connect DISTRIBUTION

Proste w obsłudze, potężne i przystępne cenowo oprogramowanie do monitorowania systemów IT, uwielbiane przez profesjonalistów

solarwinds

PRZEGLĄD PRODUKTÓW

O SOLARWINDS

Firma SolarWinds oferuje klientom na całym świecie zaawansowane, niedrogie oprogramowanie do zarządzania IT. Koncentrując się wyłącznie na specjalistach z branży IT, dążymy do eliminowania skomplikowanych rozwiązań w oprogramowaniu do zarządzania IT, których stosowanie wymuszają dostawcy tradycyjnego oprogramowania dla przedsiębiorstw. Firma SolarWinds realizuje tę obietnicę z niespodziewaną prostotą dzięki produktom, które łatwo jest znaleźć i kupić, które są proste w użytkowaniu i konserwacji oraz umożliwiają rozwiązywanie wszystkich problemów z zarządzaniem IT niezależnie od skali. Rozwiązania są inspirowane bliskim kontaktem z bazą użytkowników skupionych w naszej społeczności internetowej, thwack®. Społeczność ta rozwiązuje problemy, wymienia się technologią i najlepszymi praktykami oraz bezpośrednio uczestniczy w procesie projektowania naszych produktów.

Wypróbuj zanim kupisz - pobierz bezpłatną wersję próbną!

Czy chcesz dowiedzieć się, jak narzędzia SolarWinds mogą ułatwić zarządzanie i monitorowanie IT? Nie musisz wierzyć nam na słowo. W SolarWinds uważamy, że przed zakupem oprogramowanie należy wypróbować. Dlatego właśnie oferujemy bezpłatne wersje próbne, zapewniające pełną funkcjonalność. Po prostu pobierz, zainstaluj oprogramowanie SolarWinds i ciesz się nim przez 30 dni.

To takie proste!

Więcej informacji na stronie www.solarwinds.com

SolarWinds Software Europe Limited
Europe, Middle East and Africa Headquarters
Unit 1101, Building 1000, City Gate, Mahon, Cork, Ireland
+353 21 5002900

O CONNECT DISTRIBUTION

Założona w 1998 roku firma CONNECT DISTRIBUTION Sp. z o.o. jest wyspecjalizowanym dystrybutorem rozwiązań IT z wartością dodaną. Jesteśmy w 100% firmą z polskim kapitałem. Dostarczamy najwyższej światowej jakości rozwiązania software'owe oraz sprzętowe uzupełnione wsparciem konsultacyjnym i technicznym, zarówno na rynek krajowy jak i Europy Wschodniej. Specjalizujemy się w najnowszych, zaawansowanych rozwiązaniach technologicznych o sprawdzonej niezawodności i wysokiej jakości. Wysoki poziom świadczonych przez nas oraz naszych partnerów usług został wielokrotnie doceniony przez organizacje branżowe i media.

Szerokie portfolio produktów, bogate doświadczenie w zakresie zaawansowanych technologii informatycznych oraz orientacja na partnerstwo pozwalają nam szybko reagować na potrzeby dynamicznie zmieniającego się otoczenia rynkowego. Misją firmy CONNECT DISTRIBUTION jest ciągłe dążenie do zaspokajania potrzeb naszych klientów poprzez dostarczanie im wyspecjalizowanych rozwiązań IT.

Firma CONNECT DISTRIBUTION jest dystrybutorem rozwiązań firmy SolarWinds na polskim rynku od 2013 roku.

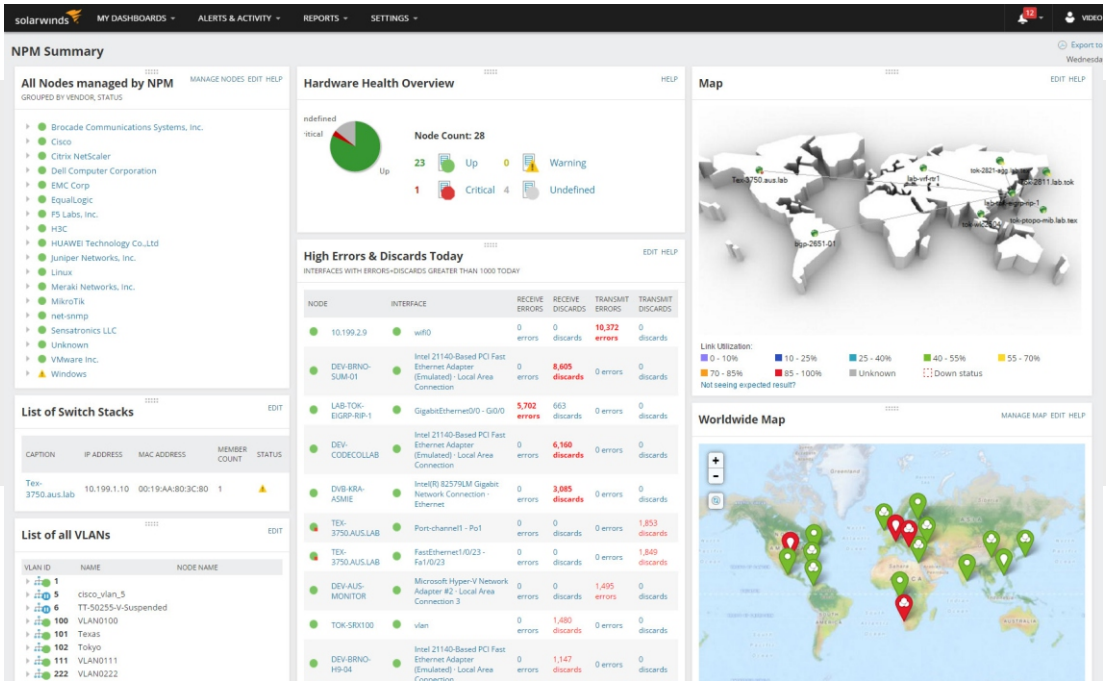
Więcej informacji na stronie www.connectdistribution.pl

CONNECT DISTRIBUTION Sp. z o.o.
ul. Woronicza 31/250, 02-640 Warszawa
+48 22 400 1234 / sales@connectdistribution.pl

connect DISTRIBUTION Autoryzowany Dystrybutor w Polsce

SPIS TREŚCI

Network Performance Monitor



SolarWinds® Network Performance Monitor (NPM) to zaawansowane i niedrogie oprogramowanie do monitorowania sieci, które umożliwia szybkie wykrywanie, diagnozowanie i rozwiązywanie problemów z wydajnością sieci oraz eliminowanie przerw w jej działaniu.

NETWORK PERFORMANCE MONITOR W SKRÓCIE

- Szybsze rozwiązywanie problemów, wyższe poziomy usług i krótszy czas przestojów
- Badanie logicznej kondycji sieci - nie tylko fizycznej - ze wsparciem Cisco ACI
- Uproszczone zarządzanie złożonymi urządzeniami sieciowymi, monitorujące informacje o unikalnej roli każdego urządzenia w sieci, dzięki funkcjom Network Insight™
- Krytyczne analizy hop-by-hop dla usług lokalnych, hybrydowych lub chmurowych
- Korelacja danych sieci cross-stack w celu przyspieszenia identyfikacji problemu
- Zwiększenie wydajności operacyjnej, dzięki gotowym do wykorzystania panelom, alertom i raportom

FUNKCJE

Monitorowanie błędów, wydajności i dostępności

Szybkie wykrywanie, diagnozowanie i rozwiązywanie problemów z wydajnością sieci oraz likwidacja przestojów, dzięki oprogramowaniu do optymalizacji sieci.

Krytyczne analizy hop-by-hop

Wgląd w wydajność, ruch i szczegóły konfiguracji urządzeń oraz aplikacji, w środowisku lokalnym, hybrydowym i chmurowym.

Korelacja danych sieci cross-stack

Przyspieszenie identyfikacji źródła problemu, przeciągając i upuszczając metryki wydajności sieci na wspólnej osi czasu, aby uzyskać natychmiastową korelację wizualną ze wszystkich danych sieciowych.

Konfigurowalne inteligentne alerty topologii i zależności

Odpowiadanie na wielokrotne kontrole warunków, skorelowane zdarzenia, topologię sieci i zależności urządzeń.

