W Stanach Zjednoczonych, tylko na serwery rządowe przeprowadzanych jest dziennie ponad 4 000 ataków. Roczna wartość płaconych z tego tytułu okupów mieści się w przedziale między 287 a 574 mln USD. A przecież ransomware, Stany Zjednoczone i komputery rządowe, to tylko wierzchołek góry lodowej. Jeśli dodamy do tego mnogość zagrożeń, botnetów, malware'u, to wyłaniający się obraz przekonuje, że to najgroźniejsza i najszybciej rosnące kategorie zagrożeń sieciowych – niebezpieczne i kosztowne.
W świecie, gdzie błyskawicznie rośnie liczba pracowników korzystających z urządzeń mobilnych działających poza swoimi naturalnymi, dobrze chronionymi sieciami korporacyjnymi, gdzie często się korzysta z połączeń VPN, a działający software jest najczęściej udostępniany jako usługa (SaaS), niezbędne się okazały system chroniące użytkowników przed złośliwym oprogramowaniem, praktycznie niezależnie od kontekstu lokalizacji i typu połączenia. Dlatego na pierwszej linii frontu walki z cybernetycznym zagrożeniem stanęły systemy klasy Secure Internet Gateway (SIG).
Ochrona chmur i styku sieci korporacyjnych z Internetem jest koniecznością i bezwzględnym wymogiem bezpieczeństwa.
Impact Report by 451 Research
Przykładem praktycznej realizacji tej koncepcji jest działającą w chmurze Cisco Umbrella Suite – zestaw programów i rozwiązań zapewniających widoczność zagrożeń i ochronę przed nimi niezależnie od lokalizacji użytkownika i typu wykorzystywanych połączeń z Internetem. Dla Cisco pakiet Umbrella jest kolejnym krokiem w realizacji strategii Cisco Security Everywhere i efektem przejęcia sprzed dwóch lat firmy OpenDNS. Eksperci oceniają, że ten ruch zapewnił Cisco mocną pozycję w szybko rozwijającym się obszarze multi-tenant cloud security, gdzie zacięta konkurencja obejmuje graczy na skalę Symantec (Blue Coat), Forcepoint I Barracuda, oraz innowacyjne startupy takie jak Alert Logic i zScaler.

# 1. Jak to działa?

Cisco Umbrella jest bezpieczną bramą internetową, która potrafi się uczyć identyfikacji i rozpoznawania internetowych zagrożeń, która rozumie zagrożenia i chroni użytkownika nie tylko przed znanymi formami ataków, ale także tymi, które będą się dopiero pojawiać, atakując dowolne porty i protokoły. Rozwijanie przez Cisco technologii sieci intuicyjnych pozwoliło na wypracowanie mechanizmów automatycznego blokowania dostępu do szkodliwych domen, adresów URL, IP, czy plików jeszcze przed nawiązaniem połączenia.

## 2. Wydajność z użyciem z Big Data

Cisco Umbrella każdego dnia obsługuje ponad 100 miliardów zapytań. Są one zestawiane i badane pod kątem korelacji z 11 miliardami historycznych zapisów w bazie danych. Taka analiza informacji, z użyciem technologii Big Data, pozwala na szybką identyfikację wzorców szkodliwych zachowań, wykrywanie anomalii ruchu sieciowego i tworzenie modeli umożliwiających automatyczne określenie, jak wygląda infrastruktura przygotowywana przez cyberprzestępców w celu wykonania kolejnych ataków. W końcu cyberprzestępcy też gdzieś muszą testować swoje nowe generacje złośliwego oprogramowania.

## 3. Szybka integracja z produktami SIEM i rozwiązaniami Sandboxowymi

W sieciach korporacyjnych Infrastrukturalna integracja Cisco Umbrella z technologią Cisco Cloudlock Cloud Access Security Broker pozwala na identyfikację wykorzystywanych aplikacji SaaS i przez to na wymuszanie obowiązującej w firmie polityki bezpieczeństwa i blokowanie aplikacji stwarzających jakiekolwiek ryzyko i zagrożenie. Cisco Umbrella to platforma otwarta, łatwo integrująca się z istniejącymi w firmie systemami, urządzeniami i narzędziami do zapewnienia cybernetycznego bezpieczeństwa firmowych urządzeń, danych i aplikacji.

## 4. Gwarancja wysokiej dostępności systemu

Dla końcowego użytkownika Cisco Umbrella praktycznie nie istnieje – działanie w chmurze oznacza, że nic nie trzeba instalować ani aktualizować. Odpowiedni zestaw urządzeń sieciowych Cisco zapewnia bezpieczeństwo niezależnie od tego, czy pracownik jest połączony, czy nie, do sieci korporacyjnej. Co ważne – mimo wykorzystania bardzo zaawansowanych mechanizmów maszynowego uczenia i wysokiego stopnia komplikacji samych algorytmów, końcowy użytkownik nie odczuje żadnego spowolnienia swojej pracy z codziennym zestawem danych i aplikacji. Zastosowanie mechanizmów „automated failover" gwarantuje najwyższą, praktycznie stuprocentową dostępność systemu.

## 5. Skuteczność

Dla administratorów i menedżerów odpowiedzialnych za bezpieczeństwo infrastruktury IT Cisco Umbrella jest bardzo pomocnym narzędziem. Technologia Cisco Stealthwatch monitoruje ruch sieciowy, ujawnia nietypowe zdarzenia — na przykład zarażenie oprogramowaniem ransomware, a potem wysyła ono ostrzeżenie, że system jest zagrożony. Nawet jeśli zdarzy się, że plik zdoła przeniknąć przez warstwę DNS i zaporę, rozwiązanie

Cisco Advanced Malware Protection (AMP) dla punktów końcowych zablokuje jego uruchamianie. Dzięki ciągłej i stałej analizie aktywność pliku w systemie możliwe jest jego znalezienie i usunięcie wszystkich jego kopii.
Dzięki Cisco Umbrella, tak groźny ransomware może już nie być aż tak straszny, co nie znaczy, że można go lekceważyć. Żadna metoda czy technologia nie zapewni całkowitego i bezpieczeństwa na zawsze. Jednak w zdecydowanej większości przypadków zostanie on zatrzymany na pierwszej linii walki – w warstwie DNS, i to jeszcze zanim będzie w stanie dotrzeć do końcowego urządzenia. Umbrella blokuje żądania pliku wysyłane do infrastruktury klucza szyfrowania, a przez to oprogramowanie ransomware nie jest w stanie nawiązać komunikacji wstecznej i uzyskać informacji niezbędnych do zaszyfrowania danych.