

Juniper Networks Security Threat Response Manager (STRM)

Opis produktu

Rodzina urządzeń STRM łączy, analizuje oraz zarządza różnorodnym zbiorem danych – zachowanie się sieci, zdarzenia bezpieczeństwa, profile podatności i informacje o zagrożeniach – co umożliwia firmom efektywnie zarządzać operacjami biznesowymi w sieci z poziomu pojedynczej konsoli. Z preinstalowanym oprogramowaniem, systemem operacyjnym o zwiększonym bezpieczeństwie oraz konfiguracją z poziomu Web, rodzina urządzeń STRM umożliwi szybką i prostą aktywację systemu bezpieczeństwa sieci. Linia produktów STRM firmy Juniper jest łatwa we wdrożeniu i szybka w implementacji, wydatnie zwiększa bezpieczeństwo przy niskich kosztach utrzymania.

STRM 500

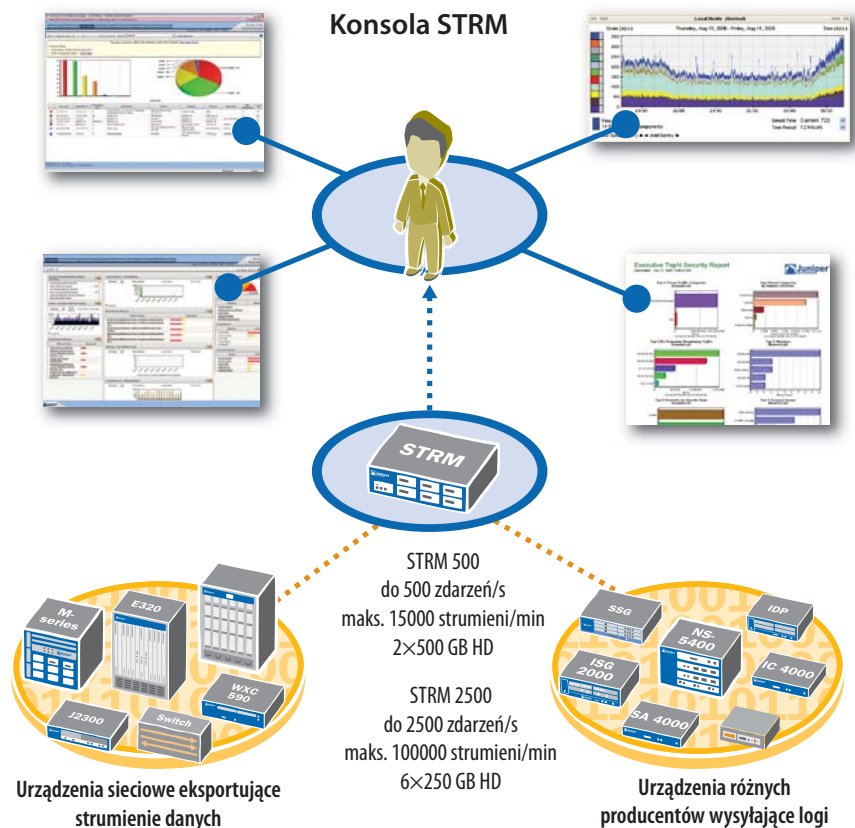
STRM 500 firmy Juniper łączy wszystkie zalety i funkcjonalność STRM w pojedynczym bezpiecznym rozwiązaniu sprzętowym. Stanowi rozwiązanie bezpieczeństwa typu „wszystko w jednym”, które włącza się bezpośrednio do sieci, co zapewnia szybkie i łatwe wdrożenie. Dzięki intuicyjnemu interfejsowi webowemu konfiguracja jest tak prosta, że można uruchomić STRM 500 i monitorować sieć w ciągu kilku minut. STRM 500 jest zoptymalizowaną platformą sprzętową, która nie wymaga drogich zewnętrznych pamięci masowych, baz danych firm trzecich czy ciągłej administracji baz danych. Te urządzenia są idealne dla małych, średnich i dużych przedsiębiorstw lub departamentów, które nie przewidują potrzeby zwiększenia wydajności lub zwiększenia się ilości pojawiających się zdarzeń lub strumienia danych. STRM 500 może być również wdrażany jako dedykowany kolektor Q-Flow w celu gromadzenia przesyłanych strumieni danych, aby zapewnić analizę na poziomie warstwy aplikacji.

Zintegrowana oferta STRM, łącząca w sobie gromadzenie danych, analizę, zdolność korelacji i audytu, pozwala organizacjom szybko i w prosty sposób zaimplementować program zarządzania bezpieczeństwem w całej korporacji oraz wdrożyć najlepsze praktyki z zakresu bezpieczeństwa, w tym:

Zarządzanie logami: STRM pozwala na skalowalne zarządzanie logami poprzez gromadzenie rozproszonych logów z całej organizacji i scentralizowany podgląd gromadzonych informacji.

