



Zapewnienie bezpieczeństwa transformacji cyfrowej

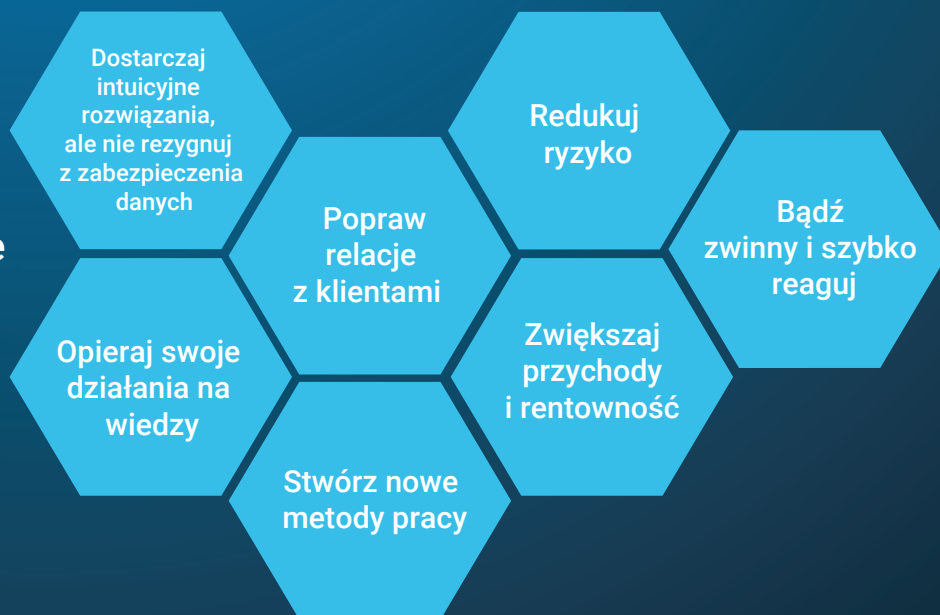
Rozwiązania NTT i Cisco dla bezpieczeństwa firm

Cyberataki i incydenty bezpieczeństwa w ostatnich miesiącach odbiły się szerokim echem w świecie IT, zmuszając przedsiębiorstwa do skierowania uwagi i środków na ten obszar, a także do poszukiwania partnerów mogących pomóc w realizacji działań pozwalających sprostać coraz to nowym zagrożeniom. Partnerstwo pomiędzy firmami Cisco i NTT łączy wiodące w branży możliwości produktowe z uznaną i sprawdzoną skutecznością oraz sprawnością działania.

Cyfrowa agenda dla biznesu

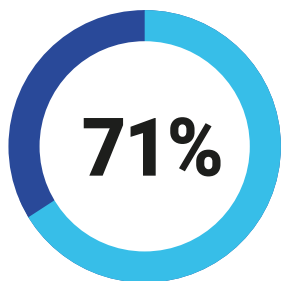
Od wielu lat współpracujemy z przedsiębiorstwami na całym świecie i wiemy, jakie cele próbują osiągnąć w działaniach online. Jest to długa lista, która obejmuje m.in: poprawę relacji z klientami, zaoferowanie pracownikom nowych sposobów pracy, współpracy i osiągania produktywności, podejmowanie decyzji na bazie gromadzonych danych, zwiększenie sprawności działania oraz kreatywne i innowacyjne wyróżnienie się na rynku. Wszystkie te cele muszą być realizowane przy jednocześnie stałym zmniejszaniu ryzyka, złożoności i oczywiście zwiększaniu przychodów i rentowności. Skala wyzwań jest więc ogromna.

