OFEROWANE PRODUKTY

KATALOG 2023

SECURIVY

Kim jesteśmy?

Dlaczego warto z nami współpracować?

Naszym celem jest zapewnienie przedstawicielom każdej branży zautomatyzowanej, inteligentnej ochrony przed zagrożeniami. Jesteśmy dystrybutorem rozwiązań bezpieczeństwa IT, które cechują się łatwością we wdrożeniu i użytkowaniu oraz intuicyjnym i przejrzystym modelem licencjonowania. Parterstwo pozwoli Ci, pod naszą opieką, oferować klientom unikatowe oraz innowacyjne w Polsce produkty.

Współparcując z nami, możesz liczyć na:

- Transparentność, łatwy i czytelny program partnerski, jasne warunki współpracy
- Unikatowe produkty - popularne za granicą i nowe w Polsce
- Wsparcie w postaci przedstawienia zasad sprzedaży i licencjonowania produktów z naszego portfolio
- Wysoką marżę (25 - 35%)
- Dostęp do najnowszych informacji na temat promocji, premier i organizowanych wydarzeń
- Pomoc w organizacji i prowadzeniu spotkań z klientami
- Prawo do rezerwacji
- Newsletter dla partnerów z aktualnościami i materiałami
- Dostęp do rozwiązań testowych i pomoc we wdrożeniu klienta
- Proste warunki kredytu kupieckiego
- Webinary przedstawiające produkty, aspekty techniczne
- Wsparcie handlowe, materiały produktowe zawsze pod ręką

Mamy odpowiedź na Twoje obawy:

Potrzeba posiadania wykwalikowanego zespołu i lokalnego wsparcia	Potrzeba pilnowania okresu wygaśnięcia projektu	Potrzeba szybkiej reakcji, elastyczności i dostępu do aktualnych materiałów
Oferujemy Ci wsparcie inżyniera, który przeprowadzi szkolenie dla Twojego zespołu i wspólnie wdroży produkt u Twojego klienta.	Przypomnimy o nadchodzącym terminie i potrzebie aktualizacji projektu.	Dostarczymy Ci potrzebne materiały, a także gotowe skrypty wiadomości do klientów. Pozostaniemy w kontakcie w razie problemów.

Monitorowanie aktywności firm zewnętrznych i pracowników

Ekran System On-Premises

Ekran System to wielofunkcyjne rozwiązanie agentowe, które umożliwia monitorowanie oraz kontrolę działań użytkowników, a także firm zewnętrznych na komputerach i serwerach.

Oprogramowanie pozwala rejestrować wszystko to, co dzieje się na ekranie komputera, tworząc indeksowany film połączony z metadanymi, dzięki czemu możesz przeszukiwać nagrania po słowach kluczowych. Ekran System pozwala także zarządzać dostępem uprzywilejowanym (Privileged Access Management, czyli PAM).

Dlaczego firmy wybierają Ekran System On-Premises?

1

Zarządzanie dostępem uprzywilejowanym (PAM) Kontroluj każde połączenie RDP i SSH.

Przekazywanie wszystkich tymczasowych poświadczeń, dzięki możliwości zarządzania dostępem uprzywilejowanym.

2

Monitorowanie aktywności firm zewnętrznych.

Kontrola pracy firm zewnętrznych bez względu na rodzaj użytkownika. Zapewnienie bezpieczeństwa firmowych danych i odpowiednie rozliczanie zleceń wykonywanych przez firmy outsourcingowe.

3

Zapis wideo nagranych sesji oraz metadane.

Nagrywanie wszystkiego, co dzieje się na ekranie komputera, wraz z zapisem metadanych np. nazwy nagłówków aplikacji i stron internetowych. Przeglądanie nagrania przy pomocy odtwarzacza podobnego do YouTube.

4

Alerty i powiadomienia w czasie rzeczywistym.

Konfiguracja alertów powiadamiających w czasie rzeczywistym o niechcianej aktywności wybranych użytkowników. Informacje niepożądanych zajściach trafiają na skrzynkę mailową.

