

ExtremeControl

Najważniejsze cechy

Bezpieczny dostęp do sieci

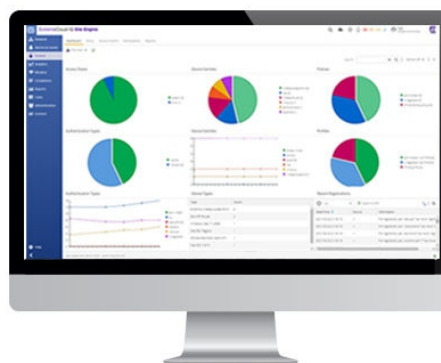
- Oparta na rolach kontrola dostępu do sieci dla wszystkich urządzeń sieciowych, w tym innych producentów
- Bezpieczny dostęp gości i wprowadzanie do sieci urządzeń BYOD
- Integracja z rozwiązaniami innych producentów, takimi jak NGFW, SIEM, CMDB, systemy bezpieczeństwa czy EMM/MDM
- Bezpieczny dostęp do sieci urządzeń IoT

Efektywność operacyjna

- Automatyczne powiadomienia o zmianach wydajności
- Zarządzanie, polityki, kontrola dostępu i analityka aplikacji dostępne z jednego interfejsu
- Szybsze rozwiązywanie problemów, przez rozdzielenie sieci i aplikacji

Dopasowanie do potrzeb biznesowych

- Kontekstowe i spójne polityki, od brzegu sieci po centrum danych
- Zabezpieczanie dostępu do sieci przed nieautoryzowanymi użytkownikami i niedostatecznie chronionymi urządzeniami końcowymi
- Wsparcie dla krytycznych projektów biznesowych związanych z BYOD i IoT



Zabezpieczanie obszaru brzegowego sieci poprzez rozwiązania bezpieczeństwa dla urządzeń końcowych

Ponieważ większość naruszeń bezpieczeństwa danych ma swój początek na poziomie urządzeń końcowych, niezbędna jest szczegółowa kontrola użytkowników oraz urządzeń IoT w sieci, a także stosowanie spójnych polityk w całym środowisku sieciowym, w tym we wdrożeniach multi-cloud. Dzięki aplikacji ExtremeControl stanowiącej element rozwiązania Extreme-Cloud IQ - Site Engine¹, administratorzy sieci posiadają scentralizowany i szczegółowy obraz oraz kontrolę wszystkich punktów końcowych w sieci - z poziomu jednego, elastycznego i prostego w obsłudze dashboardu.

ExtremeControl zapewnia bezpieczeństwo środowisk BYOD i IoT chroniąc w ten sposób sieć przed zewnętrznymi zagrożeniami. Oferuje scentralizowane zarządzanie i możliwość zdefiniowania szczegółowych polityk dla spełniania wymagań zgodności z regulacjami, a także lokalizowania i uwierzytelniania użytkowników i urządzeń oraz stosowania wobec nich dedykowanych polityk.

ExtremeControl integruje się z większością popularnych platform korporacyjnych, w tym z rozwiązaniami z dziedziny bezpieczeństwa sieci, zarządzania mobilnością, analitycznymi, cloud i centrami danych. Oprócz tego oferuje interfejs API typu Northbound dla realizacji własnych integracji z kluczowymi platformami biznesowymi.

¹ ExtremeCloud IQ - Site Engine rozszerza możliwości rozwiązania do zarządzania siecią z poziomu chmury o urządzenia innych producentów oraz produkty nie wspierające natywnie usług cloud. Zapewnia również elastyczność zarządzania siecią w środowiskach cloud i/lub lokalnych.

Szczegółowe polityki

ExtremeControl pozwala na stosowanie szczegółowych środków kontroli dla użytkowników i urządzeń posiadających dostęp do sieci. Administratorzy mogą wdrażać inicjatywy związane z BYOD, dostępem gości i IoT poprzez definiowanie polityk opierających się na stanie bezpieczeństwa urządzeń.