Zarządzanie zagrożeniami: STRM jest zaawansowanym rozwiązaniem do zarządzania bezpieczeństwem sieci, które pozwala osiągnąć kompromis pomiędzy wymogami bezpieczeństwa a operacjami sieciowymi, zapewniając nadzór w czasie rzeczywistym oraz wykrywając złożone zagrożenia IT.

Zarządzanie zgodnością ze standardami: STRM zapewnia przedsiębiorstwom, instytucjom i agencjom rozliczalność, przejrzystość, wymierność, stanowiące kluczowe czynniki sukcesu każdego programu bezpieczeństwa IT spełniającego niezbędne regulacje prawne.



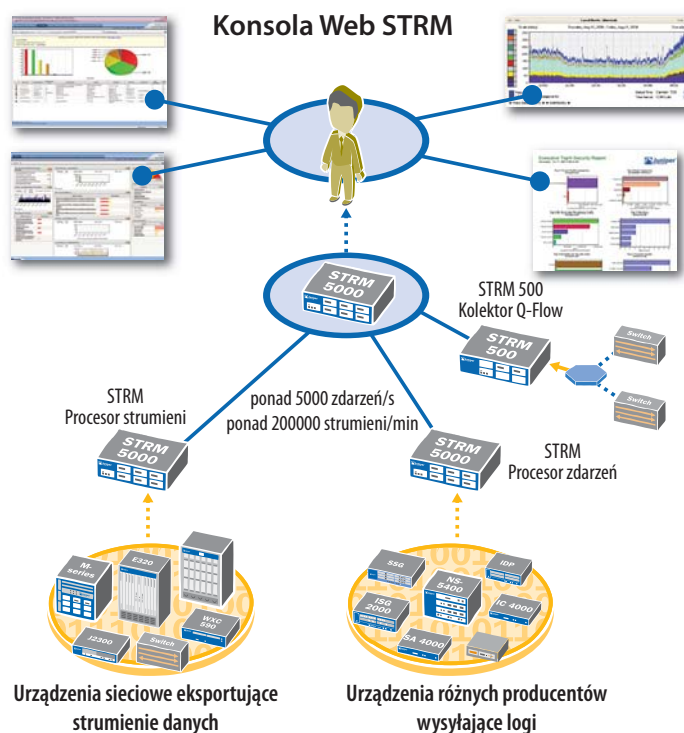
Rysunek 1: Typowe wdrożenie STRM 500 i STRM 2500

STRM 2500

STRM 2500 to skalowalne rozwiązanie klasy korporacyjnej do zarządzania bezpieczeństwem sieci od firm średnich rozmiarów do dużych, globalnych organizacji. Urządzenie STRM 2500 jest idealnym rozwiązaniem dla firm rozwijających się, które będą potrzebować w przyszłości dodatkowej wydajności i pojemności do monitorowania większej ilości zdarzeń i strumieni danych. Jest to również wyjściowa platforma dla dużych, geograficznie rozproszonych firm poszukujących skalowalnego rozwiązania klasy korporacyjnej. Urządzenie STRM 2500 zapewnia funkcje gromadzenia zdarzeń, korelacji oraz obszernego raportowania.

STRM 5000

STRM 5000 jest urządzeniem klasy korporacyjnej i operatorskiej, które zapewnia skalowalne zarządzanie bezpieczeństwem sieci od firm średnich rozmiarów do dużych, globalnych organizacji. Urządzenie STRM 5000 jest idealnym rozwiązaniem dla firm rozwijających się, które przewidują konieczność zwiększenia wydajności i pojemności w przyszłości. To także platforma wyjściowa dla dużych korporacji działających w wielu lokalizacjach fizycznych, poszukujących rozproszonych rozwiązań klasy korporacyjnej i operatorskiej. STRM 5000 korzysta z wbudowanych systemów korelacji i gromadzenia zdarzeń/strumieni, może być również rozszerzony o dodatkowe urządzenia STRM 5000 działające jako kolektory zdarzeń i strumieni danych.

