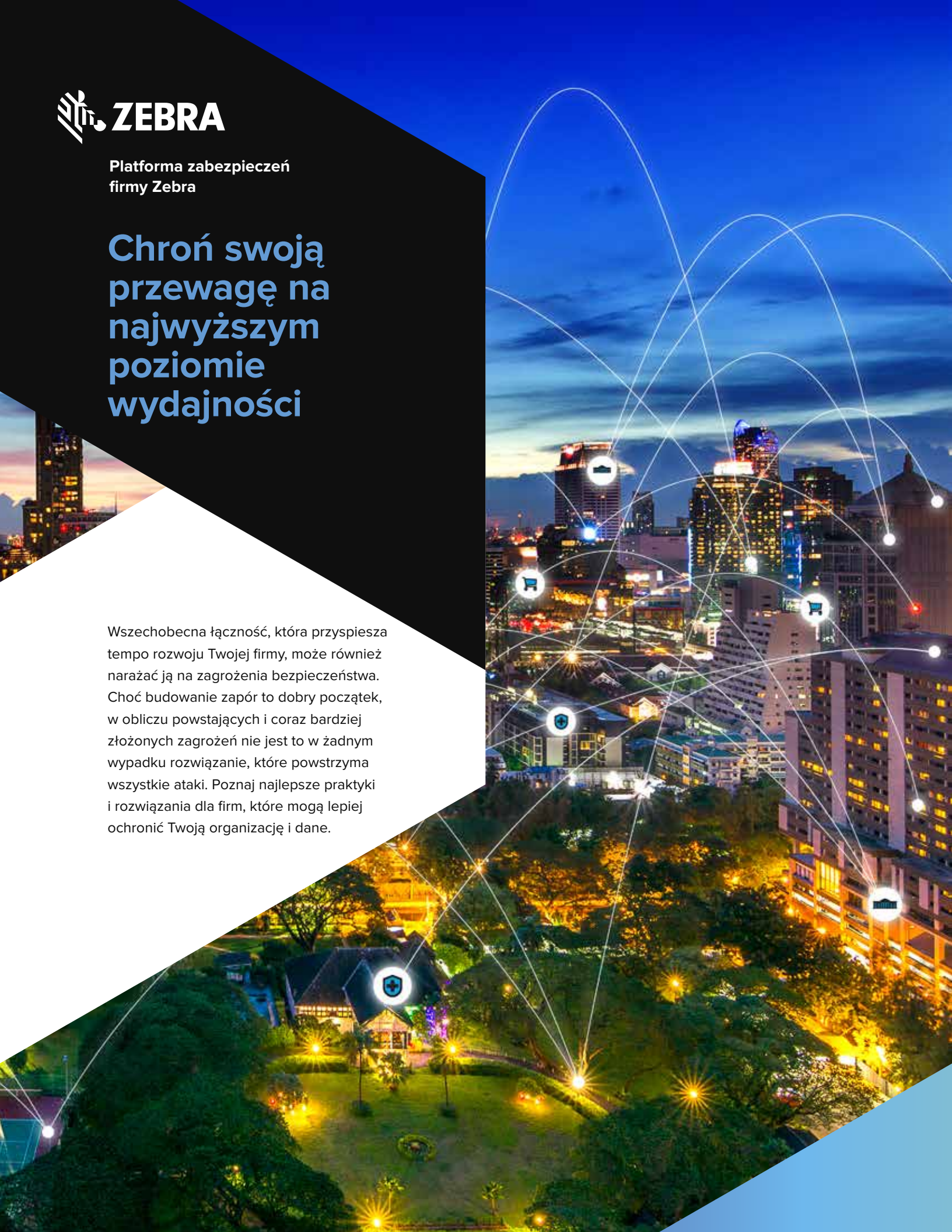
ZEBRA

Platforma zabezpieczeń firmy Zebra

Chroń swoją przewagę na najwyższym poziomie wydajności

Wszechobecna łączność, która przyspiesza tempo rozwoju Twojej firmy, może również narażać ją na zagrożenia bezpieczeństwa. Choć budowanie zapór to dobry początek, w obliczu powstających i coraz bardziej złożonych zagrożeń nie jest to w żadnym wypadku rozwiązanie, które powstrzyma wszystkie ataki. Poznaj najlepsze praktyki i rozwiązania dla firm, które mogą lepiej ochronić Twoją organizację i dane.