Bezpieczne rozwiązania mają kluczowe znaczenie dla sukcesu firmy

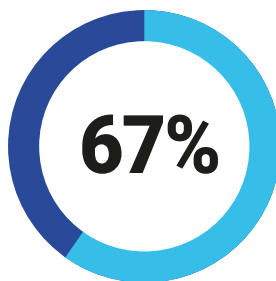


Bezpieczeństwo jest podstawą sukcesu

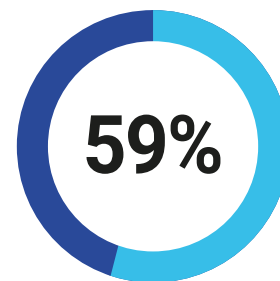
U podstaw każdej inicjatywy wspierającej transformację cyfrową leży bezpieczeństwo.



Bezpieczeństwo jest najważniejszą technologią w strategii cyfrowej¹



Zaufanie cyfrowe tworzy największą wartość organizacji w ich strategii cyfrowej¹



Firmy, które dostosowały się do wymogów RODO, są narażone na mniejszą skalę i niższy koszt naruszeń bezpieczeństwa danych²

Niezależnie od tego, czy chodzi o cyfrowe miejsca pracy i mobilność, tworzenie bardziej spersonalizowanych doświadczeń klientów, usprawnianie procesów czy modernizację IT - wszystko musi być realizowane z uwzględnieniem bezpieczeństwa. Bezpieczeństwo powinno być wbudowane we wszystkie obszary w sposób, który zwiększa przejrzystość, kontrolę i spójność całego procesu, a także odciąża działy IT. Specjaliści mają bowiem inne wyzwania, związane z nowymi technologiami i zagrożeniami, które ewoluują wraz z powiększaniem się obszaru występowania ataków, błyskawicznie rosnącymi zasobami danych i zwiększającą się złożonością środowisk.

Cyfryzacja przynosi nowe wyzwania w zakresie bezpieczeństwa

Przez ostatnie lata mogliśmy obserwować, jak przedsiębiorstwa podchodzą do wyzwań związanych z cyfryzacją. W miarę postępów w realizacji cyfrowych rozwiązań, zmienia się sama natura systemu IT, oferując wspaniałe nowe możliwości, ale także zwiększając złożoność i ryzyko.

Brak granic

Tradycyjny obszar działania został przededefiniowany wraz z ekspansją przedsiębiorstw w kierunku chmury, urządzeń brzegowych i mobilnych.

Modernizacja aplikacji

Aplikacje są projektowane (lub zmieniana jest ich architektura), tak aby działały w wielu środowiskach i korzystały z usług, których żaden dział IT nie jest w stanie w 100% kontrolować.

Dbłość o dane

Aplikacje, urządzenia i użytkownicy generują potężną ilość danych, które wymagają szczególnej uwagi w zakresie autoryzacji, dostępności, ochrony i prywatności.

“Z każdym nowym połączeniem wiąże się odpowiedzialność w zakresie kierowania i zarządzania nowymi podatnościami na naruszenia zabezpieczeń i ochroną prywatności. Firmy muszą radzić sobie z zagrożeniami związanymi z danymi wraz z osiąganiem nowych poziomów wydajności i doświadczeń klientów.”

- David Reinsel, SVP, IDC Global DataSphere

Rosnące wyzwania w zakresie bezpieczeństwa

Z każdym dniem jest coraz więcej urządzeń IoT

Do 2025 roku 41,6 mld urządzeń będzie PODŁĄCZONYCH do sieci³

Elementy pracy i aplikacje są przenoszone do chmury

Do 2025 roku 80% przetwarzania danych w firmach zostanie przeniesionych do chmury⁴

Skutki finansowe

Średni całkowity KOSZT NARUSZEŃ BEZPIECZEŃSTWA DANYCH wynosi 3,92 mln USD rocznie⁵

Użytkownicy pracują w dowolnym miejscu na różnych urządzeniach

Do 2025 roku prawie 80% CAŁEGO RUCHU W SIECI będzie pochodzić z urządzeń bezprzewodowych i mobilnych⁶