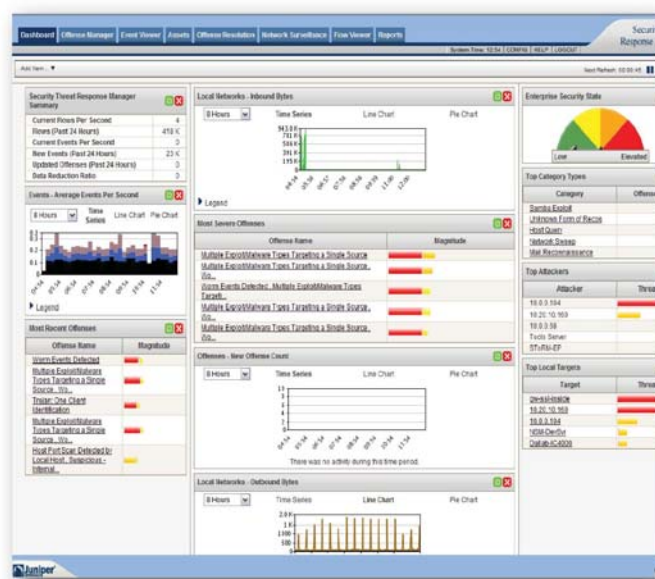
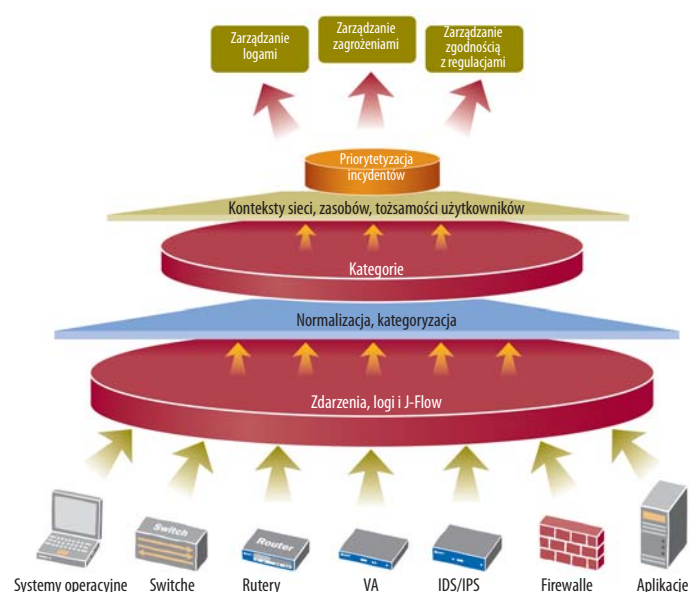


Rysunek 2: STRM 5000 zainstalowany w środowisku rozproszonym wraz z STRM 500 skonfigurowanym jako kolektor Q-Flow.

Właściwości i korzyści

Właściwości	Opis właściwości	Zalety
Wbudowany Q-Flow	Pozwala użytkownikom uzyskać wgląd w ruch warstwy aplikacji dzięki wbudowanym portom lub opcjonalnemu 4-portowemu modułowi rozszerzeń.	Zapewnia wgląd w bezpieczeństwo, aplikacje biznesowe oraz chronione zasoby.
Wsparcie architektury rozproszonej	Możliwość skalowania do dużych, rozproszonych wdrożeń od 500 do ponad 10 000 zdarzeń/s, od 15000 do 400000 strumieni/min.	Użytkownicy mogą elastycznie skalować wdrożenia wraz z rozwojem przedsiębiorstwa. STRM może być łatwo wdrożony w dużych, rozproszonych środowiskach.
System operacyjny wzmocniony pod kątem bezpieczeństwa (hardening)	Zespół ds. bezpieczeństwa Juniper monitoruje i utrzymuje system urządzeń STRM, zapewniając optymalną wydajność i bezpieczeństwo.	Użytkownicy nie muszą martwić się o zagrożenia bezpieczeństwa lub łatą dla systemu operacyjnego.
Implementacja (RAID)	Urządzenia STRM wykorzystują wbudowaną implementację systemu RAID (1-5).	Implementacja RAID zapewnia wysoką dostępność (HA) i nadmiarowość.
All – in – One	Gromadzenie zdarzeń, monitorowanie strumieni ruchu sieciowego, przetwarzanie zdarzeń oraz strumieni, korelacja, analiza i raportowanie – wszystko wbudowane w urządzenia STRM firmy Juniper.	Wszystkie istotne funkcje są dostępne w systemie dzięki czemu są łatwe do wdrożenia i zarządzania dla użytkownika. Architektura urządzeń STRM stanowi nowoczesne rozwiązanie do bezpiecznego i wydajnego zarządzania logami za pomocą standardowego interfejsu.
Łatwa i szybka instalacja	Konfiguracja „prosto z pudełka” z wykorzystaniem kreatora instalacji.	Użytkownicy mogą zainstalować i zarządzać STRM wykonując jedynie kilka prostych czynności.
Scentralizowane aktualizacje	Wszystkie aktualizacje pobierane są z jednego miejsca.	Użytkownik nie musi się martwić o utrzymanie urządzenia, aktualizacje i łatą dla systemu operacyjnego.
Ujednoczone wsparcie techniczne	Support techniczny Juniper (JTAC) zapewnia wsparcie wszystkich aspektów STRM, również w sieci, w której znajdują się urządzenia różnych producentów.	Użytkownicy nie muszą kontaktować się z różnymi działami supportu technicznego, aby uzyskać wsparcie nawet w sprawach związanych z rozwiązaniami wielu producentów.

