Extreme
Connect Beyond the Network

EXCLUSIVE NETWORKS
KARTA PRODUKTU

Najważniejsze cechy

Dopasowanie do potrzeb biznesowych

- Dzięki opartym na kontekście politykom cele biznesowe mogą wskazywać kierunki rozwoju sieci
- Ochrona danych korporacyjnych poprzez aktywną ochronę sieci przed dostępem nieautoryzowanych użytkowników, niezabezpieczonych punktów końcowych i innych podatnych systemów
- Bezpieczna realizacja krytycznych projektów np. BYOD i IoT
- Skuteczne równoważenie bezpieczeństwa i dostępności dla użytkowników, wykonawców i gości
- Efektywna realizacja wymagań zgodności z różnego rodzaju regulacjami
- Polityka cenowa dopasowana do potrzeb biznesowych - opłata za użytkownika

Bezpieczeństwo

- Dynamiczna i oparta na rolach kontrola dostępu do sieci wykorzystująca kontekstowe informacje o tożsamości
- Ścisła integracja z rozwiązaniami innych producentów takimi jak NGFW, CMDB, ochrona aktywności internetowej i EMM/MDM
- Aktywna ochrona dostępu gości oraz procesu wprowadzania urządzeń do sieci w ramach BYOD
- Wbudowane możliwości profilowania urządzeń za za pomocą zewnętrznych i wewnętrznych technik
- Wbudowane funkcje oceniania stanu zabezpieczeń systemów końcowych, przy udziale rozwiązań agentowych i bezagentowych

Efektywność operacyjna

- Szczegółowe i intuicyjne możliwości konfiguracji polityk oraz narzędzia do rozwiązywania problemów
- Natywne możliwości obsługi infrastruktury od różnych dostawców
- Elastyczne możliwości wdrożenia - rozwiązania fizyczne i wirtualne klasy korporacyjnej
- Proste wdrożenie na jednym urządzeniu dzięki wbudowanym funkcjom AAA i Radius, portalowi, profilowaniu urządzeń i serwerowi oceniającemu
- Obsługa wielu metod uwierzytelniania i autoryzacji (AD, LDAP, lokalne)

ExtremeControl™

Kontrola użytkowników i urządzeń w sieci przewodowej i bezprzewodowej wraz ze szczegółową widocznością. Wszystko realizowane z poziomu jednej centralnej lokalizacji.

Do zarządzania złożonymi środowiskami sieciowymi, w których występują urządzenia IoT i BYOD konieczne jest zastosowanie innego niż dotychczas stosowanego podejścia, w przeciwnym wypadku trudno zabezpieczyć takie sieci przed atakami typu ransomware i innymi cyber-zagrożeniami. Dzięki szczegółowej widoczności i kontroli użytkowników, urządzeń i aplikacji w całym środowisku sieciowym, od rdzenia po brzeg sieci, ExtremeControl upraszcza zarządzanie usługami mobilności. Pozwala uzyskać doskonałą wydajność, skalowalność i wysoką dostępność całej infrastruktury. Nasze rozwiązanie do kontroli dostępu oferuje scentralizowaną i szczegółową widoczność i kontrolę wszystkich punktów końcowych w sieciach przewodowych i bezprzewodowych w ramach jednego, prostego, elastycznego i łatwego w obsłudze panelu sterowania.

ExtremeControl pozwala na bezpieczne wdrożenie BYOD i zabezpiecza sieć przed zewnętrznymi zagrożeniami. Pozwala na centralne zarządzanie i definiowanie szczegółowych polityk, dzięki czemu możliwa jest realizacja wymagań dotyczących zgodności z różnego rodzaju regulacjami, usługi lokalizacyjne, uwierzytelnianie i aplikowanie dedykowanych polityk wobec użytkowników i urządzeń. Nasze rozwiązanie pozwala na wprowadzanie polityk w całej sieci przy zachowaniu bezpieczeństwa klasy korporacyjnej dla usług BYOD i IoT. Rozwiązanie dostosowuje się do potrzeb biznesowych naszych klientów, można rozpocząć od małego wdrożenia, które potem może osiągnąć znaczną skalę.