5

Zapobieganie wyciekom firmowych danych.

Zabezpieczenie firmy przed nieautoryzowanym dostępem i niechcianym przesyłaniem plików na urządzenia zewnętrze oraz do chmury. Zmniejszenie ryzyka wycieku i kradzieży danych.

6

Nagrywanie wszystkich sesji zdalnych i lokalnych.

Nagrywanie ekranu użytkowników pracujących z biura oraz tych wykonujących swoją pracę zdalnie. Monitorowanie ich aktywności oraz efektywności niezależnie od tego, w jakim miejscu się znajdują.

Wspierane platformy:

macOS vmware UNIX CITRIX

Monitorowanie aktywności wybranych pracowników i zabezpieczenie danych

Ekran System SaaS

dedykowanany małym i średnim firmom bez rozbudowanej infrastruktury IT

Ekran System pozwala na monitorowanie komputera pracownika – niezależnie od tego, czy jest to klasyczny komputer stacjonarny, czy laptop. Dzięki swojej architekturze Ekran System jako aplikacja **SaaS (ang. Software as a Service – oprogramowanie jako usługa**) przetwarza dane w chmurze obliczeniowej.

Monitorowanie aplikacji to tylko jedna z funkcji Ekran System. Na uwagę zasługuje także dokładny, szczegółowy zapis wszystkich działań wykonywanych za pomocą komputera. Raport obejmuje pełen zestaw zapisanych czynności, w tym między innymi monitorowanie odwiedzanych stron, monitorowanie wydajności komputera, danych wprowadzanych za pomocą klawiatury (tzw. keylogger) i wielu innych.

Co więcej, pomimo wykorzystywania przez Ekran System technologii wykonywania obliczeń w chmurze, program umożliwia także monitoring w sytuacjach, gdy pracownik nie ma dostępu do internetu, a śledzenie komputera odbywa się offline.

Dlaczego firmy wybierają Ekran System SaaS?

1

Kontrola efektywności pracowników

Monitorowanie i nagrywanie wszystkiego tego, co dzieje się na ekranie komputera pracownika.

2

Monitorowanie firmowych plików

Kontrola przesyłanych i kopiowanych plików na nośniki zewnętrzne lub wysyłane do chmury.

3

Blokowanie urządzeń USB

Określenie, z jakich nośników zewnętrznych mogą korzystać pracownicy, a które mają być blokowane.

4

Przeszukiwanie nagrań

Wszystkie zarejestrowane nagrania skojarzone są z powiązanymi słowami kluczowymi. Pozwala to na łatwe odnalezienie istotnych informacji.

Kontrolowane podwyższanie uprawnień administracyjnych

Admin By Request

W większości przypadków użytkownicy potrzebują uprawnień administratora, aby zainstalować lub zaktualizować niezbędne do pracy oprogramowanie. Pozostawienie pracownikom uprawnień administratora lokalnego na stałe, jest bardzo ryzykowne i może wiązać się z licznymi nadużyciami przywilejów. Pełne ich odebranie z drugiej strony znacznie zmniejszy efektywność pracy, z uwagi na ograniczenia dostępu do aplikacji.

Admin By Request zapewnia idealny kompromis w tej kwestii. Gdy użytkownik rozpoczyna instalację lub uruchamia program z uprawnieniami administratora, cały proces jest raportowany w dzienniku aktywności.

Dlaczego firmy wybierają Admin By Request?

1

Odebranie uprawnień administracyjnych

Całkowite usunięcie uprawnień administracyjnych na komputerach służbowych, przy jednoczesnym zapewnieniu komfortu pracy. Potrzeba podwyższenia uprawnień sygnalizowana jest za pomocą wysyłanych zgłoszeń, a ich akceptacja może odbywać się za pomocą aplikacji mobilnej.

2

Przyznawanie uprawnień administracyjnych

Administrator ABR otrzyma wszystkie zgłoszenia użytkowników w czasie rzeczywistym, co pozwala na ich natychmiastową autoryzację. Dostęp do logów sesji użytkowników z podwyższonymi uprawnieniami odbywa się poprzez aplikację webową. Istnieje możliwość sprawdzenia czy aktywność użytkownika była zgodna z powodem podanym przy zgłoszeniu.