Architektura i główne komponenty



Rysunek 3: Architektura i konsola monitorująca STRM

Zarządzanie logami i raportowanie

STRM stanowi wszechstronną platformę umożliwiającą skalowalne i bezpieczne zarządzanie logami, w skład której wchodzi skalowalne i bezpieczne funkcje zarządzania logami zintegrowane z korelacją zdarzeń w czasie rzeczywistym, monitorowaniem polityki, wykrywaniem zagrożeń oraz raportowaniem dotyczącym zgodności z regulacjami.

Właściwości	Opis właściwości	Zalety
Wszechstronne zarządzanie logami	Skalowalne i bezpieczne zarządzanie logami z możliwością przechowywania od GB do TB danych.	Zapewnia długoterminowe gromadzenie, archiwizację, przeszukiwanie i raportowanie logów zdarzeń, logów aktywności sieciowej i danych aplikacji, umożliwiając kategoryzację logów z poziomu centralnego zarządzania.
Obszerne raportowanie	STRM dostarcza ponad 220 predefiniowanych schematów raportów. Kreator raportów pozwala użytkownikom dostosowywać raporty do własnych potrzeb, ustawiać dzienny, tygodniowy i miesięczny harmonogram. Raporty mogą być eksportowane do plików w formacie pdf, html, rtf, word, excel i xml.	Zapewnia użytkownikom nie tylko wbudowane raporty, ale również elastyczność w tworzeniu własnych raportów dostosowanych do własnych potrzeb.
Wariant z ograniczeniem jedynie do zarządzania logami i raportowania	Kompleksowe rozwiązanie zarządzania logami i raportowania dla organizacji chcących zaimplementować wyłącznie rozproszone zarządzanie logami, aby gromadzić, archiwizować, analizować logi zdarzeń sieciowych i bezpieczeństwa.	Pozwala użytkownikom rozpocząć od opcji z ograniczeniem do zarządzania logami i raportowania, a następnie zaktualizować system do pełnej wersji STRM wraz ze wzrostem wymagań biznesowych, bez potrzeby ingerowania w istniejącą już platformę sprzętową.
Elastyczne API	Kompatybilność z szeroką gamą mniej popularnych interfejsów API oraz rozwiązania innych producentów.	Wspiera różnorodne urządzenia, aplikacje, jak również nowo pojawiające się technologie sieciowe i systemy bezpieczeństwa.
Składowanie i przechowywanie logów	Urządzenia STRM umożliwiają łatwą archiwizację logów i integrują się z istniejącą infrastrukturą baz danych w celu długoterminowego przechowywania danych.	Bazy danych STRM pozwalają organizacjom archiwizować logi zdarzeń i strumieni tak długo, jak wymagają tego odpowiednie regulacje prawne.
Bezpieczeństwo danych	Logi zdarzeń i strumieni danych chronione są za pomocą funkcji skrótu SHA-x (1-256). Wsparcie dla rozbudowanego sprawdzania integralności plików logów, w tym dla standardów zarządzania logami National Institute of Standards and Technology (NIST).	Zapewnia bezpieczne przechowywanie danych zgodnie z przyjętymi standardami.
Przeglądanie zdarzeń w czasie rzeczywistym	STRM pozwala użytkownikom monitorować i analizować zdarzenia w czasie rzeczywistym lub przeprowadzać zaawansowane badania. Przeglądarka zdarzeń pokazuje, które zdarzenia są skorelowane z zagrożeniem, a które nie.	Użytkownicy mają możliwość szybkiego i efektywnego przeglądania oraz filtrowania zdarzeń w czasie rzeczywistym. Dostępna jest funkcja elastycznego tworzenia zapytań z możliwością agregowania danych do późniejszej analizy przebiegu zdarzeń.
Magazynowanie danych	Dedykowane magazyny w celu szybkiego gromadzenia i odzyskiwania danych archiwalnych, w tym wszystkich logów bezpieczeństwa, logów zdarzeń oraz logów aktywności sieciowej (flow logs).	Pełny audyt wszystkich oryginalnych zdarzeń i zawartości strumieni danych bez żadnych modyfikacji.

Zarządzanie zagrożeniami

Rozwiązanie do zarządzania bezpieczeństwem sieci Juniper Networks STRM to innowacyjne podejście do zarządzania zagrożeniami sieciowymi w przedsiębiorstwie. Rozpoznawanie zdarzeń jest niewystarczające do właściwego wykrycia zagrożeń. STRM został opracowany, aby stworzyć zintegrowane podejście do zarządzania zagrożeniami, łącząc różne sposoby wykorzystania tradycyjnie gromadzonych informacji, aby skuteczniej wykrywać i zarządzać złożonymi zagrożeniami we współczesnych sieciach. Gromadzona informacja zawiera:

Zdarzenia sieciowe:

Zdarzenia generowane przez zasoby sieciowe, takie jak przełączniki, routery, serwery i stacje końcowe.