Jak uniemożliwić zagrożeniom bezpieczeństwa uniemożliwienie działania Twojej firmie?

Bezpieczeństwo to sprawa nadrzędnej wagi

Numery kart kredytowych. Dokumentacja medyczna. Numery użytkowników systemu ubezpieczeń społecznych i świadczeń socjalnych. Hasła. Niezależnie od tego, czy Twoja firma świadczy usługi na rzecz klientów, pacjentów, czy też obywateli, oczekuje się od niej — a często wymaga prawnie — gwarantowania prywatności danych osobowych.

Zagrożenia będą coraz większe

W miarę upływu czasu proces ten będzie się stawać tylko coraz trudniejszy. Nie ulega wątpliwości, że Internet Rzeczy i technologia chmury łączą ze sobą ludzi i informacje w niespotykany dotąd sposób, zapewniając Twojej organizacji bezprecedensowy wgląd i kontrolę operacyjną. Choć perspektywy na przyszłość są ekscytujące, nie są one pozbawione ryzyka.

Szacowane 50 mld[1] połączonych ze sobą urządzeń, które mają pojawić się do 2022 roku, może spowodować narażenie organizacji i poufnych danych na niezliczone zagrożenia związane ze słabymi punktami. Cyberprzestępcy, zachęcani wysokimi zyskami i niskim prawdopodobieństwem poniesienia konsekwencji za swoją działalność (zaledwie pięć procent hakerów zostało doprowadzonych przed wymiar sprawiedliwości[2]), nie wykazują zamiaru zwolnienia tempa.

Czym ryzykujemy?

Zaledwie jeden incydent związany z naruszeniem bezpieczeństwa danych może pociągnąć za sobą wysoką cenę, powodując straty finansowe i spadek produktywności, a także narazić na szwank renomę firmy.

Co możemy zrobić? Bezpieczeństwo należy traktować poważnie. Nawet jeżeli Twoja organizacja dysponuje programem zabezpieczeń, istnieje prawdopodobieństwo, że błędne przekonania osłabią jego integralność i niepotrzebnie doprowadzą do powstania słabych punktów.

3,9 mln USD:
średni koszt incydentu naruszenia bezpieczeństwa danych[3]

25.575 zapisów:
średni rozmiar incydentu naruszenia bezpieczeństwa danych[3]

12 godzin:
średnia ilość czasu, jaki zajmuje 88% hakerów złamanie zabezpieczeń chroniących cyberprzestrzeń[4]

197 dni:
średnia ilość czasu, jaki zajmuje organizacjom zorientowanie się, że doszło do naruszenia bezpieczeństwa.[3]

Cele:

Handel detaliczny:
80% ruchu związanego z logowaniem się na strony detalistów prowadzących sprzedaż online przypisuje się hakerom korzystającym ze skradzionych danych[5]

Administracja publiczna/ sektor publiczny:
sektor stanowiący główny cel ataków, których kluczowymi czynnikami motywującymi jest działalność szpiegowska i korzyści finansowe[6]

Ochrona zdrowia:
drugi pod względem częstości sektor, będący celem 15% cyberataków[6]

Produkcja:
sektor, w którym w ciągu ostatnich kilku lat poziom incydentów związanych z naruszeniem bezpieczeństwa powodowanym działalnością szpiegowską był wyższy niż we wszystkich innych branżach[6]

Nie pozwól, by błędne przekonania osłabiły Twoje zabezpieczenia

Pomimo ogromnej liczby szeroko nagłaśnianych incydentów związanych z bezpieczeństwem, wiele organizacji wciąż wykazuje beztroską postawę w kwestii bezpieczeństwa. Nie daj się zwieść złudnemu poczuciu bezpieczeństwa — wstępowanie w firmie poniższych przekonań może oznaczać kłopoty.