Nasze rozwiązanie kontroli dostępu jest zintegrowane z wiodącymi platformami korporacyjnymi, w tym rozwiązaniami z dziedziny bezpieczeństwa, zarządzania mobilnością w przedsiębiorstwach, analityki, usługami dostępnymi w chmurze oraz centrami danych. Ponadto, oferuje otwarty interfejs API typu Northbound pozwalający na tworzenie własnych integracji z kluczowymi platformami korporacyjnymi.

ExtremeControl to samodzielny produkt stanowiący element rozwiązania Extreme Management Center, które zapewnia w ramach jednego interfejsu niezbędne informacje, widoczność i kontrolę, przekładając się na doskonałą jakość doświadczeń użytkowników. Dzięki możliwościom integracji, konsolidacji oraz automatyzacji oferowanym przez ExtremeControl możliwe jest szybkie identyfikowanie i powstrzymywanie zagrożeń oraz wdrażanie działań naprawczych.

Świadczone przez nas usługi specjalistyczne w ramach oferty Professional Services wspierają klientów podczas projektowania, wdrażania i optymalizowania sieci. Ponadto, oferują dostosowane do potrzeb klientów szkolenia techniczne oraz usługi wsparcia.

Bezpieczeństwo sieci dzięki szczegółowej kontroli polityk i widoczności

ExtremeControl umożliwia stosowanie szczegółowych środków kontroli i pozwala określić kto, co, kiedy, gdzie i w jaki sposób może połączyć się z siecią. Można bezpiecznie wdrażać usługi BYOD, IoT oraz dostęp gości dzięki politykom czasu rzeczywistego opartym na stanie bezpieczeństwa urządzeń. ExtremeControl łączy punkty końcowe z atrybutami takimi jak użytkownik, czas, położenie, podatność lub typ dostępu, tworząc w ten sposób kompleksową i kontekstową tożsamość danego elementu infrastruktury. Oparte na rolach tożsamości podążają za użytkownikiem, niezależnie od tego z jakiego miejsca i jak łączy się z siecią. Mogą być również stosowane do egzekwowania bardzo bezpiecznych polityk dostępu.

Możliwość ustanowienia szczegółowych polityk i ich automatycznego skalowania na całą sieć pozwala na łatwe uzyskanie zgodności z wewnętrznymi i zewnętrznymi regulacjami. Za pomocą jednego kliknięcia możliwe jest egzekwowanie kontekstowych polityk wobec urządzeń uwzględniających QoS, pasmo i inne parametry w dostosowaniu do potrzeb biznesowych. Zaawansowane raportowanie wszystkich udanych i nieudanych prób uwierzytelniania użytkowników oraz aktualizowana na bieżąco tabela stanu wszystkich podłączonych do sieci urządzeń i użytkowników, pozwala powiadamiać administratora o potencjalnych problemach.

W obliczu nieustannie zmieniającej się sieci można stosować tzw. mikrosegmentację dla uzyskania spójności zabezpieczeń, bez potrzeby wprowadzania złożonych zmian w konfiguracji sieci. Podczas wdrażania dużych projektów można ograniczyć ryzyko poprzez testowanie nowych polityk oraz stosowanie pasywnych polityk dla przed produkcyjnych scenariuszy „co-jeżeli". ExtremeControl pozwala identyfikować zagrożenia przez profilowanie i śledzenie użytkowników i urządzeń, a także monitorowanie stanu zabezpieczeń i zgodności urządzeń przed i po uzyskaniu przez nie dostępu do sieci. Dzięki audytom polityk oraz raportom dotyczącym przypadków zastosowania polityk możliwe jest przeprowadzanie ocen sieci.

Bezpieczny dostęp gości do sieci i usługi BYOD

Dzięki znajomości tożsamości użytkowników możliwe jest stosowanie automatycznego rejestrowania gości bez udziału pracowników działu IT. Nasze rozwiązanie automatycznie nadzoruje ważność konta, kontroluje czas aktywności oraz jego aktywność, bez angażowania pracowników IT. Możliwe jest bezpieczne i łatwe wprowadzanie do sieci gości i urządzeń BYOD przy zastosowaniu funkcji sponsoringu, do tego dochodzą szerokie możliwości brandowania i dostosowania usługi do potrzeb klienta. Wbudowane zewnętrzne i wewnętrzne techniki profilowania dają pewność, że tylko urządzenia zgodne z politykami organizacji mogą uzyskać dostęp do sieci.