Logi bezpieczeństwa:

Zawiera logi generowane z sieciowych urządzeń bezpieczeństwa takich jak zapory ogniowe, koncentratory VPN, systemy wykrywania intruzów, antywirusy, systemy zarządzania tożsamością, skanery zagrożeń.

Logi aplikacji i hosta:

Zawiera logi z najpopularniejszych systemów operacyjnych (Microsoft Windows, UNIX i Linux) oraz z krytycznych aplikacji biznesowych (uwierzytelnianie, baza danych, poczta i Web).

Logi strumieni sieciowych i aplikacji:

Zawiera dane ze strumieni generowanych przez urządzenia sieciowe różnych producentów i udostępnia możliwość zakreślenia kontekstu aktywności sieci i protokołów.

Informacje o tożsamości użytkowników i zasobów:

Zawiera informacje z powszechnie używanych usług katalogowych w tym Active Directory i Lightweight Directory Access Protocol (LDAP). Przy użyciu technologii zarządzania incydentami bezpieczeństwa (offenses), zintegrowane informacje są normalizowane i korelowane przez STRM, co tworzy zautomatyzowaną inteligencję, która pozwala szybko wykrywać, powiadamiać i odpowiadać na zagrożenia pominięte przez inne systemy bezpieczeństwa.

Właściwości	Opis właściwości	Zalety
Reguły korelacji „prosto z pudełka”	Reguły korelacji STRM pozwalają użytkownikom na wykrywanie specyficznych lub powtarzających się zdarzeń lub ataków. Każda reguła składa się z testów i funkcji, które wymuszają podjęcie odpowiednich akcji w przypadku wystąpienia incydentu.	Zapewnia setki reguł korelacji „prosto z pudełka”, które umożliwiają natychmiastową ochronę. Użytkownicy mogą tworzyć własne reguły za pomocą kreatora reguł STRM, aby wygenerować zautomatyzowane alarmy dla grup odpowiedzialnych za przeciwdziałanie atakom i umożliwić egzekwowanie polityki bezpieczeństwa w czasie rzeczywistym.
Zarządzanie incydentami	Moduł zarządzania incydentami umożliwia śledzenie w sieci incydentów, zachowań, anomalii, celów ataków oraz atakujących. STRM może korelować zdarzenia i aktywność sieciową z celami rozlokowanymi w wielu sieciach w ramach tego samego naruszenia bezpieczeństwa, a co za tym idzie tego samego incydentu sieciowego.	Pozwala to użytkownikom na skuteczne zbadanie każdego incydentu w należącej do nich sieci. Użytkownicy mogą skorzystać ze wspólnego interfejsu, aby zbadać szczegóły incydentu w celu ustalenia poszczególnych zdarzeń, wchodzących w skład ataku.
Mapowanie QID	STRM dokonuje powiązania lub mapowania zdarzenia w postaci znormalizowanych albo oryginalnych danych, do kategorii niskiej lub wysokiej ważności.	Pozwala użytkownikowi obserwować zdarzenia zachodzące w czasie rzeczywistym, zamapowane do odpowiednich kategorii, co umożliwia STRM przypisanie nieznanym zdarzeń urządzeń do zdarzeń znanych STRM, w celu skategoryzowania ich odpowiedniej korelacji.
Profile historii zdarzeń	Profile historii zdarzeń wykorzystane są w celu zwiększenia dokładności rezultatów. STRM gromadzi i przechowuje wszystkie dane dotyczące wydarzenia, które mogą być wykorzystane w przyszłości.	Umożliwia użytkownikowi wgląd w dane historyczne w dowolnym momencie, jak również wgląd w zarządzanie incydentami oraz śledzenie zdarzeń.
Moduł oceniający STRM	Moduł oceniający STRM nadaje priorytet atakom i przypisuje im odpowiednie znaczenie na podstawie kilku czynników, takich jak liczba zdarzeń, ich siła, ważność i wiarygodność.	Umożliwia użytkownikom obserwowanie zdarzeń bezpieczeństwa z wysokim priorytetem zamiast przeszukiwać tysiące logów. Pozwala użytkownikom monitorować zdarzenia mające największy wpływ na funkcjonowanie ich przedsiębiorstwa i w krótkim czasie przeciwdziałać zagrożeniom.

Zarządzanie zgodnością ze standardami

Organizacje o różnej wielkości działające na rynkach niemalże każdego typu zmuszone są sprostać ustawicznie zwiększającej się liczbie wymogów prawnych dotyczących bezpieczeństwa IT.