ExtremeControl wiąże urządzenia końcowe z atrybutami takimi jak użytkownik, czas, położenie, stopień ochrony czy typ dostępu, aby stworzyć tożsamość kontekstową obejmującą wszystkie te elementy. Oparte na rolach tożsamości podążają za użytkownikami, niezależnie od tego z jakiego miejsca i jak łączą się z siecią. Mogą one być wykorzystane do egzekwowania bardzo bezpiecznych polityk dostępowych, zabezpieczających sieć przed nieautoryzowanymi użytkownikami i niewystarczająco chronionymi urządzeniami końcowymi.

Administratorzy mogą centralnie zarządzać bezpieczeństwem profili dostępu, co może obejmować połączenie sieci VLAN, identyfikatorów usług (L2 VSN, L3 VSN), list ACL na warstwach L2-L7 oraz reguł QoS na warstwach L2-L7, które odnoszą się do rodzaju sieci, fabric lub non-fabric. ExtremeControl pozwala także na automatyczną dystrybucję bezpiecznych profili dostępu do urządzeń sieciowych i kontrolerów Wi-Fi, a także konwertuje te profile do list dACL (downloadable ACL) na potrzeby instalacji na przełącznikach i routerach. Ponadto, bezpieczne profile dostępu mogą być przypisane do portu urządzenia sieciowego lub w sposób dynamiczny, na podstawie uwierzytelnienia użytkownika lub urządzenia, jako lista ACL, dynamiczna lub pobierana.

Integracja z różnymi ekosystemami

ExtremeControl integruje się z rozwiązaniami partnerów Extreme Networks, aby zwiększać poziom bezpieczeństwa sieci i poprawiać reagowanie na zagrożenia. Przykładowo, rozwiązanie ExtremeControl jest zintegrowane z firewallami następnej generacji i może zarządzać izolowaniem punktów końcowych i działaniami korygującymi na podstawie otrzymywanych alertów. Na potrzeby efektywnego egzekwowania polityk na poziomie firewalli, ExtremeControl przekazuje kontekstowe informacje takie jak użytkownicy, adresy IP i lokalizacje. Polityki oparte na mapowaniach ID-IP podążają za użytkownikami. ExtremeControl oferuje również obsługę polityk dla rozwiązań innych producentów poprzez listy ACL oparte na użytkownikach, w ten sposób zapewniając szczegółową kontrolę całej sieci. Aby chronić sieć przed dostępem niezgodnych i niezatwierdzonych urządzeń uproszczony został proces integracji z partnerami technologicznymi EMM/MDM, takimi jak VMware Workspace ONE UEM (Airwatch), Citrix i MobileIron.

Rozbudowane raportowanie

ExtremeControl ułatwia monitorowanie problemów w sieci, dzięki jednemu, intuicyjnemu dashboardowi. Prezentuje on informacje w ramach rozbudowanych i edytowalnych raportów, a także powiadomienia o uwierzytelnieniach, dostępie gości, dodaniu nowych urządzeń, oraz dane o stanie systemu, profilach urządzeń itp. W przypadku dużych projektów możliwe jest ograniczenie ryzyka, dzięki możliwości testowania nowych polityk lub stosowania pasywnych polityk dla scenariuszy „co-jeżeli”, przed wdrożeniem takiej polityki. Extreme Control identyfikuje zagrożenia przez profilowanie i śledzenie użytkowników i urządzeń, a także poprzez monitorowanie stanu zabezpieczeń i zgodności urządzeń, przed i po uzyskaniu przez nie dostępu do sieci. ExtremeControl może także obsługiwać audyty polityk w ramach zintegrowanych rozwiązań MDM/EMM innych producentów, w celu sprawdzenia czy polityki działają prawidłowo lub ich egzekwowania. Mogą być również prezentowane raporty o liczbie wystąpień oraz stanie urządzeń uznanych za niezgodne, o ograniczonym dostępie do sieci - wraz dodatkowym kontekstem dotyczącym miejsca, czasu i sposobu dostępu. ExtremeControl zapewnia audytorom i zespołom ds. bezpieczeństwa dane niezbędne do podejmowania decyzji w zakresie stosowania polityk dostępowych.