Bezpośredni dostęp do internetu w firmach o rozproszonej strukturze

Z analiz wynika, że średnie tempo wzrostu rynku SD-WAN w latach 2018 – 2023 wyniesie 74%, dzięki wzmożonemu popytowi na usługi DIA (Direct Internet Access)⁷

Zagrożenia są liczniejsze i nieustanne

Ryzyko doświadczenia naruszenia ochrony danych WZROSŁO DO PONAD 29% w 2019 r.⁵

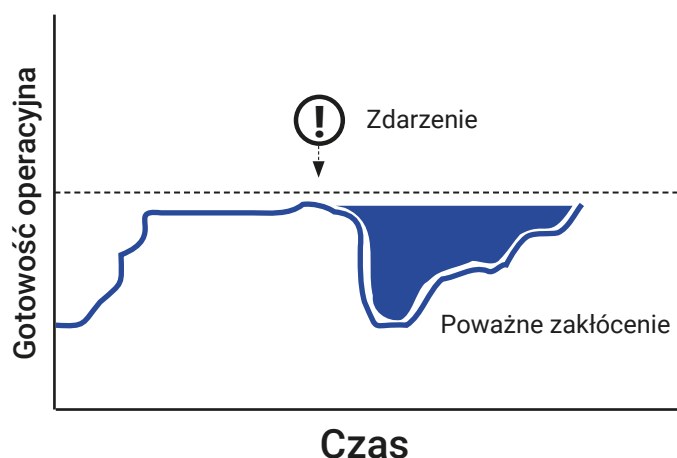


Jak stać się proaktywnym i przewidyującym

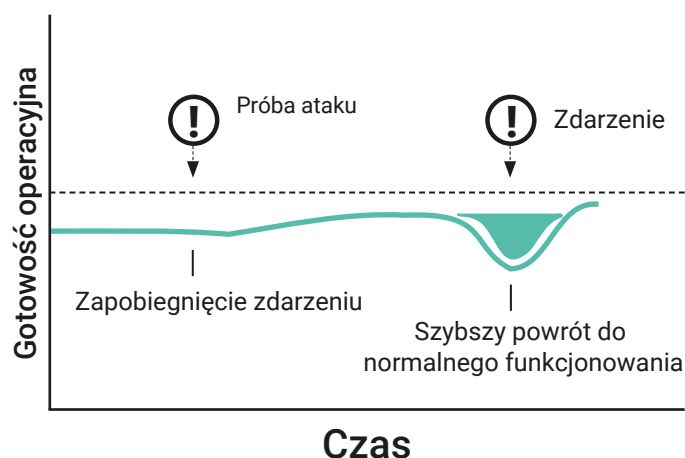
Aby przejść z trybu reaktywnego do proaktywnego i predykcyjnego, konieczne jest wprowadzenie szeregu zmian w strategii. Starsze modele bezpieczeństwa, oparte w dużej mierze na ochronie brzegowej i zaporach sieciowych, choć są istotne, po prostu już nie wystarczają. Bez kompleksowego podejścia, obejmującego każdą warstwę bezpieczeństwa, użytkownik będzie nadal narażony na ataki i inne poważne i długotrwałe konsekwencje.

Zwiększ gotowość operacyjną dzięki informacjom otrzymywanym w czasie rzeczywistym, pozwalającym zapobiegać atakom lub położyć im kres.

Model postępowania reaktywnego



Model postępowania predykcyjnego



Jak przedsiębiorstwa mogą bronić się przed atakami

Specjaliści z dziedziny IT zdają sobie sprawę, że aby uzyskać bardziej kompleksowe, całościowe podejście do bezpieczeństwa, zwiększenie możliwości obrony przed atakami musi obejmować wiele obszarów. Lista tematów, którymi należy się zająć jest długa, ale wymienimy te, które są kluczowe:



Nastawienie na bezpieczeństwo

Zadbaj o cyberbezpieczeństwo we wszystkich działaniach, począwszy od podstawowej strategii biznesowej



Skalowalne rozwiązania

Wdrażaj skalowalne narzędzia pierwszej linii obrony, takie jak platformy bezpieczeństwa w chmurze