Dostrzegając fakt, że wymogi zgodności ze standardami lub regulacjami prawnymi będą z czasem ewoluować, niezależni eksperci rekomendują opracowanie i stosowanie procesu zarządzającego standardami, który będzie uwzględniał poniższe czynniki:

Rozliczalność: zapewnienie nadzoru umożliwiającego raportowanie tego, kto i kiedy go wykazał.

Transparentność: Zapewnia wgląd w zastosowane środki bezpieczeństwa aplikacji przedsiębiorstwa i zasobów, które są chronione.

Wymierność: Mierniki i raporty oceniające ryzyko biznesowe dla systemów IT przedsiębiorstwa.



- Nieudane próby uwierzytelnienia na serwerach
- Udane zalogowania na serwery i wylogowania z serwerów
- Nieudane próby uwierzytelnienia do aplikacji
- Udane zalogowania do aplikacji i wylogowania z aplikacji
- Zmiany konfiguracji
- Wykorzystanie protokołów przez użytkowników
- Podatności
- Ataki
- Aktywność administratorów
- Aktywność w strefie DMZ
- Protokoły zaufane
- Protokoły ryzykowne

Rysunek 4: Przykładowe raporty STRM oceniające zgodność ze standardami

Właściwości	Opis właściwości	Zalety
Wbudowane raporty zgodności	Wbudowane raporty zgodności dołączone są do STRM.	Dostępność setek raportów zgodności „prosto z pudełka”.
Możliwości raportowania i alarmowania w module kontrolującym	CobiT, ISO/IEC 27002 (17799) Common Criteria (CC) (ISO/IEC 15408) specjalna publikacja NIST 800-53 korekta 1 oraz FIPS 200.	Zapewnia powtarzalny monitoring zgodności ze standardami, raportowanie i procesy audytowania.
Przetwarzanie informacji zgodnie ze standardami	Payment Card Industry Data Security Standard (PCI DSS) Health Insurance Portability and Accountability Act (HIPAA) Sarbanes-Oxley Act (SOX) Graham-Leach-Bliley Act (GLBA) Federal Information Security Management Act (FISMA).	Zgodność z wieloma regulacjami i działanie zgodnie z najlepszymi praktykami bezpieczeństwa. Szablony raportowania uwzględniające zgodność ze standardami pozwalają spełnić wymogi dotyczące raportowania i audytowania wynikające z przepisów.
Raporty o ogólnym stanie bezpieczeństwa dla kadry zarządzającej	Interfejs raportowania STRM pozwala na tworzenie, dystrybuowanie i zarządzanie raportami. Raporty te mogą być generowane w formatach pdf, html, rtf, xml oraz xls	Użytkownicy mogą korzystać z kreatora raportów, tworząc raporty dla kadry zarządzającej, które uwzględniają zdarzenia ruchu sieciowego i incydenty bezpieczeństwa.

Specyfikacja

	STRM 500	STRM 2500	STRM 5000
Wymiary i zasilanie			
Wymiary (szerokość × wysokość × głębokość)	17.72 × 17.26 × 3.5 in (45 × 43.84 × 8.8 cm)	23.52 × 17.26 × 3.5 in (59.75 × 43.84 × 8.8 cm)	23.52 × 17.26 × 3.5 in (59.75 × 43.84 × 8.8 cm)
Waga	11.8 kg	17.8 kg	19.8 kg
Montowanie w szafie rack	Tak, 2U	Tak, 2U	Tak, 2U
Zasilanie A/C	zasilacz redundantny, podwójny, wymienny na gorąco, 90 V do 264 V, 400 W AC	zasilacz redundantny, podwójny, wymienny na gorąco, 90 V do 264 V, 700 W AC	zasilacz redundantny, podwójny, wymienny na gorąco, 90 V do 264 V, 700 W AC
Zasilanie D/C	zasilacz redundantny, podwójny, wymienny na gorąco, 90 V do 264 V, 710 W DC, z opcjonalnym zasilaczem 48V DC	zasilacz redundantny, podwójny, wymienny na gorąco, 90 V do 264 V, 710 W DC, z opcjonalnym zasilaczem 48V DC	zasilacz redundantny, podwójny, wymienny na gorąco, 90 V do 264 V, 710 W DC, z opcjonalnym zasilaczem 48V DC
Równoległa praca zasilaczy AC i DC	Tak	Tak	Tak
Materiał	blacha stalowa walcowana na zimno o grubości 1.2 mm	blacha stalowa walcowana na zimno o grubości 1.2 mm	blacha stalowa walcowana na zimno o grubości 1.2 mm
Wentylatory	Wentylator redundantny, wymienny na gorąco 2 × 80 mm (drugi opcjonalnie)	Wentylator redundantny, wymienny na gorąco 3 × 80 mm (drugi opcjonalnie)	Wentylator redundantny, wymienny na gorąco 3 × 80 mm (drugi opcjonalnie)
Porty sieciowe	2x RJ45 10/100/1000	2x RJ45 10/100/1000	2x RJ45 10/100/1000
Port konsoli	1x RJ45 port szeregowy	1x RJ45 port szeregowy	1x RJ45 port szeregowy
Parametry środowiskowe			
Temperatura pracy	41° – 104° F (5° – 40° C)	41° – 104° F (5° – 40° C)	41° – 104° F (5° – 40° C)
Temperatura przechowywania	-40° – 158° F (-40° – 70° C)	-40° – 158° F (-40° – 70° C)	-40° – 158° F (-40° – 70° C)
Wilgotność względna (praca)	8% do 90% bez kondensacji	8% do 90% bez kondensacji	8% do 90% bez kondensacji
Wilgotność względna (przechowywanie)	5% do 95% bez kondensacji	5% do 95% bez kondensacji	5% do 95% bez kondensacji
Wysokość (praca)	do 3048 m	do 3048 m	do 3048 m
Wysokość (przechowywanie)	do 12192 m	do 12192 m	do 12192 m