Aby chronić sieci naszych klientów przed dostępem niezgodnych i nieautoryzowanych urządzeń ułatwiamy integracje z rozwiązaniami naszych partnerów EMM/MDM takich jak Airwatch, Citrix i MobileIron.

Ponadto, dostępne są wbudowane funkcje agentowego i bezagentowego oceniania stanu zabezpieczeń systemów, z możliwością integracji zewnętrznych rozwiązań takich jak skanery zabezpieczeń urządzeń końcowych.

Wprowadzanie nowych urządzeń BYOD oraz gości do sieci jest bardzo łatwe i bezpieczne dzięki samoobsługowemu portalowi, który oferuje możliwość uwierzytelniania poprzez wiadomość SMS lub portale społecznościowe. W ten sposób użytkownicy mogą zarządzać urządzeniami w zgodzie z politykami biznesowymi. Urządzenia są automatycznie wprowadzane do sieci, profilowane i określany jest poziom zabezpieczeń zgodny z obowiązującymi politykami. Jednocześnie, użytkownicy mogą korzystać ze swoich własnych urządzeń w sieci, bez pomocy ze strony pracowników IT.

Mniejsza liczba luk bezpieczeństwa dzięki ocenie stanu zabezpieczeń systemów końcowych

ExtremeControl oferuje dwie opcje oceniania urządzeń końcowych - agentową i bezagentową. Agent stały lub tymczasowy może być zainstalowany na systemie końcowym klienta lub może być on pobrany z portalu captive. Oprogramowanie agentowe może być również zainstalowane poprzez system do masowej dystrybucji oprogramowania taki jak Group Policy czy System Center Configuration Manager. Bezagentowe ocenianie nie wiąże się z koniecznością instalacji lub uruchamiania jakiegokolwiek oprogramowania na systemie końcowym.

Rozszerzanie integracji z narzędziami bezpieczeństwa poprzez firewalle następnej generacji

ExtremeControl jest zintegrowane z naszym eko-systemem partnerów pozwalając na rozszerzanie bezpieczeństwa sieci i możliwości reagowania na zagrożenia. W oparciu o informacje z firewalli następnej generacji, możliwe jest zarządzanie procesem izolowania punktów końcowych i działaniami korygującymi. Na potrzeby egzekwowania polityk przez obwodowe firewalle udostępniane są kontekstowe informacje takie jak dane o użytkownikach, adresach IP czy lokalizacji. Polityki oparte na powiązaniach ID z IP podążają za użytkownikami.

Pełna widoczność sieci dzięki zaawansowanym funkcjom raportowania i powiadamiania

ExtremeControl ułatwia proces monitorowania problemów występujących w sieci - jest to realizowane w ramach jednego intuicyjnego panelu sterowania. Klienci otrzymują rozbudowane i dostosowane do swoich potrzeb raporty oraz powiadomienia dotyczące uwierzytelniania, dostępu gości, wprowadzania nowych urządzeń, profili urządzeń, a także stanu zabezpieczeń systemów końcowych.

Dostępne rozwiązania

Rozwiązania sprzętowe

Fizyczne rozwiązania ExtremeControl to serwery rackowe z zainstalowanymi wszystkimi funkcjonalnościami. Zakupione aplikacje (licencjonowane oddzielnie) są aktywowane za pomocą kluczy licencyjnych:

- ExtremeControl Appliance IA-A-25 - zarządzanie maks. 12 tys. systemów końcowych
- ExtremeControl Appliance IA-A-305 - zarządzanie maks. 24 tys. systemów końcowych

Rozwiązania wirtualne

Wirtualne rozwiązania ExtremeControl muszą być zainstalowane na serwerze VMWare lub Hyper-V z formatem dysku VHDX:

- Wirtualne rozwiązanie VWWare Management Center jest zapisane w pliku o rozszerzeniu .OVA (zdefiniowanym przez VMWare)
- Wirtualne rozwiązanie Hyper-V Management Center jest zapisane w archiwum .ZIP