Segmentacja sieci

Stosuj segmentację sieci, aby ograniczyć ryzyko rozprzestrzenienia ataku



Przewidywanie zagrożeń

Zapewnij sobie dostęp do aktualnych i dokładnych informacji o zagrożeniach dla systemów monitorowania bezpieczeństwa i obsługi zdarzeń



Łagodzenie skutków ataku

Przestrzegaj zasad ograniczonego dostępu i odpowiedzialnego przetwarzania danych



Ochrona punktów końcowych

Stosuj narzędzia nowej generacji do monitorowania procesów w punktach końcowych

NNT i Cisco pomagają identyfikować, ograniczać skutki i reagować na zagrożenia bezpieczeństwa

Nie da się przewidzieć, kiedy dojdzie do próby naruszenia cyberbezpieczeństwa – fakt, że to się stanie, jest bezsporny. Pytanie nie brzmi: czy, ale kiedy? Wraz ze wzrostem popularności ransomware i innych zagrożeń, kluczowe znaczenie ma ochrona przed, w trakcie i po ataku. Produkty Cisco wyposażone w wielowarstwową ochronę w połączeniu z usługami bezpieczeństwa firmy NTT dostępnymi przez cały cykl eksploatacyjny produktu, pomagają klientom wzmocnić ochronę ich systemów firmowych poprzez przygotowanie na ataki i szybką reakcję.

Pomagamy firmom mieć wgląd w działanie sieci i aplikacji, wykrywać i eliminować zagrożenia, kontrolować dostęp użytkowników oraz reagować na incydenty i rozwiązywać je. Cisco i NTT pomagają w upraszczaniu systemów IT i wspierają innowacje, tak aby organizacje mogły konkurować w dzisiejszym środowisku biznesowym, wymagającym bezpieczeństwa w każdym obszarze.

Razem pomożemy Twojej organizacji:

Redukować ryzyko

Dbać o zapewnienie bezpieczeństwa we wszystkich inicjatywach związanych z transformacją cyfrową

Przewidywać zagrożenia i proaktywnie im zapobiegać

Identyfikować możliwe zagrożenia i zabezpieczać się przed atakami, zanim one nastąpią

Szybko likwidować skutki

Natychmiast identyfikować, reagować i ograniczać siłę rażenia ataku, aby jak najszybciej powrócić do normalnej działalności

Zapewniać zgodność z przepisami

Dostosowywać działania do rosnącej liczby przepisów poprzez zwiększoną przejrzystość, automatyzację i sprawniejsze raportowanie

Nieustannie wprowadzać innowacje

Zadbać o to, żeby podejście do cyberbezpieczeństwa i plan działań w zakresie technologii odpowiadały obecnym i przyszłym potrzebom

Client success

Jak Cisco Umbrella chroni firmę produkującą odzież sportową

Wyzwanie

Międzynarodowa firma produkująca odzież sportową miała trudności z reagowaniem w czasie rzeczywistym na zagrożenia. Nie była też w stanie blokować ataków złośliwego oprogramowania, phishingu i ransomware. Konieczne było szybkie poprawienie bezpieczeństwa w całej firmie, aby zmniejszyć ryzyko i podjąć bardziej proaktywne działania.

Współpraca NTT i Cisco

Nasze wspólne rozwiązanie obejmowało Cisco Advanced Threat Security, Cloud Security i Umbrella, które ułatwiają wdrażanie i zarządzanie, a także usprawniają automatyzację komponentów Cisco i zwiększają bezpieczeństwo.