	STRM 500	STRM 2500	STRM 5000
Certyfikaty bezpieczeństwa i zgodności			
Certyfikaty bezpieczeństwa	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001+A11 IEC 60950-1:2001	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001+A11 IEC 60950-1:2001	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001+A11 IEC 60950-1:2001
Certyfikaty emisji	FCC Klasa A, EN 55022 klasa A, EN 55024 Odporność, EN 61000-3-2, VCCI Klasa A	FCC Klasa A, EN 55022 klasa A, EN 55024 Odporność, EN 61000-3-2, VCCI Klasa A	FCC Klasa A, EN 55022 klasa A, EN 55024 Odporność, EN 61000-3-2, VCCI Klasa A
Gwarancja	Sprzęt 1 rok, oprogramowanie 90 dni	Sprzęt 1 rok, oprogramowanie 90 dni	Sprzęt 1 rok, oprogramowanie 90 dni

Specyfikacja sprzętowa

HDD	2 x 500 GB RAID 1	6 x 250 GB RAID 5	6 x 250 GB RAID 5
Pamięć	8 GB	8 GB	8 GB
Ilość zdarzeń na sekundę (EPS)	Do 500	Do 2500	Do 2500
Strumienie na minutę	Maks. 15000	Maks. 100000	Maks. 100000

Informacje do zamówień

STRM 500	Opis
STRM500-A-BSE	Platforma sprzętowa STRM 500
STRM500-ADD-250EPS-15KF	Licencja na 250 EPS i 15000 strumieni
STRM500-UPG-500EPS-15KF	Licencja na modernizację do 500 EPS z 15000 strumieni

Opcja tylko do zarządzania logami

STRM500-LM-ADD-500EPS	Licencja na zarządzanie logami do 500 EPS
-----------------------	---

Rozbudowa opcji zarządzania logami do pełnego STRM

STRM500-LM-500EPS-TO-TM	Licencja na rozbudowę do pełnego STRM na 500 EPS i 15000 strumieni
-------------------------	--

Kolektor QFlow

UNIV-1GE-4ETH	Karta 4-portowa 10/100/1000 Mb Ethernet
STRM500-QFC-ADD-50MB	Kolektor Q-Flow STRM o łącznej prędkości do 50 MB
STRM500-QFC-UPG-200MB	Rozbudowa kolektora Q-Flow STRM do łącznej prędkości do 200 Mb

STRM 2500	Opis
STRM2500-A-BSE	Platforma sprzętowa STRM 2500
STRM2500-ADD-1KEPS-50KF	Licencja na 1000 EPS i 50000 strumieni
STRM2500-UPG-2500EPS-50KF	Licencja na rozbudowę do 2500 EPS i 50000 strumieni
STRM2500-UP-2500EPS-100KF	Licencja na rozbudowę do 2500 EPS i 100000 strumieni
STRM2500-UPG-1KEPS-100KF	Licencja na rozbudowę do 1000 EPS i 100000 strumieni

Opcja tylko do zarządzania logami

STRM2500-LM-ADD-1KEPS	Licencja na zarządzanie logami do 1000 EPS
STRM2500-LM-UPG-2500EPS	Licencja na zarządzanie logami i rozbudowę do 2500 EPS

STRM 2500	Opis
Rozbudowa opcji zarządzania logami do pełnego STRM	
STRM2500-LM-1KEPS-TO-TM	Licencja na rozbudowę do pełnego STRM na 1000 EPS i 50000 strumieni
STRM2500-LM-2500E-TO-TM	Licencja na rozbudowę do pełnego STRM na 2500 EPS i 50000 strumieni