3

Tworzenie white i black list dla wybranych aplikacji

Definiując listę dozwolonych aplikacji określa się, które programy będą mogły być używane przez pracowników bez konieczności wysyłania zgłoszeń do zespołu IT. Z kolei blacklisty mogą zawierać spis niedostępnych aplikacji, których uruchomienie będzie niemożliwe nawet podczas sesji administracyjnej.

4

Zabezpieczenie przed malware i ransomware

Automatyczne skanowanie plików w czasie rzeczywistym (nawet podczas sesji administracyjnej) zapewnia firmie dodatkowe zabezpieczenie przed atakami malware i ransomware. Co najważniejsze, tego typu ochrona jest w pełni kompatybilna z innymi antywirusami, więc nie będzie zakłócała ich poprawnego funkcjonowania.

Wspierane platformy:

macOS

Zarządzanie informacjami i zdarzeniami

Logsign Unified SO Platform

Narzędzie Logsign to rozwiązanie pozwalające na gromadzenie, przechowywanie oraz monitorowanie informacji z dowolnego źródła w infrastrukturze IT organizacji. System ten odpowiada za indeksację zebranych danych, w celu późniejszej analizy i umocnienia zabezpieczeń. Określane są wówczas informacje o zagrożeniach, a także dane o tożsamości i aktywności użytkowników w obszarze firmowej sieci.

Logsign wykrywa w czasie rzeczywistym incydenty cyberbezpieczeństwa. Cały proces odbywa się przy użyciu wbudowanych alertów, reguł oraz zaawansowanych funkcji dochodzeniowych.

Logsign łączy w sobie rozwiązania klasy SIEM oraz SOAR (Security Automation, Orchestration and Response), stając się tym samym narzędziem pozwalającym na skuteczną automatyzację procesów cyberbezpieczeństwa, zapewnienie płynności pracy i natychmiastową reakcję na zagrożenia.

Dlaczego firmy wybierają Logsign?

1

Infrastruktura Big Data z nieskończoną skalowalnością

- Szybkie wdrożenie i łatwa konfiguracja w każdym środowisku.
- Nieograniczone możliwości gromadzenia i przechowywania danych.
- Odporny na awarie system.

2

Szybka i skuteczna ochrona danych

- Łagodzenie i eliminacja cyberzagrożeń.
- Automatyczne powiadamianie o incydentach.
- Zapobieganie phishingowi i podejrzanemu ruchowi sieciowemu.

3

Nieograniczone możliwości gromadzenia i przechowywania danych

- Możliwość dostosowania zakresu wykorzystywanych funkcjonalności do potrzeb firmy.
- Zaawansowane techniki analizy i indeksacji danych.
- Intuicyjność i prostota klasyfikacji zebranych informacji.

4

Automatyzacja i zarządzanie procesami w firmie

- Zachowanie stałego przepływu pracy.
- Interaktywne zarządzanie procesami.
- Badanie cykli życia potencjalnych cyberzagrożeń.

Najwyższy poziom zabezpieczeń infrastruktury sieciowej

Arista NG Firewall

Firewall Nowej Generacji to rozwiązanie dla firm, którym zależy na najwyższym poziomie bezpieczeństwa IT. Oprogramowanie znajdzie zastosowanie w każdym przedsiębiorstwie – bez względu na jego wielkość i branże. Dzięki rozbudowanym funkcjom administrator zyskuje wgląd do ruchu sieciowego, filtrowania treści oraz zaawansowanej ochrony przed zagrożeniami.

Firewall Nowej Generacji zbiera dane i informacje telemetryczne z plików oraz adresów IP i URL, które następnie analizuje. Dzięki temu, sprawnie zabezpieczy infrastrukturę sieciową przed zagrożeniami wewnętrznymi oraz zewnętrznymi.

Dlaczego firmy wybierają Arista NG Firewall?