„Moja organizacja nie jest wystarczająca duża, aby stanowić cel ataków”.

Celem 43% cyberataków są małe przedsiębiorstwa.[6] Hakerzy wykorzystują to, że małym przedsiębiorstwom często brakuje zasobów i wiedzy. Mogą nawet wykorzystać Twoją organizację do uzyskania dostępu do Twoich powiązań z większymi podmiotami.

„Chroni nas nasza sieć”.

Solidny program bezpieczeństwa to sprawa wieloaspektowa, którą należy stale rozwijać. Zamknięcie na klucz drzwi wejściowych nie powstrzyma złodzieja przed wejściem przez okno, jeśli zostawimy je otwarte. Jedno z badań wykazało nawet, że tradycyjne środki zaradcze, takie jak zapory i programy antywirusowe, prawie nigdy nie spowalniały hakerów, za to bardziej skuteczne w powstrzymywaniu ataków były technologie zabezpieczające punkty końcowe.[4]

„Nie doszło u nas do naruszenia bezpieczeństwa, więc nasze zabezpieczenia działają dobrze”.

Z tego, że do naruszenia już doszło, można zwyczajnie nie zdawać sobie sprawy. Badania pokazują, że samo tylko wykrycie przez firmę takiego incydentu może potrwać nawet aż 197 dni.[3]

„Dysponujemy już formalnym programem bezpieczeństwa”.

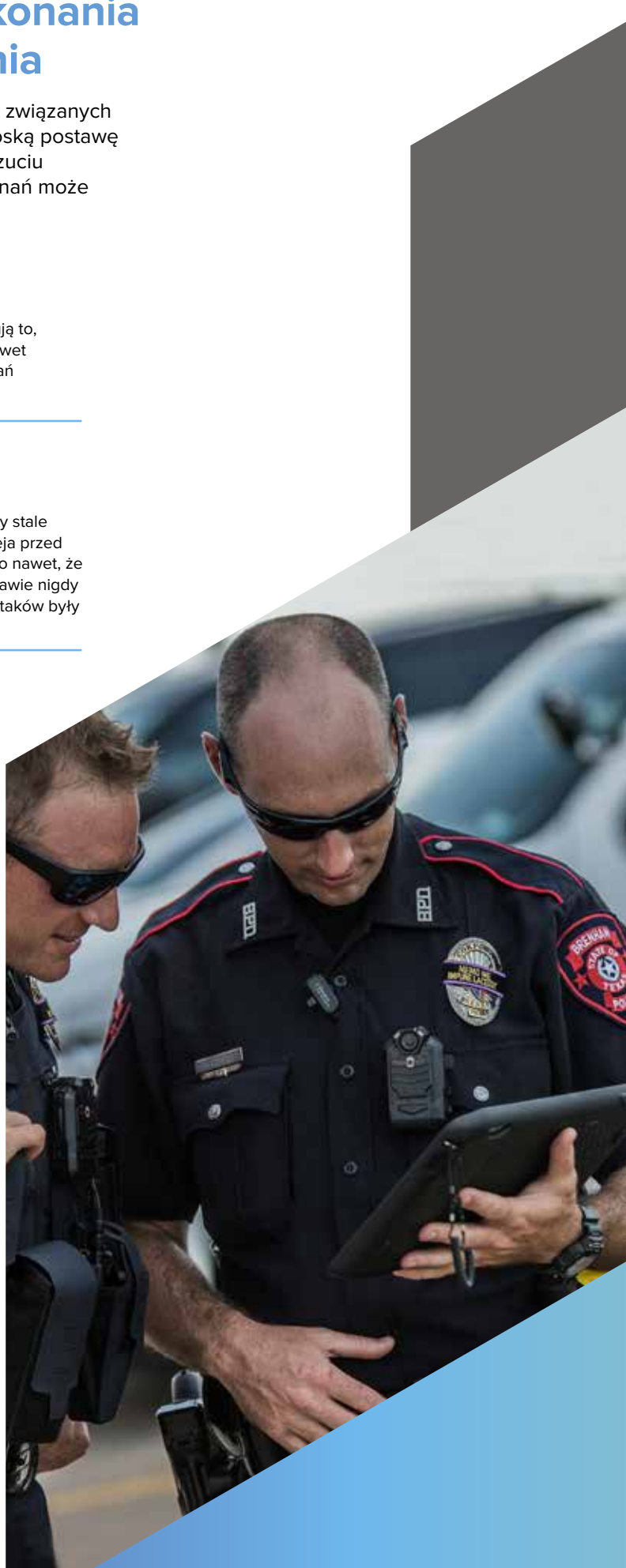
Doskonale. Czy program ten stale ewoluuje, aby nadążyć za nieustannie zmieniającymi się zagrożeniami? Czy obejmuje całą technologię firmy? Podejście typu „jeden i gotowe” nie jest wystarczające, jeśli chodzi o dzisiejszych wyrafinowanych cyberprzestępców.