STRM 5000	Opis
STRM5000-A-BSE	Platforma sprzętowa STRM 5000
STRM5K-ADD-5KE-200KF	Licencja na 5000 EPS i 200000 strumieni

Procesor Zdarzeń (architektura rozproszona)

STRM5K-ADD-EP-5KEPS	Licencja na STRM 5000 jako Procesor Zdarzeń do 5000 EPS
STRM5K-UPG-EP-10KEPS	Licencja na rozbudowę Procesora Zdarzeń do 10000 EPS

Procesor Strumieni (architektura rozproszona)

STRM5K-ADD-FP-200KF	Licencja na STRM 5000 jako Procesor Strumieni do 200000 strumieni/min
STRM5K-UPG-FP-400KF	Licencja na rozbudowę Procesora Przepływu do 400000 strumieni/min

Konsola STRM (architektura rozproszona)

STRM5K-ADD-CON	Licencja na STRM 5000 jako konsolę zarządzającą
----------------	---

Opcja tylko do zarządzania logami

STRM5K-LM-ADD-5KEPS	Licencja na zarządzanie logami do 5000 EPS
---------------------	--

Opcja tylko do zarządzania logami (architektura rozproszona)

STRM5K-LM-ADD-EP-5KE	Licencja na zarządzanie logami jako Procesor Zdarzeń do 5000 EPS
STRM5K-LM-UP-EP-10KE	Licencja na rozbudowę zarządzania logami przez Procesor Zdarzeń do 10000 EPS
STRM5K-LM-ADD-CON	Licencja na STRM 5000 jako konsolę zarządzania w opcji tylko do zarządzania logami

STRM 5000	Opis
Rozbudowa opcji zarządzania logami do pełnego STRM	
STRM5K-LM-5KE-TO-TM	Licencja na rozbudowę do pełnego STRM na 5000 EPS i 100000 strumieni
STRM5K-LM-EP-5KE-TO-TM	Licencja na rozbudowę Procesora Zdarzeń w opcji tylko do zarządzania logami do pełnego Procesora Zdarzeń na 5000 EPS
STRM5K-LM-CON-TO-TM	Licencja na rozbudowę konsoli zarządzającej w opcji tylko do zarządzania logami do pełnej konsoli zarządzającej STRM
Elementy uniwersalne	Opis
UNIV-500G-HDD	Dysk twardy do STRM 500 i STRM 5000
UNIV-250G -HDD	Dysk twardy do STRM 2500
UNIV-MR2U-FAN	Wentylator do STRM 500
UNIV-HE2U-FAN	Wentylator do STRM 2500 i STRM 5000
UNIV-PS-400W-AC	Zasilacz AC do STRM 500
UNIV-PS-700W-AC	Zasilacz AC do STRM 2500 i STRM 5000
UNIV-PS-710W-DC	Zasilacz DC do STRM 500, STRM 2500 i STRM 5000
UNIV-MR2U-RAILKIT	Zestaw montażowy do STRM 500
UNIV-HE2U-RAILKIT	Zestaw montażowy do STRM 2500 i STRM 5000

Wspierane urządzenia Juniper

- Juniper Networks NetScreen Firewall (ISG, SSG, NetScreen)
- Juniper Networks Intrusion Detection and Prevention (IDP)
- Juniper Networks NetScreen-Security Manager (NSM)
- Juniper Networks Routing Platform (J-series)
- Juniper Networks Infranet Controller (IC)
- Juniper Networks Secure Access SSL VPN (SA)

W celu uzyskania aktualnej listy wspieranych urządzeń i aplikacji należy się skontaktować ze swoim przedstawicielem Juniper Networks.

Informacje o Juniper Networks

Juniper Networks Inc. jest liderem wysokowydajnych rozwiązań sieciowych. Juniper oferuje wysokowydajną infrastrukturę sieciową, tworzącą elastyczne i zaufane środowisko przyspieszające wdrażanie serwisów i aplikacji wewnątrz pojedynczej sieci. Wszystko to napędza biznes o dużym potencjale rozwoju. Więcej informacji można znaleźć na www.juniper.net

Dystrybucja w Polsce:



CLICO Sp. z o.o.
Budynek CC Oleandry
30-063 Kraków, ul. Oleandry 2
tel. 012 378-37-00
tel. 012 632-51-66
tel. 012 292-75-22 ... 24
fax 012 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-568 Katowice, ul. Ligocka 103
tel. 032 444-65-11
tel. 032 203-92-35
tel. 032 609-80-50...51
fax 032 203-97-93
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
Budynek Centrum Milenium
03-738 Warszawa, ul. Kijowska 1
tel. 022 201-06-88
tel. 022 518-02-70...75
fax 022 518-02-73
e-mail: warszawa@clico.pl