1

Wydajność

Optymalna przepustowość oraz wydajności dla aplikacji krytycznych. Narzędzie zapewnia najwyższy poziom QoS (Quality of Service).

2

Łączność

Konfiguracja połączeń zdalnych, w tym także połączeń VPN i zarządzanie dostępem do sieci firmowej

3

Filtrowanie

Weryfikacja podejrzanych aplikacji, punktów dystrybucji złośliwego oprogramowania oraz zaszyfrowanych żądań internetowych.

4

Zabezpieczenie

Kontrola oraz blokowanie zagrożeń na poziomie bramy sieciowej, chroniące użytkowników oraz elementy infrastruktury IT.

5

Zarządzanie

Zarządzanie dostępem dla użytkowników, grup oraz aplikacji. Kontrola przeglądanych stron internetowych oraz używanych programów i wzmacnianie zabezpieczeń do danych biznesowych.

6

Elastyczność

NG Firewall może zostać skonfigurowany na sprzęcie, który posiada firma albo skompletować specjalnie przeznaczone do tego celu urządzenie. NG Firewall wymaga zainstalowania w bramie do sieci dedykowanego serwera opartego na technologii Intel.

Kontrola jakości ruchu sieciowego

Arista Micro Edge SD-WAN

Arista Micro Edge SD-WAN Router to kompleksowe narzędzie, które pozwoli Ci zadbać o jakość ruchu sieciowego i dostępu do serwerów. Wbudowany firewall filtruje potencjalnie niebezpieczne aplikacje, hosty oraz adresy URL, dzięki czemu zapewnia odpowiednią prewencję przed cyberzagrożeniami.

Wdrożenie SD-WAN Router pomoże Ci zarządzać ruchem sieciowym, a także regulować przepustowość łącza. Funkcje optymalizacji WAN pozwalają również na priorytetyzację działań wszystkich aplikacji krytycznych, niezależnie od lokalizacji biura.

Dlaczego firmy wybierają Arista Micro Edge SD-WAN?

1

Łączność między oddziałami w różnej lokalizacji

Sprawna łączność między różnymi oddziałami firmy. SD-WAN Router dostarczy firmie wiele ścieżek dostępu do Internetu i zabezpieczy sieć przed awariami. Utworzenie tunelu VPN umożliwi bezpieczne i łatwe połączenie wszystkich oddziałów z siecią korporacyjną.

2

Zero-Touch Provisioning

Zero Touch Provisioning, czyli "bezobsługowa konfiguracja", która pozwoli na szybkie wdrożenie rozwiązania Untangle SD-WAN Router. Wystarczy uruchomić urządzenie i podłączyć je do sieci, a wszystkie potrzebne ustawienia zostaną pobrane automatycznie.

3

Optymalizacja sieci WAN

Maksymalizacja QoS wewnątrz infrastruktury firmowej, prioretyzacja ruchu krytycznego i poprawa łączności z Internetem. Monitoring wydajności łącza w czasie rzeczywistym za pomocą równoważenia sieci WAN.

4

Wbudowany firewall

Zapewnienie optymalnego poziomu zabezpieczeń, dzięki wbudowanemu firewallowi. Rozwiązanie filtruje aplikacje wysokiego ryzyka, hosty, adresy URL oraz zmniejsza ruch, który może spowodować uszkodzenie sieci.

5

Elastyczne wdrożenie - aplikacja w wirtualnym środowisku

Arista Micro Edge SD-WAN Router może zostać uruchomione jako urządzenie pracujące w zwirtualizowanym środowisku VMware ESX lub ESXi. Firma może wykorzystać wcześniejsze inwestycje w infrastrukturę, zapewniając prioretyzację aplikacji o znaczeniu krytycznym.

SKONTAKTUJ SIĘ Z NAMI
ABY DOWIEDZIEĆ SIĘ WIĘCEJ

SECURIVY

Odwiedź nas na:
www.securivy.com

Obserwuj nas:

Kontakt:
Securivy Sp. z o.o.
NIP: 7792534607
biuro@securivy.com
tel. +48 573 568 234

Ekran system
Admin By Request
ARISTA
Logsign