„Bezpieczeństwo to problem zbyt skomplikowany”.

Dobrze zaprojektowane zabezpieczenia są intuicyjne i łatwe do wdrożenia. Można liczyć na płynność ich działania, której potrzebują pracownicy, oraz prostotę zarządzania nimi, której potrzebuje dział informatyczny.

„Zabezpieczenia mają niekorzystny wpływ na produktywność”.

Zarzuty takie jak twierdzenie, że systemy bezpieczeństwa są uciążliwe, zbyt trudne do zintegrowania lub że opóźniają procesy operacyjne, są niestety bardzo powszechne. Naruszenie bezpieczeństwa może jednak nie tylko utrudnić, ale całkowicie zatrzymać pracę. Rozwiązaniem jest dobór takiej technologii, w którą funkcje bezpieczeństwa zostały wbudowane już na etapie projektowania. W ten właśnie sposób zabezpieczenia mogą wspierać, a nie hamować produktywność.



Ochraniaj swoją organizację za pomocą wielu warstw zabezpieczeń

Nie wszystkie środki bezpieczeństwa są w stanie zaspokoić Twoje potrzeby. Rozważając wybór rozwiązań technicznych, należy wziąć pod uwagę poniższe kluczowe atrybuty bezpieczeństwa, wbudowane w technologie firmy Zebra i zapewniające spokój ducha.

Wbudowana ochrona i wydajność:
Wybierz markę, która od samego początku integruje ze swoimi technologiami zabezpieczenia i funkcje zwiększające produktywność. Przekonasz się, że nasze rozwiązania są celowo projektowane tak, aby zwiększać wydajność, a jednocześnie płynnie włączać szereg wysoce efektywnych protokołów i funkcji bezpieczeństwa.

Zautomatyzowane funkcje bezpieczeństwa:
Certyfikaty Wi-Fi®, których ukończenie kiedyś zajmowało Twojemu działowi informatycznemu kilka tygodni, teraz mogą być wykonywane automatycznie, przyspieszając tworzenie bezpiecznego środowiska połączonych urządzeń dla Ciebie i Twojego zespołu.

Możliwość dostosowania do swoich potrzeb:
Wolisz ustawiać własny poziom tolerancji zabezpieczeń? Zebra ułatwia to zadanie, oferując konfigurowalne rozwiązania, które umożliwiają dostosowanie poziomu bezpieczeństwa w zależności od potrzeb firmy lub działu.

Prostsza konserwacja i serwisowanie:
Możesz mieć pewność, że nasze funkcje bezpieczeństwa, oprogramowanie i sprzęt zostały opracowane i przetestowane tak, aby działać przy minimalnych wymogach konserwacyjnych i maksymalnym czasie sprawności. Ponadto w razie potrzeby do dyspozycji masz nasz całodobowy zespół serwisowy.

Płynna integracja:
Z firmą Zebra możesz cieszyć się zaletami płynnej i szybkiej integracji. Dzięki naszemu dogłębnemu zrozumieniu Twojej branży i zastosowań, nasze rozwiązania od podstaw projektujemy tak, aby przewidywały i zaspokajały Twoje potrzeby integracyjne.