Specyfikacja

Urządzenia wirtualne

ExtremeControl dla ExtremeCloud IQ - Site Engine może być zainstalowane jako urządzenie wirtualne, pobierane przez klientów po zakupie. Wirtualne instancje ExtremeControl muszą być zainstalowane na serwerze VMware lub Hyper-V.

- Urządzenia wirtualne VMware Management Center są spakowane w formacie plików OVA (zdefiniowanym przez VMware)
- Urządzenia wirtualne Hyper-V Management Center są spakowane w formacie plików ZIP

Informacje o skalowalności urządzeń wirtualnych dostępne są w notach wersji.

Obsługiwane przeglądarki internetowe

Poniżej wymieniono obsługiwane przeglądarki internetowe na komputery PC oraz urządzenia mobilne łączące się z siecią poprzez portal captive Extreme Control.

Komputery PC

- Microsoft Edge: 41 i nowszy
- Microsoft Internet Explorer: 11 i nowszy
- Mozilla Firefox: 34 i nowszy
- Google Chrome: 33.0 i nowszy

Urządzenia mobilne

- Internet Explorer Mobile: 11 i nowszy (Windows Phone)
- Microsoft Edge: Wszystkie wersje
- Microsoft Windows 10 Touch Screen Native (Surface Table): N/A
- iOS Native: 9 i nowszy
- Android Chrome: 4.0 i nowszy
- Android Native: 4.4 i nowszy
- Dolphin: Wszystkie wersje
- Opera: Wszystkie wersje

Informacje dotyczące zamawiania

Kod produktu	Opis produktu
Korporacyjne licencje subskrypcyjne NAC	
XIQ-NAC-S-1K-EW	Subskrypcja ExtremeCloud IQ NAC SaaS i wsparcie ExtremeWorks SaaS dla 1 tys. systemów końcowych (1 rok)
XIQ-NAC-S-10K-EW	Subskrypcja ExtremeCloud IQ NAC SaaS i wsparcie ExtremeWorks SaaS dla 10 tys. systemów końcowych (1 rok)
XIQ-NAC-S-100K-EW	Subskrypcja ExtremeCloud IQ NAC SaaS i wsparcie ExtremeWorks SaaS dla 100 tys. systemów końcowych (1 rok)
XIQ-NAC-S-1K-PWP	Subskrypcja ExtremeCloud IQ NAC SaaS i wsparcie PartnerWorks Plus SaaS dla 1 tys. systemów końcowych (1 rok)
XIQ-NAC-S-10K-PWP	Subskrypcja ExtremeCloud IQ NAC SaaS i wsparcie PartnerWorks Plus SaaS dla 10 tys. systemów końcowych (1 rok)
XIQ-NAC-S-100K-PWP	Subskrypcja ExtremeCloud IQ NAC SaaS i wsparcie PartnerWorks Plus SaaS dla 100 tys. systemów końcowych (1 rok)

Usługi i wsparcie techniczne

Extreme Networks oferuje pełną gamę usług, od usług profesjonalnych wspomagających projektowanie, wdrażanie i optymalizowanie sieci komputerowych klientów, przez dedykowane szkolenia techniczne, po usługi wsparcia technicznego dopasowane do indywidualnych potrzeb każdego klienta. Prosimy o kontakt z Państwa przedstawicielem w Extreme Networks w celu uzyskania dodatkowych informacji w tym zakresie.

Informacje dodatkowe

Jeżeli chcą Państwo uzyskać więcej informacji zapraszamy do odwiedzenia naszej strony internetowej: www.extremenetworks.com lub skontaktowania się z nami: kreski@kreski.pl