Dynamiczne wykrywanie i mapowanie sieci

Automatyczne wykrywanie i mapowanie urządzeń, metryki wydajności, wykorzystanie łącza i zasięgu sieci bezprzewodowej.

Automatyczne prognozowanie, alarmowanie i raportowanie pojemności

Automatyczne obliczanie daty eksploatacji zasobów, przy użyciu dostosowywanych progów opartych na szczytowym i średnim użyciu.

Logiczne i fizyczne monitorowanie sieci w jednym narzędziu

Monitoring składników logicznych środowiska SDN, w tym APIC, dzierżawców, profile aplikacji, grupy punktów końcowych i jednostki fizyczne z pomocą wsparcia Cisco ACI.

Inteligentne mapy

Intuicyjna kondensacja i wizualizacja danych pomaga szybciej wykryć przyczynę problemu, nawet w złożonym środowisku.

Kompleksowe monitorowanie zaawansowanych urządzeń sieciowych

Wizualizacja i wgląd w stan oraz wydajność load balancer'ów F5® BIG-IP®, zapór Cisco ASA i Palo Alto Networks® oraz przełączników Cisco Nexus z funkcjami Network InsightTM.

Dynamiczne dane statystyczne dotyczące wydajności sieci

Dynamiczne kalkulacje progów na podstawie historycznych danych dotyczących wydajności sieci.

Monitorowanie stanu sprzętu

Monitorowanie, ostrzeganie i raportowanie kluczowych parametrów urządzeń, w tym temperatury, prędkości wentylatorów i zasilania.

MINIMALNE WYMAGANIA SYSTEMOWE

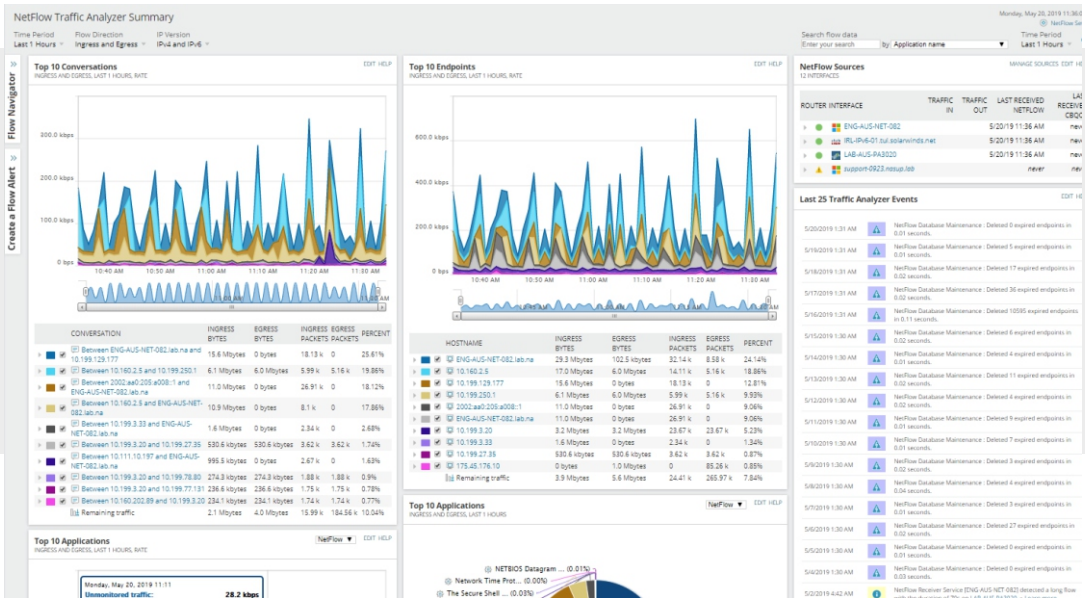
UWAGA: Powyższe wymagania systemowe określają minimalne wymagania dla Network Performance Monitor. Wymagania mogą się różnić w zależności od poziomu licencji.

SPRZĘT	MINIMALNE WYMAGANIA
CPU	Procesor czterordzeniowy lub lepszy
Pamięć	6GB
Dysk twardy	Minimum 10GB
OPROGRAMOWANIE	**MINIMALNE WYMAGANIA**
OS	Windows Server 2016 lub późniejsze
Baza danych	**On-premises** SolarWinds wspiera wersje Express, Standard oraz Enterprise w wersjach: • SQL Server® 2014, 2014 SP1, 2014 SP2 • SQL Server 2016, 2016 SP1 • SQL Server 2017 (w tym instalacje w systemie Linux®) • SQL Server 2019 **Cloud** • Amazon® RDS • Azure® SQL database

solarwinds

NetFlow Traffic Analyzer

Wykorzystanie sieci w czasie rzeczywistym i monitorowanie przepustowości



SolarWinds® NetFlow Traffic Analyzer (NTA) pozwala na przechwytywanie danych ze strumieni ruchu sieciowego i konwertowanie tych surowych liczb na łatwe do zinterpretowania wykresy i tabele, które określają ilość ruchu w sieci korporacyjnej.

NETFLOW TRAFFIC ANALYZER W SKRÓCIE

- NTA gromadzi i analizuje dane od różnych producentów, w tym NetFlow v5 i v9, Juniper® J-Flow™, sFlow®, Huawei® NetStream™ oraz IPFIX
- NTA obsługuje zaawansowane rozpoznawanie aplikacji za pomocą Cisco® NBAR2
- NTA ostrzega o zmianach w ruchu aplikacji lub jeśli urządzenie przestaje wysyłać dane ruchu
- NTA pozwala na optymalizację zasad CBQos
- NTA pomaga zidentyfikować złośliwy lub zniekształcony ruch z monitorowaniem portu 0
- NTA obejmuje analizę ruchu sieciowego WLC, dzięki czemu można zobaczyć, co wykorzystuje przepustowość bezprzewodową
- NTA uzupełnia Network Performance Monitor, pomagając zidentyfikować przyczynę dużej utylizacji łącza. Zbudowany na platformie Orion®, NTA zapewnia możliwość zakupu i pełnej integracji z dodatkowymi modułami monitorowania sieci (zarządzanie konfiguracją, zarządzanie siecią WAN, VoIP, śledzenie urządzeń, zarządzanie adresami IP), a także zarządzanie systemami, pamięcią masową i wirtualizacją w pojedynczej konsoli internetowej.

FUNKCJE

Network Insight™ dla Palo Alto Networks®

Network Insight™ dla Palo Alto Networks® obejmuje zbiór przepływów z zapór Palo Alto, aby pokazać przepływ przez węzły i interfejsy.

Azure SQL Database Deployment

Elastyczne opcje wdrażania z bazą danych SQL Azure - przejmij kontrolę nad wdrożeniem NTA z elastycznością, aby wdrożyć NTA lokalnie lub w chmurze z Azure SQL Database czy Amazon RDS.

Dane o ruchu lokalnym

Wgląd w ruch pochodzący z serwera przepływu danych, dodając nowe źródło danych o ruchu i umożliwiając użytkownikom natychmiastowe scharakteryzowanie lokalnego ruchu.

Monitorowanie wykorzystania przepustowości

Dostarcza natychmiastowe powiadomienie alarmowe, w tym listę najbardziej absorbujących elementów, gdy interfejs przekracza próg wykorzystania przepustowości.

Wykorzystanie przepustowości przez aplikację

Dostarcza cennych informacji o tym, które aplikacje wykorzystują największą przepustowość sieci i śledzi ruch aplikacji docierający z wyznaczonych portów, źródłowych adresów IP, docelowych adresów IP, a nawet protokołów.

Wykorzystanie przepustowości przez grupy IP

Analizuje ruch sieciowy za pomocą niestandardowych nakładających się grup adresów IP. Tworzy własne grupy adresów IP, aby wyświetlać ruch w sieci w taki sposób, w jaki chcesz go zobaczyć.

Monitorowanie ruchu sieciowego

Zapewnia kompleksowy, konfigurowalny widok ruchu sieciowego w jednym panelu, pomagając szybko dostrzec potencjalne problemy, dzięki dziesięciu najlepszym widokom danych o ruchu sieciowym. Znajduje źródło problemów z przepustowością, dzięki intuicyjnemu interfejsowi "point-and-click".