Ciągła czujność i wsparcie:
Lata aktualizacji zabezpieczeń systemu operacyjnego i ulepszeń oprogramowania układowego łączymy z rozwiązywaniem problemów, oceną podatności i współpracą w zakresie bezpieczeństwa wewnętrznego.

Postępowanie zgodnie z uznanymi na całym świecie najlepszymi praktykami:
Zyskaj spokój, wiedząc, że Zebra przestrzega najlepszych praktyk i wytycznych ustalonych przez światowych ekspertów w dziedzinie bezpieczeństwa, w tym ISO, National Institute of Standards and Technology (NIST) oraz Center for Internet Security Benchmark Controls. Nasze produkty i rozwiązania są wykorzystywane do zastosowań, które pomagają organizacjom spełniać wymogi HIPAAA, PCI-DSS i GDPR (RODO).

Lider w dziedzinie technologii bezpiecznych przedsiębiorstw:
Połącz siły z firmą, która wzmocniła system operacyjny Google Android™ dla przedsiębiorstw i oferuje do dziesięciu lat wsparcia w zakresie bezpieczeństwa dla systemu operacyjnego. Od wzmocnionych komputerów mobilnych klasy korporacyjnej po bezpieczne drukarki i wizjonerskie technologie — przekonasz się, że wydajność i bezpieczeństwo są podstawą wszystkiego, co robimy.

Produkty, rozwiązania i usługi firmy Zebra
Wsparcie dla każdego etapu ram cyberbezpieczeństwa NIST Cybersecurity Framework

IDENTYFIKACJA	Monitorowanie zarządzania ryzykiem Kreator oceny bezpieczeństwa drukarek — Printer Security Assessment Wizard Usługi specjalistyczne	Zarządzanie ryzykiem w łańcuchu dostaw Komitet ds. bezpieczeństwa
OCHRONA	LifeGuard™ for Android Tryb chroniony drukarek Kontrola nad urządzeniami	Aktualizacje PrintSecure Automatyczne zarządzanie certyfikatami Wi-Fi Ramy zarządzania ryzykiem
WYKRYWANIE	Aplikacja do zarządzania drukarkami Printer Profile Manager Enterprise Monitorowanie bezpieczeństwa	Wykrywanie w czasie rzeczywistym
REAGOWANIE	Zarządzanie urządzeniami Środki zaradcze w razie wykrycia zagrożenia	Reagowanie na incydenty Powiadomienia dla klientów
NAPRAWA	Usługi specjalistyczne Wzmocnienia	Przywracanie do stanu znanego

Zabezpieczanie przewagi na najwyższym poziomie wydajności

Bezpieczeństwo ma kluczowe znaczenie dla Twojej działalności i procesów roboczych. Dlatego właśnie firma Zebra proaktywnie chroni przed lukami w zabezpieczeniach, integrując ze swoimi rozwiązaniami wiele warstw ochrony. Urządzenia, technologie i usługi firmy Zebra są projektowane z myślą o ochronie bez ograniczania wydajności pracy. Przekonasz się, że nasze zabezpieczenia są łatwe do wdrożenia i że zapewnią Twoim pracownikom pierwszej linii płynne działanie. Nasza inteligentna, konfigurowalna technologia umożliwia równoważenie celów operacyjnych i bezpieczeństwa w czasie rzeczywistym, w realnym świecie. Zdaj się na firmę Zebra, aby zyskać spokój ducha, który pomoże Ci wdrożyć strategie biznesowe i technologiczne na najwyższym poziomie wydajności.

ZEBRA

Sprawdź, jak nasze standardy bezpieczeństwa poprawią Twoje

Odwiedź stronę **www.zebra.com/product-security**

Źródła:
1. Juniper Research, 2018 r. **2.** „Carbon Black Incident Response Threat Report", listopad 2018 r.
3. Badanie „Cost of Data Breach" na rok 2018 i 2019, Ponemon Institute **4.** „Black Report", Nuix 2017 r.
5. „Shape Credential Spill Report" 2018 r. **6.** „Verizon 2019 Data Breach Investigations Report"