Specyfikacja rozwiązań sprzętowych

Wersja produktu	IA-A-25 (87100)	IA-A-305 (87101)
Specyfikacja sprzętowa		
Dysk	150GB Enterprise SSD	240GB Enterprise SSD
Interfejsy sieciowe	2 x 1GbE	2 x 1GbE
Porty obrazu	Przód VGA, tył VGA	Przód VGA, tył VGA
Interfejs szeregowy	RJ45	RJ45
Porty USB	2 z przodu, 3 z tyłu	2 z przodu, 3 z tyłu
TPM w wersji 2.0	Tak	Tak
Możliwości urządzenia		
Liczba obsługiwanych systemów końcowych	do 12,000	do 24,000
Specyfikacja zasilania		
Zasilanie	750W 80+ Platinum, możliwość wymiany podczas pracy	750W 80+ Platinum, możliwość wymiany podczas pracy
Rodzaj zasilacza	AC redundantny	AC redundantny
Napięcie wejściowe	90Hz do 132V i 180V do 264V	90Hz do 132V i 180V do 264V
Częstotliwość wejściowa	47Hz do 63Hz	47Hz do 63Hz
Dane fizyczne		
Montaż w racku	1U	1U
Wymiary	16.93" x 27.95" x 1.72"	16.93" x 27.95" x 1.72"
Waga	29 lb. (13.15 kg) maks.	29 lb. (13.15 kg) maks.
Dane środowiskowe		
Parametry operacyjne	• ASHRAE Class A2 - praca ciągła. 10°C do 35°C (50°F do 95°F) z maksymalnym przyrostem temperatury nie większym niż 10°C na godzinę • ASHRAE Class A3 - obejmuje pracę w temperaturze do 40°C przez maks. 900 godzin w roku. • ASHRAE Class A4 - obejmuje pracę w temperaturze do 45°C przez maks. 90 godzin w roku.	• ASHRAE Class A2 - praca ciągła. 10°C do 35°C (50°F do 95°F) z maksymalnym przyrostem temperatury nie większym niż 10°C na godzinę • ASHRAE Class A3 - obejmuje pracę w temperaturze do 40°C przez maks. 900 godzin w roku. • ASHRAE Class A4 - obejmuje pracę w temperaturze do 45°C przez maks. 90 godzin w roku.
Transport	-40°C do 70°C (-40°F do 158°F)	-40°C do 70°C (-40°F do 158°F)
Wilgotność (podczas transportu)	50% do 90%, bez kondensacji przy temperaturze mokrego termometru maks. 28° C (zakres temperatur od 25° C do 35°C)	50% do 90%, bez kondensacji przy temperaturze mokrego termometru maks. 28° C (zakres temperatur od 25° C do 35°C)
Wibracje (bez opakowania)	5 Hz do 500 Hz 2.20 g RMS losowe	5 Hz do 500 Hz 2.20 g RMS losowe
Gwarancja		
Sprzętowa	1 rok na części i pracę	1 rok na części i pracę

Ocenianie agentowe - wymagania dotyczące systemów operacyjnych

W poniższej tabeli wymieniono obsługiwane systemy operacyjne urządzeń końcowych podłączanych do sieci poprzez wdrożenie ExtremeControl wykorzystujące agentowe ocenianie.

Ponadto, urządzenie końcowe musi spełniać wymagania dotyczące dostępnej przestrzeni dyskowej oraz pamięci dla systemu operacyjnego określone przez Microsoft® i Apple®.

System operacyjny		Przestrzeń dyskowa na system operacyjny	Dostępna pamięć
Windows	• Windows® Windows Vista • Windows XP • Windows 2008 • Windows 2003 • Windows 7 • Windows 8 • Windows 8.1 • Windows 10	80 MB	40 MB (80 MB z Service Agent)
Mac OS	• Tiger • Snow Leopard • Lion • Mountain Lio • Mavericks • Yosemite • El Capitan • Sierra	10 MB	120 MB

Uwaga: Wybrane testy oceniające wymagają Windows Action Center (wcześniejsza nazwa Windows Security Center), które jest obsługiwane przez systemy operacyjne WindowsXP SP2+, Windows Vista, Windows 7, Windows 8 i Windows 8.1.

Wymagania dotyczące przeglądarek internetowych

W poniższej tabeli wymieniono obsługiwane przeglądarki internetowe urządzeń stacjonarnych i mobilnych łączących się z siecią poprzez Mobile Captive Portal rozwiązania ExtremeControl.