Cross-stack Network Data Correlation

Przyspiesza identyfikację przyczyny problemu źródłowego, przeciągając i upuszczając metryki wydajności sieci na wspólnej linii czasu, aby uzyskać natychmiastową korelację wizualną ze wszystkich danych sieciowych.

Network Traffic Forensics

Umożliwia przechodzenie do ruchu sieciowego dowolnego elementu przy użyciu wielu widoków, aby uzyskać potrzebne dane. Możesz badać i izolować nadmierne wykorzystanie przepustowości w sieci i nieoczekiwany ruch aplikacji.

Widoki wydajności CBQoS

Umożliwia przeglądanie ruchu sieciowego w podziale na klasy usług, pomiar efektywności polityki CBQoS oraz ilościowe określenie zużycia pasma według mapy klas.

Monitorowanie Portu 0

Monitorowanie ruchu TCP/UDP portu 0 wyświetla wszelkie przepływy kierowane do portu 0, aby można było zidentyfikować niechciany ruch.

Autonomiczny system analizowania ruchu sieciowego

Autonomiczny system monitorowania ruchu pozwala zobaczyć ruch kierowany przez połączenia ISP.

Alerty przekroczenia progu przepustowości

Generowanie powiadomień, aby móc szybko działać, jeśli ruch aplikacji nagle się zwiększy, zmniejszy lub całkowicie zniknie. Tworzenie alertów, aby otrzymywać powiadomienia, gdy urządzenie przestanie wysyłać dane o przepływie.

Raporty przepustowości

Umożliwia tworzenie szczegółowych raportów o ruchu sieciowym za pomocą kilku kliknięć lub zaplanowanie automatycznego dostarczania cotygodniowego raportu dla zespołu.

Optymalizacja Top-Talker

Określa, które przepływy zajmują większość wykorzystywanej przepustowości. Przechowuje te przepływy, pomijając dane przepływu od użytkowników i aplikacji, które mają znikomy wpływ na ogólną przepustowość. Zwiększa ogólną wydajność SolarWinds NTA do 10x przy przechwytywaniu przepływów, które stanowią 95% całkowitego ruchu sieciowego.

Zintegrowane zarządzanie błędami, wydajnością i konfiguracją

Integruje się z SolarWinds Network Performance Monitor (NPM), SolarWinds Network Configuration Manager (NCM) i SolarWinds User Device Tracker (UDT). Ta integracja zapewnia ujednolicone rozwiązanie dla błędów, wydajności, zarządzania konfiguracją automatycznego śledzenia urządzeń i zarządzania portami przełączania.

Integracja z Microsoft® Active Directory®

Wykorzystuje istniejące konta użytkowników usługi Active Directory w celu uproszczenia logowania i zarządzania kontami.

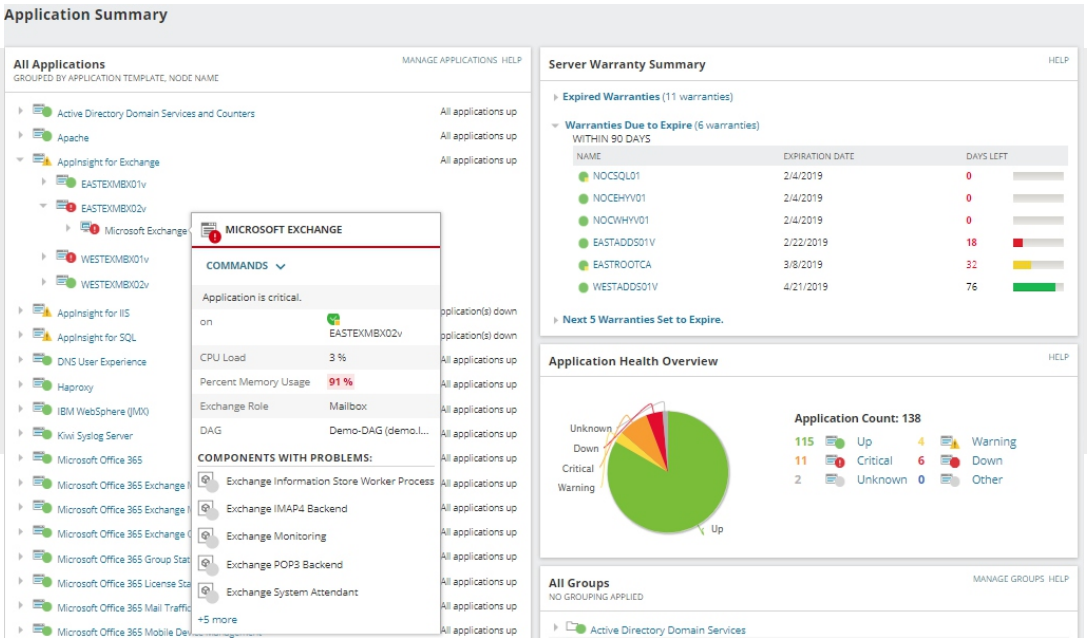
MINIMALNE WYMAGANIA SYSTEMOWE

UWAGA: Aby wdrożyć NTA, NPM musi być zainstalowany na tym samym serwerze. Te wymagania systemowe definiują minimalne wymagania dla NTA zainstalowanego na podstawowym Pollerze NPM. Wymagania mogą się różnić w zależności od poziomu licencji. Na support.solarwinds.com uzyskasz bardziej szczegółowe wymagania systemowe. Te minimalne wymagania serwera zakładają domyślną konfigurację. Znaczne zwiększenie częstotliwości odpytywania lub szybkości zbierania przepływu może spowodować dodatkowe obciążenie serwera, co może wymagać większego procesora lub dodatkowej pamięci.

SPRZĘT	MINIMALNE WYMAGANIA
CPU	Orion Server (NPM/NTA Main Poller) – processor czterordzeniowy lub lepszy; NTA Flow Storage Database – 6 core 2.5GHz lub lepszy (wersja 4.4)
Pamięć	Orion Server (NPM/NTA Main Poller) – 8GB minimum/16GB rekomendowany; NTA Flow Storage Database – 32GB (wersja 4.4)
Dysk twardy	Orion Server (NPM/NTA Main Poller) – 20GB minimum/40GB rekomendowany; NTA Flow Storage Database – 600GB (wersja 4.4)
OPROGRAMOWANIE	**MINIMALNE WYMAGANIA**
OS	NPM/NTA Main Poller – Windows Server 2016® lub późniejsze wersje, Windows Server 2019
Baza danych	Główne - NTA dzieli główną bazę danych SQL z Network Performance Monitor. SolarWinds wspiera Express, Standard oraz Enterprise w wersjach: • SQL Server 2014, 2014 SP1, 2014 SP2 • SQL Server 2016, 2016 SP1, 2016 SP2 • SQL Server 2017 Flow Database – Microsoft SQL Server 2016 SP1 lub późniejsze wersje NTA Flow Storage Database – Windows Server® 2016 lub późniejsze wersje, Windows Server 2019 SolarWinds wspiera zarówno główną bazę danych, jak i bazę danych NTA SQL Flow Storage w tej samej instancji serwera SQL, pod warunkiem, że jest to SQL 2016 lub późniejsza wersja. Wymagane jest połączenie z bazą danych Orion SQL, ponieważ dane CBQoS i niektóre dodatkowe szczegóły niskiego poziomu są nadal przechowywane w bazie danych Orion SQL.
Cloud	NTA obsługuje również korzystanie z Azure SQL Database i Amazon® RDS do przechowywania przepływów.

Server & Application Monitor

Szybkie wykrywanie i rozwiązywanie problemów z wydajnością



SolarWinds® Server & Application Monitor (SAM) jest przeznaczony do monitorowania aplikacji i ich infrastruktury pomocniczej, niezależnie od tego, czy działa lokalnie, w chmurze, czy w środowisku hybrydowym. Nie pozwól, aby wolne aplikacje i przestoje miały wpływ na użytkowników końcowych i usługi biznesowe. Określ główną przyczynę problemów z aplikacjami na różnych warstwach. Automatycznie identyfikuj środowisko aplikacji i rozpocznij monitorowanie zazwyczaj w ciągu godziny. Nie są potrzebne żadne profesjonalne usługi ani konsultacje.

