KATALOG PRODUKTÓW I USŁUG 2023

SECURIVY

Spis treści:

Produkty:

Usługi:

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).

Co wyróżnia Ekran System?

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

Logsign

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. Arista Micro Edge 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 Arista Micro Edge. 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.

Zapewnienie komfortu pracy zdalnej

Microsoft 365

Rozwiązania dostępne w ramach usług Microsoft 365 pozwalają na komfortową i wydajną pracę w dowolnej lokalizacji. Wykonywanie obowiązków zawodowych oraz współpraca w ramach zespołów może odbywać się niezależnie od tego, w jakim miejscu znajdują się pracownicy.

Jednocześnie narzędzia proponowane przez międzynarodowego giganta branży IT są budżetowe i intuicyjne, dlatego ich wdrożenie jest możliwe w każdej firmie – bez względu na jej wielkość.

Dlaczego firmy wybierają Microsoft?

1. Dostęp do profesjonalnej poczty firmowej utworzonej we własnej domenie
2. Zarządzanie plikami z dowolnego miejsca z wykorzystaniem chmury One Drive i SharePoint
3. Kontakt w czasie rzeczywistym oraz organizacja spotkań video
4. Innowacyjny klient poczty - outlook pozwala pracować wydajniej, integrując pocztę e-mail, kalendarz, kontakty, zadania w jednym miejscu
5. Zredukowana liczba e-maili i przestojów w komunikacji poprzez wysyłanie wiadomości na czacie
6. Zabezpieczona współpraca wewnętrzna i zewnętrzna - dane są szyfrowane zarówno podczas przesyłania, jak i spoczynku.

Możliwość korzystania z aplikacji dostępnych w ramach pakietów Microsoft w dowolnym miejscu:

Wielowarstwowa ochrona
Comodo Xcitium

COMODO CYBERSECURITY

Kompleksowa platforma ITSM zarządzana z poziomu przeglądarki internetowej dla całego działu informatycznego. Comodo zawiera system przyjmowania i obsługi zgłoszeń. Pełne zarządzanie bezpieczeństwem firmy od oprogramowania antywirusowego, po: zarządzanie aktualizacjami (patch manager), automatyczne piaskownice (sandbox), dostęp do aplikacji, kontrole wycieków danych Wszystkie narzędzia jakich potrzebujesz (DLP), własnych procedur. w jednym miejscu m.in zdalny pulpit power schell, proces-manager, przesyłanie plików, aż po zdalne uruchamianie własnych procedur.

Pakiet Comodo Xcitium zawiera:
- Antywirus,
- Firewall,
- Auto sandbox,
- Zdalny Pulpit,
- WebFilter,
- Ochrona urządzeń mobilnych,
- Patch Manager,
- Centralne zarządzanie Web,
- Service desk,
- Ochrona serwerów,
- EDR.

Dlaczego firmy wybierają Comodo?

1

Wysoce konfigurowalny firewall odpowiada za filtrowanie pakietów, chroni przed zagrożeniami przychodzącymi i wychodzącymi oraz włamywaczami jak i atakami internetowymi.

2

Oparty na zasadach systemu zapobiegania włamaniom. Monitoruje on wszystkie działania aplikacji i procesów w systemie i zapobiega jego uszkodzeniu.

3

Aktywny silnik antywirusowy, który automatycznie wykrywa i eliminuje wirusy, robaki i inne złośliwe oprogramowanie.

4

Usługa odnośnika plików w chmurze (FLS). Sprawdza reputacje plików, identyfikuje ją na białej lub czarnej liście

5

Behawioralnie monitorowanie wszystkich procesów i wpisów pod względem szkodliwości działania, może odwracać szkodliwe akcje.

Usługi

Outsourcing IT i obsługa informatyczna firm

Współpracujemy z klientami, którzy oczekują poprawy efektywności infrastruktury informatycznej. Jest to możliwe przy jednoczesnym zmniejszeniu kosztów związanych z zapleczem IT. Dlaczego? Przedsiębiorstwo nie musi budować swojego zespołu inżynierów, aby obsługiwać kluczowe procesy w firmie. Posiadamy bogatą wiedzę, która pozwala na zapobieganie przerwom w działaniu sieci i urządzeń.

Jako doświadczeni specjaliści rozwiązaliśmy setki problemów i awarii, dzięki czemu potrafimy sprawnie zmierzyć się z każdym wyzwaniem. Dysponujemy najnowszymi narzędziami, wspierającymi rozwój biznesu i zarządzanie kluczowymi aspektami systemów informatycznych. Doradzamy, dopasowujemy i wdrażamy rozwiązania, które poprawią wydajność pracy i komfort użytkowników.

Jak wygląda współpraca z nami?

1

Opieka specjalisty
Zapewniamy dedykowanego opiekuna, który służy bezpośrednim oraz sprawnym kontaktem, w razie zleceń, awarii, czy pytań.

2

Rozliczanie minutowe
W ramach współpracy, otrzymasz dostosowany do Twojej firmy pakiet godzin do wykorzystania w miesiącu. Naszą pracę rozliczamy na podstawie minut przeznaczonych na każde zadanie

3

Zakres działań
Przejmujemy na siebie cały zakres obowiązków informatycznych lub pewną ich część, w zależności od Twoich potrzeb.

