STORMSHIELD

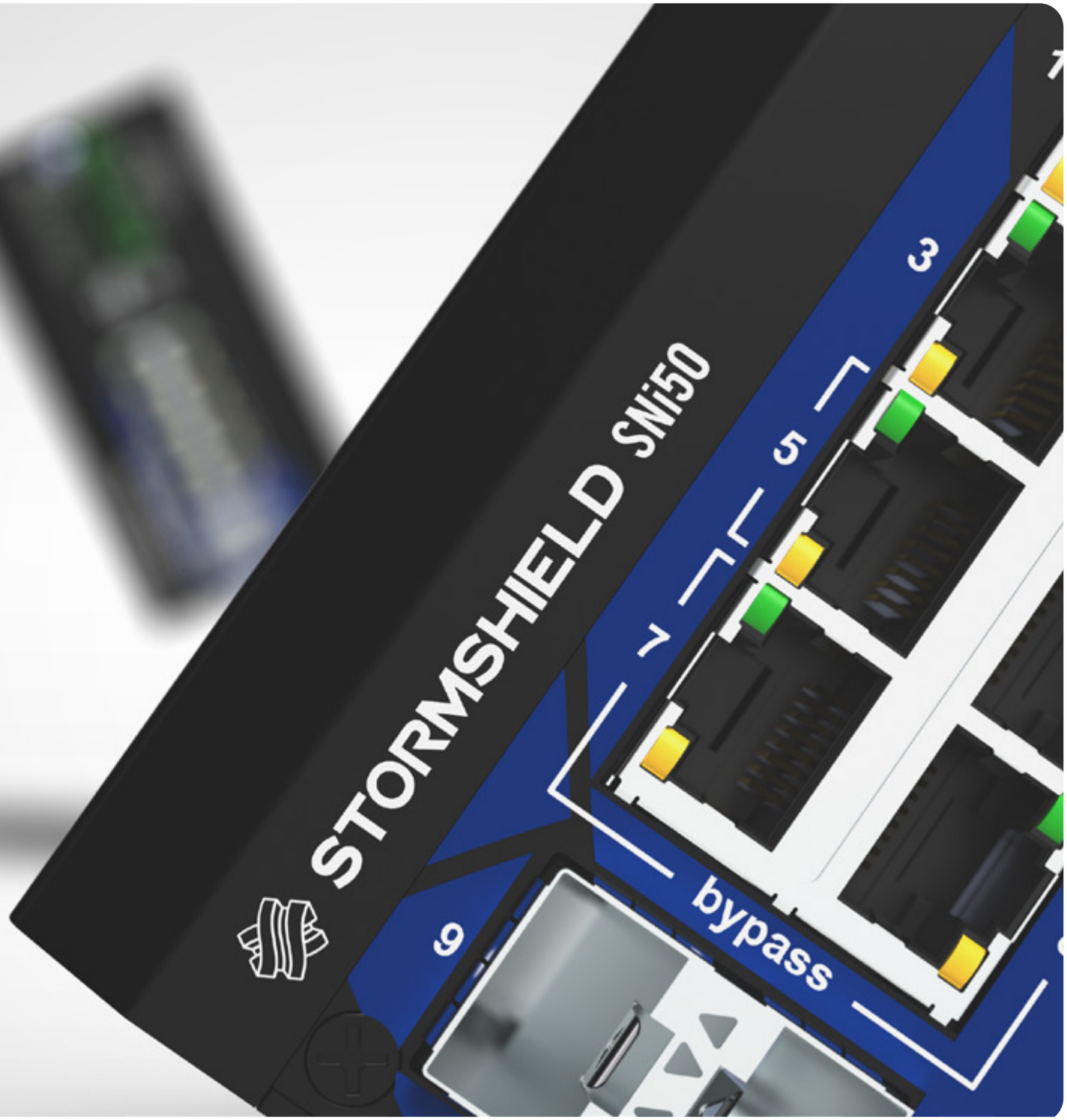
SNi50

Ochrona przemysłowa

Do 20 Gbps
PRZEPUSTOWOŚĆ FIREWALL

MTBF 108 lat
WYSOKA NIEZAWODNOŚĆ

Norma IEC 62443
UŁATWIA INTEGRACJE



NETWORK SECURITY

FIREWALL KLASY PRZEMYSŁOWEJ

Transparentna izolacja stref

Możliwości integracji sieciowej zapewniają optymalną separację pomiędzy różnymi strefami operacyjnymi przy minimalnym wpływie na istniejącą infrastrukturę. Dzięki certyfikacji IEC 62443*, SNi50 zapewnia bezproblemową integrację systemu operacyjnego z platformami innych dostawców.

Niezawodność

SNi50 jest zaprojektowany aby spełnić wszystkie wymagania Twojej sieci przemysłowej.Wyjątkowo wysoka niezawodność urządzenia (MTBF wynoszący 108 lat) oraz zintegrowany, rozszerzony tryb bezpieczeństwa gwarantują optymalną dostępność i bezpieczeństwo systemu ochrony.