SERVER & APPLICATION MONITOR W SKRÓCIE

- Monitoruje całe środowisko aplikacji - lokalne, chmurowe lub hybrydowe oraz infrastrukturę - za pomocą jednego narzędzia
- Ponad 1200 szablonów monitorowania aplikacji, systemu i infrastruktury
- Kompleksowe monitorowanie aplikacji Microsoft, systemów, hypervisora, produktów IaaS, PaaS i SaaS
- Wizualizuje i mapuje dynamiczne relacje oparte na komunikacji między aplikacjami i serwerami, aby wskazać problemy z siecią, które spowalniają aplikacje

FUNKCJE

Monitoring dostępności i wydajności aplikacji

Ponad 1200 szablonów aplikacji, systemów, infrastruktury i chmur, w tym Windows®, Linux®, Java®, Active Directory®, SharePoint®, Citrix®, Office 365® i wiele innych. Możliwość łatwego rozszerzenia monitorowania na dowolne niestandardowe lub własne aplikacje i wykorzystanie istniejących skryptów do budowy nowych monitorów.

Mapowanie zależności infrastruktury aplikacji

Wbudowany pulpit nawigacyjny AppStack™ został zaprojektowany w celu zapewnienia kontekstowego wglądu w sposób łączenia aplikacji z innymi komponentami w ramach infrastruktury IT, w tym serwerów, maszyn wirtualnych i systemów pamięci masowej.

Korelacje danych IT sieci cross-stack

Szybka identyfikacja źródła problemu, przeciągając i upuszczając wskaźniki wydajności sieci na wspólnej osi czasu, aby natychmiast uzyskać korelację wizualną dla wszystkich danych sieciowych.

Monitoring aplikacji chmurowych

Wdrożenia agentowe i bezagentowe można rozszerzyć o monitorowanie środowisk IaaS, takich jak Azure® i AWS, usługi PaaS dla Microsoft Azure oraz usługi SaaS dla Office 365. SAM zapewnia również monitorowanie kontenerów dla Docker®, Kubernetes® i Mesos®.

Dynamiczne mapy

SAM może automatycznie wykrywać relacje między aplikacjami i serwerami w oparciu o aktywną komunikację aplikacji i może zbierać statystyki połączeń sieciowych, takie jak utrata pakietów i opóźnienia.

Dogłębne monitorowanie Microsoft Exchange, IIS i SQL Server

Wbudowane szablony monitorowania AppInsight™ są zaprojektowane tak, aby zapewnić doskonały wgląd, wspierając identyfikację złożonych problemów z wydajnością w Microsoft Exchange™, IIS™ i SQL Server®.

- Active Directory®: uzyskanie szczegółowej statystyki AD, takiej jak replikacja, role FSMO, szczegóły witryny z podsieciami, zdarzenia użytkowników i komputerów, zdarzenia logowania, szczegóły procesów oraz usług i inne
- Exchange: wyświetlanie stanu bazy danych skrzynki pocztowej i jej przechowywania, identyfikacja problemów z replikacją i monitoring aktywności skrzynki pocztowej użytkownika
- IIS: monitoring dostępności witryn internetowych i puli aplikacji, zgłaszanie wygaśnięcie certyfikatu SSL i wykonywanie akcji zdalnych, aby uruchamiać / zatrzymywać pule aplikacji
- SQL Server: monitoring połączenia, sesji, transakcji bazy danych, operacji I/O na dysku, pamięci masowych, blokad, statusu zadania agenta SQL, obciążających zapytań według czasu procesora i inne

Konfigurowalne raporty i alerty dotyczące wydajności i dostępności

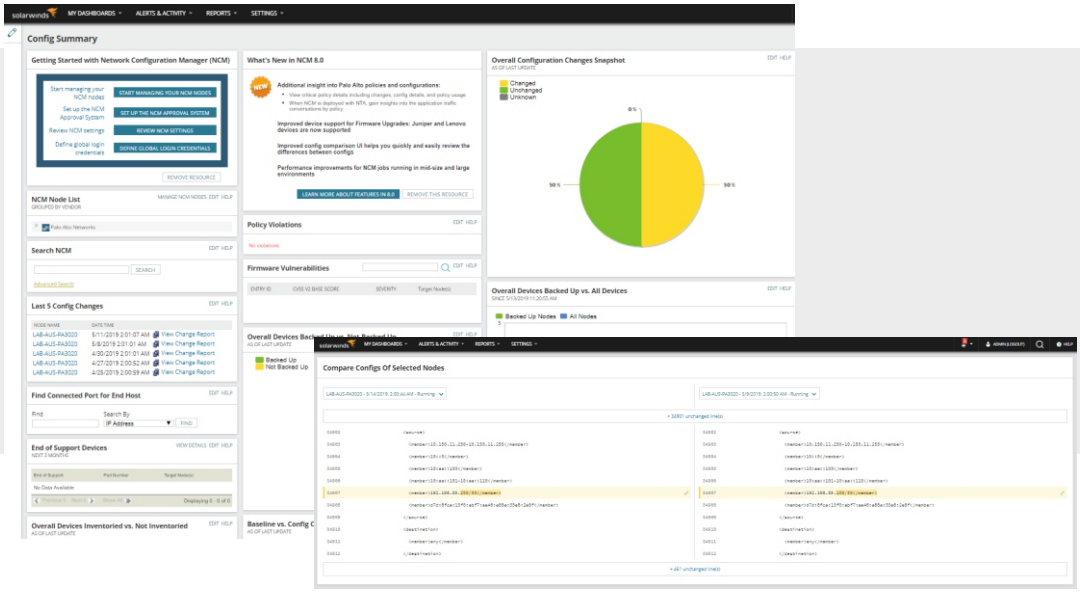
Planowanie i generowanie niestandardowych raportów wydajności systemu i alertów z setkami gotowych szablonów raportów. Szybka konfiguracja alertów i raportów dotyczących skorelowanych zdarzeń, trwałych warunków i złożonych kombinacji stanów urządzeń.

SAM jest częścią oprogramowania do zarządzania IT na platformie SolarWinds Orion®. SAM może bezproblemowo zintegrować się z innymi produktami na platformie Orion, w tym NPM, Virtualization Manager, Storage Resource Monitor i Web Performance Monitor, aby ujednolicić monitorowanie IT.

SPRZĘT	MINIMALNE WYMAGANIA
CPU	Procesor czterordzeniowy lub lepszy
Pamięć	6GB
Dysk twardy	Minimum 20GB
OPROGRAMOWANIE	**MINIMALNE WYMAGANIA**
OS	Windows Server® 2016
Baza danych	SolarWinds wspiera Express, Standard oraz Enterprise w wersjach: • SQL Server 2014, 2014 SP1, 2014 SP2 • SQL Server 2016, 2016 SP1 • SQL Server 2017

Network Configuration Manager

Zautomatyzowana konfiguracja sieci i zarządzanie zmianami



SolarWinds® Network Configuration Manager (NCM) może pomóc zaoszczędzić czas i poprawić niezawodność oraz bezpieczeństwo sieci, zarządzając konfiguracjami, zmianami i zgodnością dla routerów, przełączników i innych urządzeń sieciowych.