Rezultat

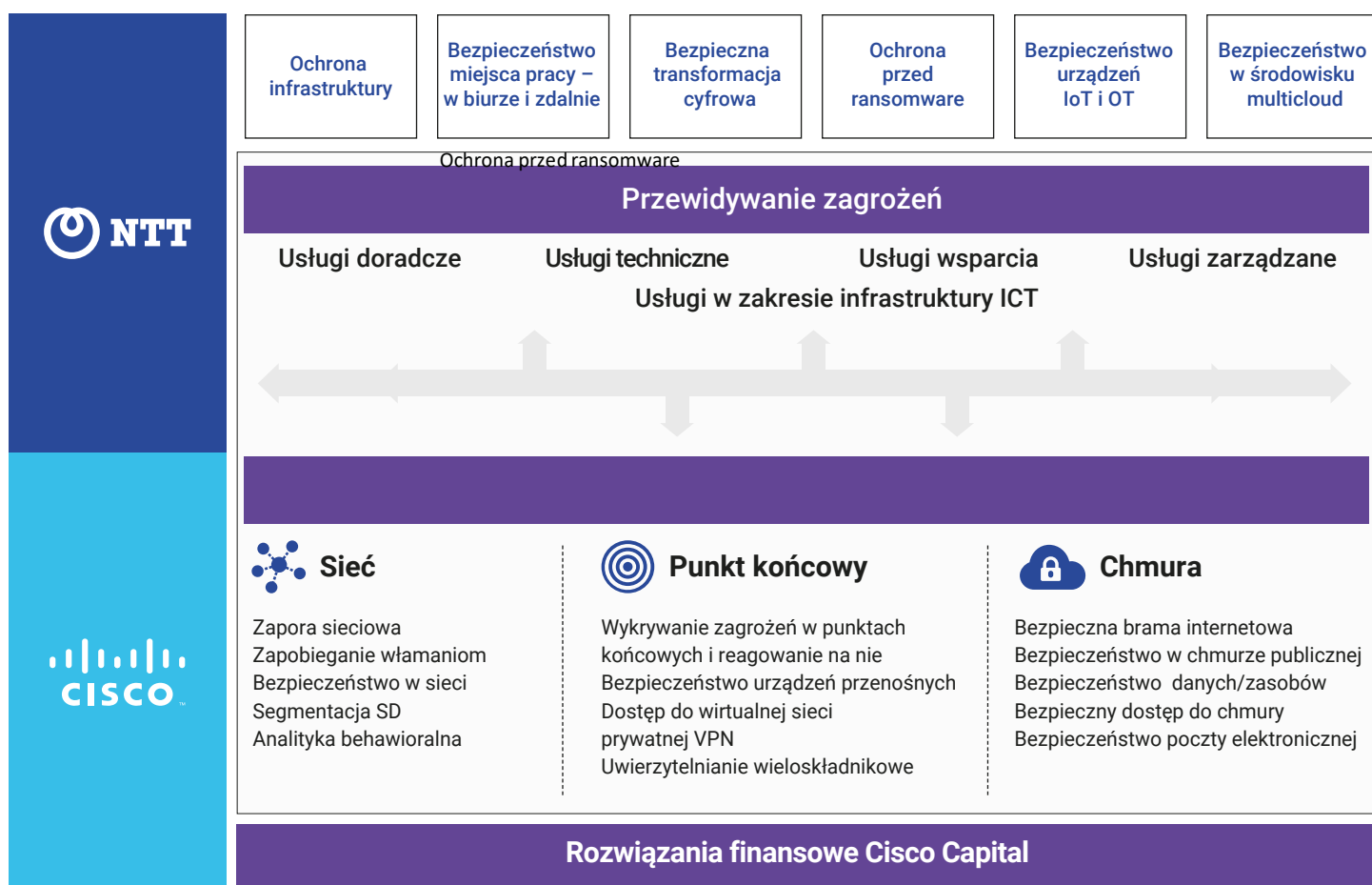
Oprócz zwiększenia widoczności zagrożeń, firma poprawiła bezpieczeństwo sieci i rozszerzyła ochronę użytkowników poprzez blokowanie phishingu, złośliwego oprogramowania i ransomware - przy jednoczesnym obniżeniu kosztów dzięki uproszczonemu wdrażaniu i zarządzaniu.