Ochrona rozległych sieci operacyjnych

Połączenie mechanizmów kontroli dostępu dla poszczególnych stref z zaawansowaną analizą przemysłowych przepływów komunikacyjnych (Deep Packet Inspection) zapewnia kompleksową ochronę rozległej infrastruktury. Tryb bezpieczeństwa SNi50 gwarantuje nieprzerwaną realizację procesów operacyjnych.

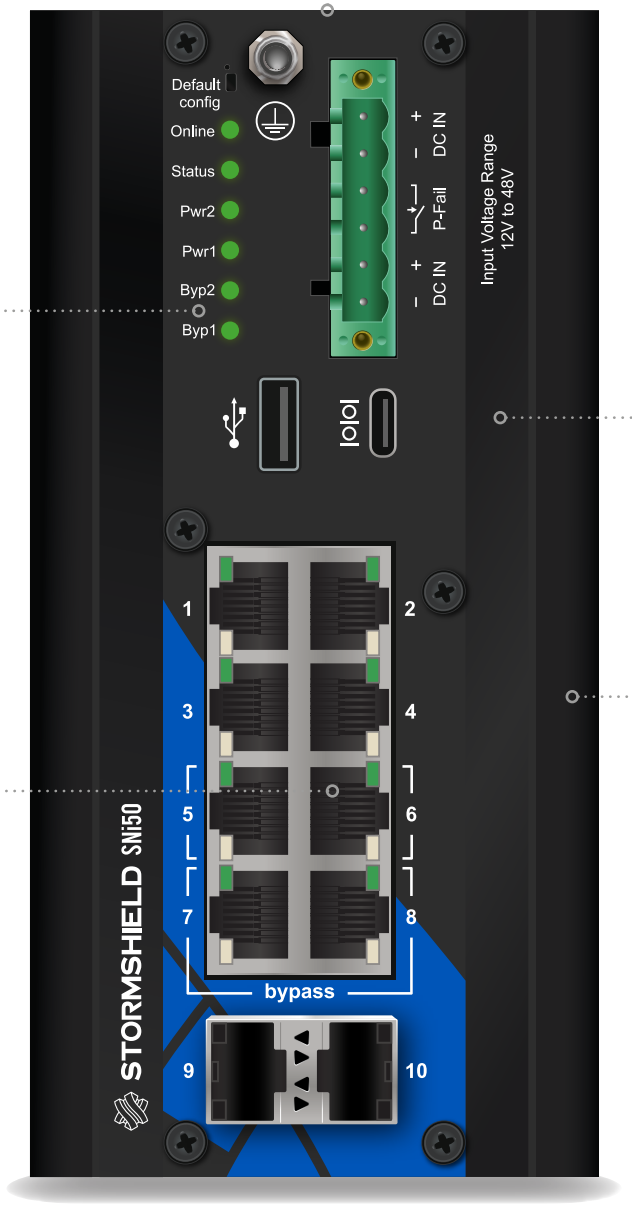
DLA EUROPEJSKIEGO CYBERBEZPIECZEŃSTWA

Wybierając Stormshield, zyskujesz realną niezależność strategiczną oraz spokój w dynamicznym i wymagającym otoczeniu geopolitycznym. Opracowane w całości we Francji oprogramowanie sprzętowe uzyskało certyfikaty wiodących europejskich instytucji ds. cyberbezpieczeństwa, takich jak ANSSI (Francja) i CCN (Hiszpania), a także Standard Qualification.