NETWORK CONFIGURATION MANAGER W SKRÓCIE

- NCM zapewnia gotowe wsparcie dla głównych dostawców urządzeń sieciowych, w tym Cisco, Palo Alto Networks, Juniper, HP, Huawei, F5, Avaya, Ruckus i innych
- NCM umożliwia automatyczne wdrażanie standardowych konfiguracji urządzeń
- NCM umożliwia ustawienie automatycznych kopii zapasowych konfiguracji urządzeń, a w razie potrzeby przywrócenie ostatnich znanych prawidłowych konfiguracji
- NCM automatycznie identyfikuje urządzenia IOS z potencjalnymi lukami w zabezpieczeniach, korzystając z usługi repozytorium NIST CVE, a nawet zapewni narzędzia do zarządzania dochodzeniem, identyfikacją i naprawą każdej luki
- NCM kontroluje konfiguracje urządzeń pod kątem zgodności z NIST FISMA, DISA STIG i DSS PCI
- Zbudowany na platformie Orion®, NCM zapewnia możliwość pełnej integracji z dodatkowymi modułami monitorowania sieci (monitorowanie wydajności sieci, analiza ruchu NetFlow, zarządzanie siecią WAN, VoIP, śledzenie urządzeń i zarządzanie adresami IP), a także systemami, pamięcią masową i zarządzanie wirtualizacją - wszystko w jednej konsoli internetowej
- NCM daje wybór sposobu wdrożenia - lokalnie lub w chmurze
- Oszczędzaj czas na identyfikację konfiguracji niezgodnych z wymaganiami przy użyciu wartości początkowych wielu urządzeń. Użyj pojedynczej linii bazowej lub wielu w całej sieci, aby monitorować krytyczne dla Ciebie konfiguracje

FUNKCJE

Network Insight™ dla Palo Alto Networks

Uzyskanie lepszego wglądu w złożone urządzenia, takie jak firewall'e Cisco ASA, przełączniki Cisco Nexus® oraz firewall'e Palo Alto Networks. Połączenie NCM z analizatorem ruchu NetFlow Traffic Analyzer (NTA) w celu wyświetlenia informacji o ruchu według zasad w kontekście polityk NCM na jednej stronie.

Elastyczność opcji wdrażania z bazą danych SQL Azure

Pełna kontrola nad wdrożeniem NCM, dzięki elastyczności wdrożenia lokalnie lub w chmurze z Azure SQL Database czy Amazon RDS.

Config-to-config Diff View

Wgląd w widoki diff config-to-config dodatkowo do widoku diff baseline-to-config. Wykorzystanie przeglądarki diff, aby szybko zidentyfikować zmiany w tych konfiguracjach.

Automatyzacja zmian konfiguracji

Uzyskanie pomocy w uproszczeniu i standaryzacji powtarzających się lub złożonych zmian konfiguracji, tworząc pojedynczy, niezależny od dostawcy skrypt, który można zaplanować i wykonać na routerach, przełącznikach i innych urządzeniach sieciowych firmy Cisco, Palo Alto Networks, Juniper, HP, Dell®, Brocade®, F5, Aruba®, Ruckus i innych.

Kopie zapasowe i przywracanie konfiguracji

Możliwość szybkiego przywrócenia działania po zmianie konfiguracji lub awarii urządzenia, dzięki przywróceniu najnowszych archiwów konfiguracji urządzenia.

Monitoring zmian

Alerty zmiany konfiguracji - alerty sygnalizujące zmiany w urządzeniu, pozwalają zobaczyć, jakie konkretne zmiany zostały wprowadzone.

Zarządzanie zmianami i aktualizacja oprogramowania sprzętowego

Zapobieganie błędom, dzięki przeglądaniu i zatwierdzaniu proponowanych zmian za pomocą zintegrowanego procesu zatwierdzania zmian. Wykorzystanie ról i uprawnień dostępu, w celu ulepszenia delegowania zadań, kontrolując kto może wprowadzać zmiany w urządzeniach i konfiguracjach. Aktualizacja urządzenia Lenovo i Juniper, dzięki funkcji aktualizacji oprogramowania sprzętowego NCM.

Baseline and Configuration Drift

Oszczędność czasu przy identyfikacji konfiguracji niezgodnych z wymogami przy użyciu wartości początkowych wielu urządzeń. Użycie pojedynczej linii bazowej lub wielu w całej sieci pozwala monitorować krytyczne konfiguracje, a wykorzystanie przeglądarki różnic, pozwala szybko zidentyfikować zmiany w tych konfiguracjach.

Wgląd w sieć Cisco Nexus

Przegląd konfiguracji interfejsu wraz z parametrami wydajności - filtrowanie, przeszukiwanie i identyfikacja zmiany konfiguracji dla list kontroli dostępu (ACL) – pozwala uzyskać monitorowanie i tworzenie kopii zapasowych dla każdego kontekstu urządzenia wirtualnego.

Wgląd w sieć Cisco ASA

Wykrywanie kontekstu zabezpieczeń, tworzenie kopii zapasowych i przywracanie plików konfigurowalnych, plików wizualizacji, audytowanie listy kontroli dostępu, a także zarządzanie aktualizacjami oprogramowania sprzętowego Cisco ASA.

Wgląd w sieć Palo Alto Networks

Pozwala na nie tylko dogłębne zrozumienie konfiguracji polityk, ale także fragmentów konfiguracji polityki i interfejsu, różnic konfiguracji dla zasad i zarządzania zasadami dla zapór sieciowych Palo Alto. Połączenie z NetFlow Traffic Analyzer (NTA) w celu zapewnienia widoczności konwersacji w ruchu sieciowym w kontekście polityk NCM na jednej stronie.

Skanowanie podatności w IOS

Poprawa bezpieczeństwa sieci przez automatyczne identyfikowanie luki i łatwe aktualizacje oprogramowania IOS.

Ocena i egzekwowanie zgodności

Łatwa ocena zgodności i gotowych raportów dotyczących krytycznych standardów bezpieczeństwa, takich jak DISA STIG, NIST FISMA, HIPAA, PCI DSS i wielu innych - a następnie za pomocą zautomatyzowanych skryptów naprawczych - usuwanie wszelkich naruszeń.

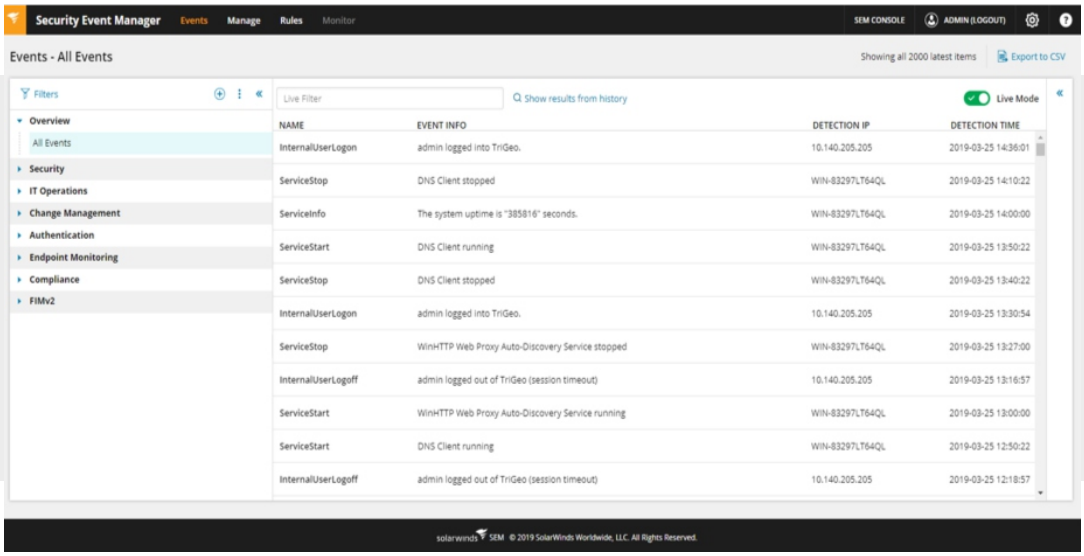
Integracja z Network Performance Monitor

Sprawdzenie czy konfiguracja w ścieżce usługi sieciowej uległa zmianie, dzięki integracji z funkcją NetPath™ NPM. Identyfikacja problemu z wydajnością lub konfiguracją na kluczowych urządzeniach sieciowych, dzięki Network Insight dla urządzeń Cisco Nexus, Cisco ASA i Palo Alto Networks.

SPRZĘT	MINIMALNE WYMAGANIA
CPU	3GHz podwójny procesor dwurdzeniowy
Pamięć	6GB minimum (8GB rekomendowane)
Dysk twardy	30GB
OPROGRAMOWANIE	**MINIMALNE WYMAGANIA**
OS	Windows Server® 2016 i 2019
.NET Framework	Wymagany Version 4.6.2
Baza danych	**On-premises:** • SQL Server® 2014, 2014 SP1, 2014 SP2 z Always On Availability Groups • SQL Server 2016, 2016 SP1 • SQL Server 2017 Cloud: • Azure SQL Database • Amazon RDS **Cloud:** • Azure SQL Database • Amazon RDS
OBSŁUGIWANE PROTOKOŁY	
SolarWinds Network Configuration Manager został zaprojektowany do obsługi wielu protokołów, w tym SNMP v1/v2/v3, Telnet, SSH v1/v2 i TFTP.	
INTEGRACJA Z INNYMI PRODUKTAMI I ZASOBAMI SOLARWIND	
Network Configuration Manager oferuje ścisłą integrację z Network Performance Monitor, NetFlow Traffic Analyzer, Web Help Desk®, Engineer's Toolset™ i THWACK®.	