Rozwiązania bezpieczeństwa Cisco i NTT

Łączymy wiedzę ekspertów w dziedzinie bezpieczeństwa, sieci, chmury i centrów danych z najlepszymi praktykami i procesami, elastycznymi programami finansowymi i zaopatrzeniowymi, najlepszą w swojej klasie technologią, a także pełnym cyklem życia usług w zakresie bezpieczeństwa.



Nasze rozwiązania i usługi w zakresie cyberbezpieczeństwa



Usługi NTT w zakresie bezpieczeństwa



Usługi zarządzane w dziedzinie bezpieczeństwa

Kompleksowe zarządzanie infrastrukturą bezpieczeństwa i operacjami zapewniające Twojej firmie bezpieczeństwo i zgodność z przepisami.

- Usługi wykrywania zagrożeń
- Monitorowanie bezpieczeństwa przedsiębiorstw
- Zarządzanie urządzeniami zabezpieczającymi
- Zarządzanie podatnością na zagrożenia



Usługi doradcze w zakresie bezpieczeństwa

Ochrona kluczowych aktywów firmy poprzez efektywne korzystanie z zasobów i stosowanie kontroli we właściwych miejscach.

- Usługi w zakresie tworzenia strategii bezpieczeństwa
- Usługi w zakresie monitorowania bezpieczeństwa
- Usługi w zakresie zarządzania bezpieczeństwem, ryzykiem i zgodnością
- Usługi w zakresie architektury i projektowania rozwiązań w dziedzinie bezpieczeństwa
- Usługi w zakresie zarządzania i reagowania na incydenty bezpieczeństwa



Usługi wsparcia

Przyspieszenie dostępności i zmniejszenie złożoności operacyjnej w środowisku hybrydowym.

- Usługi wsparcia w zakresie utrzymywania sprawności
- Usługi wsparcia w zakresie działań proaktywnych



Usługi techniczne

Wsparcie w szybkim i skutecznym projektowaniu i wdrażaniu inicjatyw transformacji cyfrowej.

- Usługi projektowe
- Zarządzanie projektem i programem
- Rozwiązania w zakresie kadr
- Usługi wdrażania i integracji

Dlaczego NTT i Cisco?

Od ponad 28 lat pracujemy razem, aby wspomagać organizacje na całym świecie w wykorzystywaniu technologii do wprowadzania innowacji.



Służymy naszym globalnym doświadczeniem klientom
w 47 krajach

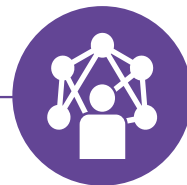
Posiadamy wspólne centra innowacji
na całym świecie, żeby szybciej zaspokajać potrzeby klientów



Codziennie analizujemy 9,5 terabajtów danych,
żeby pomóc Ci znaleźć igłę w stogu siana

Łącznie pracuje dla nas ponad 6 000

specjalistów ds. bezpieczeństwa cybernetycznego na całym świecie



Obsługujemy ponad 5000
wspólnych klientów na całym świecie

Jesteśmy zaangażowani społecznie
na rzecz ludzi, społeczeństwa i naszej planety



Jak możemy Ci pomóc osiągnąć kolejny sukces?

Więcej informacji na temat rozwiązań NTT i Cisco w zakresie bezpieczeństwa dla przedsiębiorstw można znaleźć na stronie <http://www.cisco.com/go/cybersecurity-ntt>.

Źródła:

- NTT 2019 Digital Means Business Benchmarking Report
- Cisco 2019 Data Privacy Benchmark Study
- IDC forecast, "The Growth in Connected IoT Devices," June 2019
- Oracle's Top 10 Cloud Predictions 2019

- Ponemon, Cost of a Data Breach Study, 2019
- <https://cybersecurityventures.com/mobile-security-report-2017/>
- Apps Run The World, "Top 10 SD-WAN Software Vendors, Market Size and Market Forecast 2018-2023", Dec 2019