4

Kanał komunikacyjny
Skonfigurujemy formularz help-desk, dzięki któremu będziesz mógł zgłosić wszelkie potrzeby i problemy. Będzie to jeden, wygodny i sprawny kanał komunikacyjny dla Ciebie i Twoich pracowników.

5

Raporty
Raportujemy wszelkie działania podjęte w ramach outsourcingu IT. Dzięki temu, pod koniec każdego miesiąca udostępniamy dokument zawierający listę wykonanych usług oraz czas ich wykonania.

6

Zlecenia i projekty
Podejmujemy się projektów, które zmierzają w kierunku rozwoju IT Twojej firmy. Nie ograniczamy się jedynie do zleceń help-desk. Pomocy udzielamy przez zdalny dostęp oraz w siedzibie Twojej firmy.

Usługi

Audyt pracowników

Audyt pracowników to usługa, która pomoże Ci sprawdzić efektywność poszczególnych osób i zespołów.

Ocenę opieramy na następujących danych:
- aplikacjach i stronach, które odwiedzali pracownicy
- godzinach logowania, które pozwalają poznać realny czas pracy
- czas aktywności podczas wykonywania obowiązków
- alerty informujące o niepożądanej aktywności

Dodatkowo zapewni Ci ona dostęp do informacji na temat podłączanych urządzeń USB i plików przesyłanych do niepożądanych osób. Korzystając z usługi audytu pracowników, nie musisz martwić się o wdrożenie oprogramowania czy samodzielne analizowanie raportów — wszystko zrobimy za Ciebie. Po zakończeniu okresu audytu otrzymasz sprawozdanie oraz podsumowanie, dzięki któremu dostaniesz wszystkie najpotrzebniejsze informacje, wnioski i zalecenia, które od razu pozwolą Ci podjąć kroki w celu poprawienia bezpieczeństwa firmy i produktywności Twoich pracowników.

Szkolenia produktowe

Efektywne korzystanie z wszystkich możliwości zakupionego produktu jest możliwe tylko wtedy, gdy osoby z niego korzystające dysponują odpowiednią wiedzą. Securivy oferuje szkolenia, które pozwolą na sprawne posługiwanie się dostępnymi narzędziami.

Nasi eksperci są gotowi przeprowadzić przez wdrożony produkt użytkowników o każdym poziomie zaawansowania. Szkolenia odbywają się we wcześniej uzgodnionej formie.

Szkolenia z bezpieczeństwa IT

Warsztaty zawierają szereg praktycznych porad dotyczących poprawy cyberbezpieczeństwa firmy. Z naszych wykładów dowiesz się jak:
- dokonać audytu bezpieczeństwa
- przeprowadzić analizę ryzyka i zagrożeń
- tworzyć polityki i strategie bezpieczeństwa
- wdrożyć najlepsze praktyki dotyczące bezpieczeństwa
- reagować w przypadkach ataków

Szkolenie podzielone jest na poziomy zaawansowania, dzięki czemu oferta dopasowana jest do tych, którzy dopiero stawiają pierwsze kroki w bezpieczeństwie IT, jak również do ekspertów, którzy chcą poznać narzędzia i działania podnoszące cyberbezpieczeństwo firmy na wyższy poziom.

Usługi

Testy penetracyjne

Testy penetracyjne to wykorzystanie luk w zabezpieczeniach oraz próba ich przełamania w kontrolowanych i bezpiecznych warunkach, w celu oceny faktycznego, aktualnego stanu bezpieczeństwa infrastruktury IT. Przeprowadzenie testu penetracyjnego pozwoli określić Ci, jakie są słabe punkty systemu oraz uszeregować metody naprawy, a więc umożliwi prewencję ataków oraz wszelkich cyberzagrożeń.

Jeśli jesteś właścicielem strony internetowej, sklepu internetowego lub aplikacji webowej, testy penetracyjne są kluczowym narzędziem, aby odpowiednio zabezpieczyć infrastrukturę witryny. Pentesty to nie tylko weryfikacja zabezpieczeń, szacowanie ryzyka, ale też uświadamianie i edukacja administratorów stron o możliwych zagrożeniach i atakach.

Usługa jest więc skierowana do osób odpowiedzialnych za witryny internetowe, chcących dbać o ich bezpieczeństwo, a także podążać za stale rozwijającymi się „trendami" cyberataków, by móc ich uniknąć.

Darmowe konsultacje

Wielu przedsiębiorców ma problem, aby znaleźć narzędzie odpowiednie dla prowadzonej działalności gospodarczej. Prawidłowy dobór rozwiązań wymaga wiedzy i doświadczenia. Zadbanie o cyberbezpieczeństwo jest możliwe dzięki zastosowaniu podejścia procesowego, które pozwala stale podnosić poziom zabezpieczeń. Securivy zajmuje się kompleksowym doradztwem w zakresie wyboru i wdrażania narzędzi, które podnoszą poziom bezpieczeństwa w firmie. Darmowe konsultacje to wyjście naprzeciw potrzebom organizacji, które chciałyby zadbać o ochronę przed zagrożeniami, ale nie wiedzą od czego zacząć.

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