UWAGA: Wymienione minimalne wymagania serwera zakładają konfigurację domyślną. Znaczne zwiększenie współczynnika odpytywania lub wskaźnika zbierania statystyk, może spowodować dodatkowe obciążenie serwera, co może wymagać większego procesora lub dodatkowej pamięci.

Security Event Manager



SolarWinds® Security Event Manager (dawniej Log & Event Manager) to potężne, instalowane lokalnie narzędzie, którego niska cena i skuteczność wykrywania zagrożeń, automatyczna analiza incydentów i odpowiedzi oraz raportowanie zgodności dla infrastruktury IT, zostało wybrane i docenione przez tysiące specjalistów ds. bezpieczeństw IT na całym świecie. To wszechstronne urządzenie SIEM (system do zarządzania informacją i zdarzeniami bezpieczeństwa) łączy zarządzanie logami, wykrywanie zagrożeń, normalizację i korelację, przekazywanie, raportowanie, monitorowanie integralności plików, monitorowanie aktywności użytkowników, wykrywanie i zapobieganie zagrożeniom z USB, wykrywanie zagrożeń oraz aktywną odpowiedź w urządzeniu wirtualnym, które jest łatwe do wdrożenia, zarządzania i używania. SolarWinds zaprojektował swój SIEM, aby zapewnić funkcjonalność, prostotę oraz cenę niższą niż większość znanych rozwiązań konkurencyjnych.

SECURITY EVENT MANAGER W SKRÓCIE

- Zaprojektowany, aby zbierać, konsolidować i analizować dzienniki oraz zdarzenia z firewall'i czy urządzeń IDS/IPS, przełączników, routerów, serwerów, dzienników systemu operacyjnego i innych aplikacji
- Korelacja w czasie rzeczywistym w celu identyfikacji zagrożeń i wzorów ataków
- Przekazywanie nieprzetworzonych danych dziennika do innych rozwiązań w celu dalszej analizy
- Zaprojektowany do wykrywania znanych złośliwych adresów IP i złośliwych działań, dzięki zintegrowanej inteligencji zagrożeń
- Automatyczna reakcja na podejrzane działania za pomocą akcji Active Response, w tym blokowanie wykrytych urządzeń USB, zamykanie działających procesów, wylogowywanie użytkowników
- Monitorowanie integralności plików (FIM) do monitorowania plików, folderów i ustawień rejestru systemu Windows pod kątem nieautoryzowanych lub podejrzanych zmian
- Generowanie gotowych raportów zgodności dla HIPAA, PCI DSS, SOX, ISO, DISA STIG, FISMA, FERPA, NERC CIP, GLBA, GPG13 i wielu innych

FUNKCJE

Skalowalne i łatwe zbieranie logów z urządzeń sieciowych i dzienników Windows/Linux

SEM zbiera i kataloguje dane dzienników oraz zdarzeń w czasie rzeczywistym z dowolnego miejsca, w którym generowane są dane w sieci.

Korelacja zdarzeń w czasie rzeczywistym

Przetwarzając dane dziennika przed ich zapisaniem w bazie danych, SEM może dostarczyć prawdziwą korelację z logami i zdarzeniami w czasie rzeczywistym, pomagając natychmiast rozwiązać problemy i zbadać naruszenia bezpieczeństwa i inne krytyczne problemy.

Przekazywanie logów

SEM przesyła surowe dane dziennika za pomocą protokołów syslog (RFC3164 i RFC 5244) do innych aplikacji w celu dalszej analizy.

Eksport logów do CSV

SEM pozwala na eksport logów do pliku CSV i załączanie ich do ticket'ów technicznych, udostępnianie zewnętrznym dostawcom i kontrahentom, przesyłanie do innych narzędzi w celu dalszej analizy, dzienników archiwalnych itp.

Threat Intelligence Feed

Wykorzystanie gotowych zbiorów szkodliwych adresów IP do identyfikacji nieprawidłowej aktywności. Regularna aktualizacja ze zbiorem źródeł badawczych i automatyczne oznaczanie zdarzeń, gdy mają one zły wpływ na urządzenia. Pozwala to na szybkie uruchamianie wyszukiwania, aby wyświetlić podejrzaną aktywność lub utworzyć reguły do wykonywania automatycznych działań.

Zaawansowane wyszukiwanie IT dla analizy podejrzanych zdarzeń

Zaawansowana funkcja wyszukiwania ad hoc IT SEM ułatwia wykrywanie problemów za pomocą interfejsu „przeciągnij i upuść", który natychmiast śledzi zdarzenia. Pozwala na zapisanie ustawień często wyszukiwanych danych, aby w móc z nich skorzystać w przyszłości.

Kompresja i przechowywanie logów

SEM przechowuje terabajty danych dziennika z wysokim stopniem kompresji w celu raportowania zgodności - kompresując i wypakowując dane, zmniejsza wymagania dotyczące pamięci zewnętrznej.

Ulepszone monitorowanie integralności plików w czasie rzeczywistym

Monitorowanie integralności plików (FIM) zostało zaprojektowane w celu zapewnienia szerszego wsparcia zgodności i głębszej inteligencji bezpieczeństwa dla zagrożeń wewnętrznych, szkodliwego oprogramowania typu zero-day i innych zaawansowanych ataków.

Wbudowana funkcja Active-Response

SEM może pomóc w natychmiastowym reagowaniu na zdarzenia związane z bezpieczeństwem, operacjami i regułami za pomocą automatycznych aktywnych odpowiedzi, które poddają kwarantannie zainfekowane komputery, blokują adresy IP i dostosowują ustawienia usługi Active Directory®.

Wykrywanie i zapobieganie zagrożeniom za strony łączy USB

SEM może pomóc w zapobieganiu utraty danych w punktach końcowych i ochronie wrażliwych danych za pomocą powiadomień w czasie rzeczywistym, gdy urządzenia USB się łączą. Może automatycznie blokować ich wykorzystanie oraz raportować z audytu wykorzystania USB.

Monitorowanie aktywności użytkownika

Powiększenie wiedzy poprzez wgląd w krytyczne działania użytkowników - kiedy używane są konta uprzywilejowane, w jaki sposób i przez kogo.

Gotowe szablony raportowania bezpieczeństwa i zgodności

SEM ułatwia szybkie generowanie i planowanie raportów zgodności przy użyciu ponad 300 szablonów raportów i konsoli, która pozwala dostosować raporty do specyficznych potrzeb organizacji.

Łatwe wdrażanie i obsługa

SEM został zbudowany w celu szybkiego i łatwego wdrożenia. Pozwala być na bieżąco i kontrolować dzienniki za pomocą modelu wdrażania urządzeń wirtualnych, konsoli internetowej i intuicyjnego interfejsu.

KTO POWINIEN UŻYWAĆ SECURITY EVENT MANAGER?