Przeglądarka		Wersja
Komputery stacjonarne	Microsoft Edge	41 lub nowsza
	Microsoft Internet Explorer	11 lub nowsza
	Mozilla Firefox	34 lub nowsza
	Google Chrome	33.0 lub nowsza
	Safari	Wszystkie wersje
Urządzenia mobilne	Internet Explorer Mobile	11 lub nowsza (Windows Phone)
	Microsoft Edge	Wszystkie wersje
	Microsoft Windows 10 Touch Screen Native (Surface Table)	N/A
	Safari	7 lub nowsza
	IOS Native	9 lub nowsza
	Android Chrome	4.0 lub nowsza
	Android Native	Wszystkie wersje
	Dolhin	Wszystkie wersje
	Opera	

Informacje dotyczące zamawiania

Aby uprościć proces składania zamówień dla klientów, którzy korzystają z oprogramowania do zarządzania siecią od innego dostawcy, proponujemy ceny za rozwiązanie ExtremeControl zależne od liczby użytkowników. Dostępna jest także subskrypcja zależna od liczby urządzeń.

Urządzenia fizyczne ExtremeControl

Nr katalogowy	Opis
87100	ExtremeControl Appliance -IA-A-25, obsługa maks. do 12 tys. systemów końcowych
87101	ExtremeControl Appliance -IA-A-305, obsługa maks. do 24 tys. systemów końcowych

Subskrypcja zależna od liczby użytkowników

ExtremeControl (97207-27001)

Obejmuje nieograniczoną liczbę licencji na systemy końcowe uzależnioną od ograniczeń wydajnościowych oraz usługi ExtremeWorks dla tych licencji, liczone dla każdego użytkownika na rok.

Licencje na systemy końcowe

Nr katalogowy	Opis
IA-ES-1K	Licencja Identity and Access na 1 tys. systemów końcowych, do stosowania z urządzeniami Identity and Access
IA-ES-3K	Licencja Identity and Access na 3 tys. systemów końcowych, do stosowania z urządzeniami Identity and Access
IA-ES-12K	Licencja Identity and Access na 12 tys. systemów końcowych, do stosowania z urządzeniami Identity and Access

Licencje na ocenę stanu zabezpieczeń systemów

Nr katalogowy	Opis
IA-PA-3K	Licencja Identity and Access Posture Assessment dla 3 tys. systemów końcowych (zawiera ocenianie typu agentowego i bezagentowego)
IA-PA-12K	Licencja Identity and Access Posture Assessment dla 12 tys. systemów końcowych (zawiera ocenianie typu agentowego i bezagentowego)

Gwarancja

Extreme Networks jako firma zorientowana na klienta i jego potrzeby, zobowiązuje się do dostarczania produktów i rozwiązań najwyższej jakości. W przypadku, gdy jeden z naszych produktów ulegnie awarii, świadczymy gwarancję, pozwalającą w prosty sposób naprawić lub wymienić uszkodzony produkt, najszybciej jak to możliwe.

Rozwiązanie sprzętowe objęte jest roczną gwarancją na wady produkcyjne. Gwarancja na oprogramowanie trwa 90 dni i obejmuje tylko wady dotyczące nośników danych. Pełne warunki i postanowienia gwarancji dostępne są na stronie:

http://learn.extremenetworks.com/rs/641-VMV-602/images/Extreme-Networks-Product-Warranty.pdf

Usługi i wsparcie techniczne

Firma Extreme Networks oferuje kompleksowy zestaw usług, rozciągający się od działu Professional Services zajmującego się projektowaniem, wdrażaniem i optymalizowaniem sieci klientów, przez dostosowane do klienta szkolenia techniczne, aż do działu usług i wsparcia technicznego koncentrującego się na indywidualnych potrzebach klientów. Prosimy o kontakt z lokalnym przedstawicielem Extreme Networks w celu uzyskania szczegółowych informacji na temat naszych usług i wsparcia.

Dodatkowe informacje

Dodatkowe informacje techniczne dostępne są na stronie:

http://www.extremenetworks.com/product/extreme-access-control

Informacje dodatkowe

Jeżeli chcą Państwo uzyskać więcej informacji zapraszamy do odwiedzenia naszej strony internetowej: www.extremenetworks.com lub skontaktowania się z naszym dystrybutorem: www.exclusive-networks.com/pl/

Extreme
Connect Beyond the Network

EXCLUSIVE NETWORKS

JMM, 01/2018