Zaprojektowany z myślą o specjalistach ds. bezpieczeństwa, którzy mają problemy z:

- brakiem widoczności ataków, a także ograniczonym czasem monitorowania personelu
- zgodnością wymagająca automatyzacji i/lub monitorowania integralności plików
- brakiem możliwości ustalania priorytetów, zarządzania i reagowania na incydenty bezpieczeństwa
- niskim czasem reakcji na incydenty
- niemożność określenia głównej przyczyny podejrzanych aktywności
- potrzebą monitorowania użytkowników wewnętrznych pod kątem dopuszczalnego użycia i zagrożeń wewnętrznych
- potrzebą udostępniania danych dziennika i danych o aktywności w zabezpieczeniach, sieci, aplikacjach i systemach

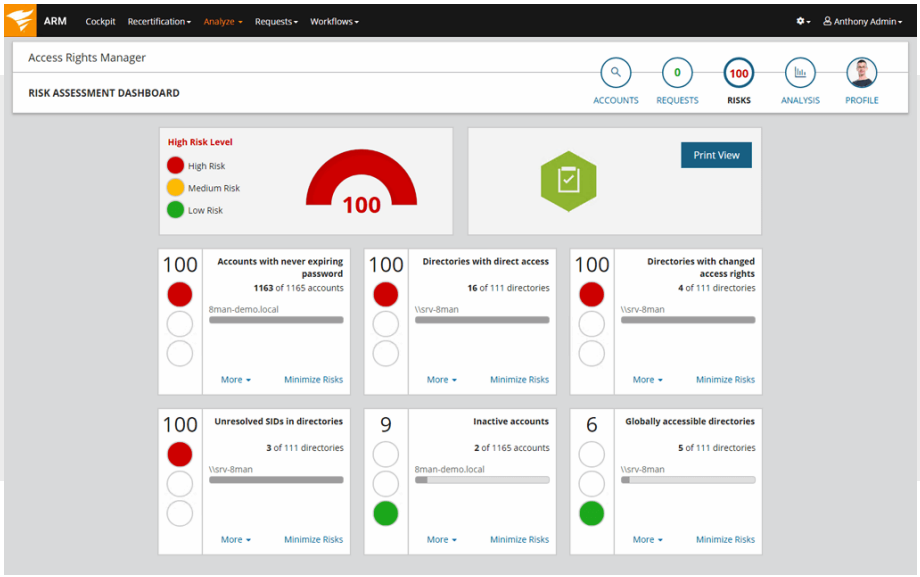
JAK SECURITY EVENT MANAGER WPŁYWA NA BEZPIECZEŃSTWO IT?

- Szybsze wykrywanie zdarzeń i powiadamianie o dopasowaniach informacji o zagrożeniach na podstawie adresów IP
- Bardziej inteligentne i niezawodne wykrywanie podejrzanych i złośliwych działań - w tym złośliwego oprogramowania, poufnych informacji i zaawansowanych zagrożeń
- Eliminacja czasochłonnych ręcznych procesów raportowania
- Skraca czas oczekiwania na odpowiedź, dzięki wydajnym funkcjom śledczym
- Automatycznie blokuje nadużycia, poprzez aktywną reakcję na naruszenia zasad sieci, systemu i dostępu
- Rozszerzona integracja narzędzi bezpieczeństwa, dzięki możliwości przesyłania logów do innych narzędzi
- Monitoruje i blokuje wykorzystanie USB na podstawie reguł
- Eksportuje logi do pliku CSV i pozwala na dołączanie ich do zgłoszeń technicznych lub udostępnianie zewnętrznym dostawcom
- Przyjazny dla użytkownika proces logowania z integracją pojedynczego logowania - użyj identyfikatora użytkownika i hasła, inteligentnej karty, jednorazowego hasła lub urządzenia biometrycznego

SPRZĘT	SMALL	MEDIUM	LARGE
CPU	2 – 4-rdzeniowy processor 2.0 GHz	6 – 10-rdzeniowy processor 2.0 GHz	10 – 16-rdzeniowy processor 2.0 GHz
Pamięć	8GB RAM	16 GB – 48 GB RAM	48 GB – 256 GB RAM
Dysk twardy	250GB, 15K twardego dysku (RAID 1/mirrored settings)	500GB, 15K twardego dysku (RAID 1/mirrored settings)	1TB, 15K twardego dysku (RAID 1/mirrored settings)
I/O operacji na sek. (IOPS)	40 – 200 IOPS	200 – 400 IOPS	400 lub więcej IOPS
NIC	1 GBE NIC	1 GBE NIC	1 GBE NIC
OPROGRAMOWANIE	MINIMALNE WYMAGANIA		
OS/Virtual	VMware vSphere ESX 5.5 lub ESXi 5.5 i późniejsze wersje		
Środowiska	Microsoft Hyper-V® Server 2016, 2012 R2, lub 2012		
Baza danych	Zintegrowana z urządzeniem wirtualnym		

Access Rights Manager

Zarządzaj prawami dostępu użytkowników i kontroluj je w całej infrastrukturze IT



SolarWinds® Access Rights Manager (ARM) ma na celu pomóc administratorom IT i administratorom bezpieczeństwa w szybkim i łatwym udostępnianiu, usuwaniu, zarządzaniu i kontrolowaniu praw dostępu użytkowników do systemów, danych i plików, aby mogli chronić swoje organizacje przed potencjalnym ryzykiem utraty i naruszenia danych. Analizując autoryzacje użytkowników i uprawnienia dostępu uzyskasz wizualizację tego, kto ma dostęp oraz kiedy go uzyskał. Wystarczy kilka kliknięć, aby wygenerować niestandardowe raporty oraz wykazać zgodność z większością wymogów regulacyjnych. Udostępnianie i usuwanie użytkowników za pomocą szablonów specyficznych dla ról, aby zapewnić zgodność delegowania uprawnień dostępu zgodnie z zasadami bezpieczeństwa.

ACCESS RIGHTS MANAGER W SKRÓCIE

- Łatwa analiza praw dostępu użytkowników w całej infrastrukturze IT
- Szybka identyfikacja i zmniejszenie ryzyka nieautoryzowanego dostępu do systemu i naruszenia danych
- Szybka prezentacja zgodności z raportami tworzonymi na żądanie lub zaplanowanymi do zautomatyzowanej dostawy
- Identyfikacja i zarządzanie ryzykiem poprzez wykrywanie złośliwych lub przypadkowych prób dostępu i zainfekowanych kont
- Łatwe tworzenie kont użytkowników i przeglądanie uprawnień użytkowników, grup i dostępu do wszystkich systemów, danych i plików
- Wsparcie dla terminowego i kompletnego usuwania dostępu dla użytkowników
- Zmniejszenie obciążenia IT i oszczędność czasu, delegowanie zarządzania uprawnieniami do właścicieli danych

FUNKCJE	ARM (AUDIT EDIDTION)	ARM (FULL VERSION)
Analiza praw dostępu użytkowników w całej infrastrukturze IT, uprawnień dla Active Directory, serwerów plików (Windows, EMC, NetApp) SharePoint, Exchange, OneDrive, SAP/R3	●	●
Audyt dla Active Directory, serwerów plików (Windows, EMC, NetApp) SharePoint, Exchange, OneDrive, SAP/R3	●	●
Monitorowanie (rejestrowanie) usługi Active Directory, serwerów plików (Windows, EMC, NetApp) SharePoint online, Exchange, OneDrive	●	●
Przegląd ryzyka analizy	●	●
Zarządzanie ryzykiem		●
Udostępnianie użytkowników dla usługi Active Directory		●
Zarządzanie użytkownikami Active Directory, serwerami plików (Windows, EMC, NetApp) SharePoint, Exchange, OneDrive		●
Koncepcja właściciela danych (delegowanie zarządzania prawami dostępu)		●
Samoobsługowy portal zarządzania uprawnieniami		●
Remediacja		●

ACCESS RIGHTS MANAGER - AUDIT EDITION

Active Directory

Zwiększa bezpieczeństwo monitorując, analizując i kontrolując Active Directory® oraz zasady grupy, aby zobaczyć, jakie zmiany zostały wprowadzone, przez kogo i kiedy te zmiany wystąpiły.

Udostępnianie pliku

Monitoring i kontrola serwerów plików, aby zapobiegać wyciekom danych i nieautoryzowanym zmianom wrażliwych plików i danych poprzez wizualizację uprawnień na serwerach plików.

Exchange

Uproszczenie monitorowania i audytu Exchange™, aby zapobiec naruszeniom danych. Śledzenie zmiany w skrzynkach pocztowych, folderach skrzynek pocztowych, kalendarzach i folderach publicznych.

SharePoint™

Wyświetlanie uprawnień SharePoint w strukturze drzewka pozwala szybko sprawdzić, kto jest upoważniony do dostępu danego zasobu SharePoint. Korzystając z raportu porównawczego skanowania, można dowiedzieć się, kto dokonał zmian w uprawnieniach i na czym one polegały.

Analiza uprawnień użytkownika

Ochrona systemu przed wewnętrznymi zagrożeniami bezpieczeństwa, analizując dostęp użytkowników do usług i serwerów plików z widocznością członkostwa w grupach z Active Directory i serwerów plików.

Generowanie niestandardowych raportów

Tworzenie i generowanie raportu dotyczącego zarządzania i audytu, który pomaga wykazać zgodność z przepisami, pokazując prawa dostępu użytkowników za pomocą zaledwie kilku kliknięć. Rejestrowanie działań w usłudze Active Directory i serwerach plików według użytkownika.

ACCESS RIGHTS MANAGER – FULL EDITION

ARM Full Edition zawiera wszystkie funkcje Audit Edition oraz poniższe.

Udostępnianie i zarządzanie użytkownikami dla Active Directory

Konfiguracja nowych kont użytkowników i zarządzanie nimi w ciągu kilku sekund, dzięki znormalizowanym szablonom dla roli, które zapewniają dostęp do serwerów plików i Exchange.

Koncepcja właściciela danych, przekazywanie praw dostępu dla właścicieli danych

Definiowanie kategorii danych w całej organizacji, przypisanie ich właścicieli funkcjonalnych i delegowanie części zarządzania uprawnieniami do właścicieli danych.

Samoobsługowy portal zarządzania uprawnieniami

Przenoszenie prawa dostępu do danych bezpośrednio w ręce właścicieli danych zamiast administratora, korzystając z internetowego, samoobsługowego portalu uprawnień.

WYMAGANIA SYSTEMOWE	DO 1000 UŻYTKOWNIKÓW	1001-4000 UŻYTKOWNIKÓW	PONAD 4000 UŻYTKOWNIKÓW
Dysk twardy	30 GB	40 GB	40 GB
Pamięć	4 GB	8 GB	16 GB
CPU	Dual Core Processor lub lepszy		
System operacyjny	Microsoft Windows Server® 2008 R2, 2012, 2012 R2, 2016 i 2019		
NIC	SQL Server® 2008 SP1, 2012, 2014, 2016, 2017 (32-bit i 64-bit), 2017		
.NET Frameworks	wymagana .NET 3.5 SP1 i .NET 4.5.2 (lub wyższa wersja)		
WYMAGANIA DLA KOLEKTORA			
Dysk twardy	5 GB		
CPU	Procesor dwurdzeniowy lub lepszy		
Pamięć	4 GB		
System operacyjny	Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 and 2019		
.NET Framework	.NET 3.5 SP1 i .NET 4.5.2 lub nowszy		

Narzędzia SolarWinds

WEB HELP DESK®
Obsługa zgłoszeń do pomocy technicznej i zarządzanie zasobami w przystępnej cenie

DAMEWARE® REMOTE SUPPORT
Zdalne sterowanie i narzędzia do zarządzania systemami

ENGINEER'S TOOLSET
Sześćdziesiąt narzędzi niezbędnych w rozwiązywaniu i diagnostyce problemów z siecią

KIWI SYSLOG® SERVER
Scentralizowane zarządzanie dziennikami urządzeń sieciowych i serwerów

NETWORK TOPOLOGY MAPPER
Automatyczne rozrysowywanie sieci zazwyczaj w ciągu zaledwie kilku minut

MOBILE ADMIN
Uproszczenie administrowania systemem IT oraz zarządzania nim za pomocą urządzeń przenośnych

SERV-U® MANAGED FILE TRANSFER
Bezpieczne przesyłanie plików wewnątrz organizacji oraz poza nią

Produkty zabezpieczające SolarWinds

LOG & EVENT MANAGER
ACCESS RIGHTS MANAGER
BACKUP
RISK INTELLIGENCE
SERV-U
PATCH MANAGER
NETWORK CONFIGURATION MANAGER
THREAT MONITOR™
SERVER CONFIGURATION MONITOR

IP ADDRESS MANAGER

Łatwe w użyciu oprogramowanie do zarządzania adresami IP

- Zautomatyzowane śledzenie, alarmowanie i raportowanie adresów IP
- Zintegrowane zarządzanie adresami DHCP, DNS i IP
- Śledzenie szczegółowych informacji i historii adresów IP

solarwinds.com/IPAM

LOG ANALYZER

Proste badanie danych z komputera usprawniające wykrywanie głównej przyczyny problemów w systemie IT

- Wydajne i intuicyjne agregowanie dzienników, znakowanie, filtrowanie oraz wysyłanie ostrzeżeń umożliwiające efektywne rozwiązywanie problemów
- Pełne zintegrowanie z produktami z platformy Orion umożliwiające ujednolicony podgląd monitorowania infrastruktury IT i powiązanych dzienników

solarwinds.com/LA

NETWORK AUTOMATION MANAGER

Zunifikowane oprogramowanie do zarządzania automatyzacją i operacjami w sieci

- Zaawansowane monitorowanie sieci
- Monitorowanie ruchu, przepustowości i sieci WAN
- Zarządzanie zmianami i konfiguracją
- Wysoka dostępność

solarwinds.com/NAM

DATABASE PERFORMANCE ANALYZER

Monitorowanie głównych platform baz danych przez całą dobę, 7 dni w tygodniu w czasie rzeczywistym oraz historycznie zarówno lokalnie, jak i w chmurze

- Prosta i intuicyjna analiza głównych przyczyn problemów oparta na badaniu czasu oczekiwania z poziomu bazy danych lub zapytania
- Aktywne optymalizowanie nieefektywnego obciążenia za pomocą narzędzia Table Tuning Advisors
- Wykrywanie anomalii oparte na uczeniu maszynowym w celu rozpoznawania odchyleń od oczekiwanego działania

solarwinds.com/DPA

VIRTUALIZATION MANAGER

Zarządzanie wydajnością, rozwiązywanie problemów z przepustowością i przyrostem - od maszyn wirtualnych do magazynów danych

- Dogłębny wgląd w wykorzystanie i wydajność maszyn wirtualnych, hostów, klastrów i magazynów danych
- Ulepszone informacje operacyjne umożliwiające wprowadzanie wieloetapowych rozwiązań w zakresie aktywnej i przewidywanej wydajności maszyn wirtualnych oraz alokacji zasobów za pomocą jednego kliknięcia
- Rozszerzenie monitorowania na chmurę dzięki platformie Azure®i usługom AWS IaaS

solarwinds.com/VMAN

STORAGE RESOURCE MONITOR

Pojemność umożliwiająca obsługę wielu dostawców oraz monitorowanie wydajności, przesyłanie ostrzeżeń i tworzenie raportów

- Rozwiązanie zaprojektowane z myślą o zapewnieniu wglądu w wydajność historyczną oraz w czasie rzeczywistym na wielu poziomach (macierzy, puli magazynu, jednostek LUN, grup RAID i innych)
- Zautomatyzowane planowanie pojemności magazynowej w całej flocie w celu zidentyfikowania szczególnie aktywnych miejsc w godzinach szczytu
- Identyfikowanie systemowej rywalizacji pomiędzy jednostkami LUN i innymi zagrożonymi jednostkami w środowisku magazynowania

solarwinds.com/SRM

WEB PERFORMANCE MONITOR

Pomiary aktywności użytkowników i rozwiązywanie problemów z opóźnieniami w aplikacjach internetowych

- Wgląd w środowisko użytkownika końcowego w przypadku transakcji aplikacji internetowych SaaS
- Monitorowanie wydajności aplikacji za zaporą sieciową z wielu lokalizacji
- Wbudowana integracja z platformą Orion umożliwiająca podgląd zależności w obrębie infrastruktury w celu przyśpieszenia rozwiązywania problemów

solarwinds.com/WPM

SERVER CONFIGURATION MONITOR

Informacje o dacie i godzinie wprowadzenia zmian w konfiguracji serwera oraz identyfikacja osoby odpowiedzialnej za ich wprowadzenie

- Wykrywanie zmian w konfiguracji sprzętowej, oprogramowaniu, plikach, rejestrze, danych wyjściowych skryptu i innych parametrach serwera
- Ocena zmian w stosunku do niestandardowych wartości odniesienia oraz w czasie
- Korelowanie zdarzeń dotyczących wydajności ze zmianami konfiguracji

solarwinds.com/SCM