** Development processes are IEC62443-4-1 certified*

Redundantny
zasilacz przemysłowy

Safety mode
(para interfejsów bypass)



Ponad 10 zabezpieczonych
protokołów przemysłowych

Szyna DIN
Łatwy montaż
w szafach

Wzmocniona obudowa
dla wymagających środowisk

KLUCZOWE DANE

Przemysłowy
SNi50

Łączność
10
interfejsów (8 miedzianych 2,5G + 2 SFP+)

Bypass
2 pary

Wydajność
20 Gbps
Firewall

VPN
5,7 Gbps
przepustowość IPsec

Wydajność
15 Gbps
IPS

VPN
750
tunele IPsec

FUNKCJE

Dokument nie jest umową. Wymienione funkcje są dostępne w wersji 5.x.

Segmentacja sieci

Różne tryby wdrożenia służące do podziału Twojego systemu operacyjnego (router, transparentny i hybrydowy) należą do najbardziej elastycznych na rynku. Zapewniają **bezproblemową integrację zapory sieciowej z istniejącą architekturą sieci.**

Bezpieczna administracja

Narzędzie do zdalnego połączenia (klient VPN) wspiera administratorów w uzyskiwaniu **kontrolowanego i bezpiecznego dostępu do systemów wymagających utrzymania**. Zgodnie z wymaganiami wdrożeniowymi dla środowisk operacyjnych masz możliwość wdrożenia jednostek dostępowych w swojej infrastrukturze.

Zapewnianie bezpieczeństwa operacyjnego

Moduł IPS zwiększa kontrolę dostępu do obszarów infrastruktury sieciowej, umożliwiając **bardziej bezpieczne działania powiązane z procesami operacyjnymi**. Dogłębna analiza protokołów (Deep Packet Inspection) sprawdza prawidłowe użycie poleceń, a tryb "safty mode" zapewnia ciągłość działania Twoich procesów.

... oraz unikalne oprogramowanie

Stormshield oferuje unikalny, przyjazny interfejs do zarządzania swoim asortymentem produktów. To pozwala **obniżyć koszta operacyjne i uprościć zarządzanie zespołem oraz ułatwić konwergencję IT/OT**, oszczędzając organizacji znaczną ilość czasu.

Więcej funkcjonalności

Kontrola użytkowania

Tryb Firewall/IPS/IDS • Reguły firewall w zależności od użytkownika • Wykrywanie i zarządzanie aplikacjami • Filtrowanie Microsoft Services • Przemysłowy Firewall/IPS/IDS • Kontrola aplikacji przemysłowych • Wykrywanie i kontrolowanie korzystania z terminali mobilnych • Geolokalizacja (kraje, kontynenty) • Dynamiczna reputacja hosta • URL Filtering • Transparentne uwierzytelnianie (Active Directory, SSO Agent, SSL) • Uwierzytelniania VDI wielu użytkowników za pomocą dedykowanego agenta (Citrix, TSE) • Uwierzytelnianie w trybie gościa i polecenia • Usługi internetowe • Sprawdzanie hosta • Zero Trust Network Access (ZTNA)

Ochrona przed zagrożeniami

Wykrywanie i zapobieganie włamaniom (IPS) • Wykrywanie protokołów oraz sprawdzanie ich zgodności • Inspekcja aplikacji • Ochrona przed atakami DoS • Ochrona przed SQL injections • Ochrona przed Cross-Site Scripting (XSS) • Ochrona przed złośliwym kodem Web2.0 oraz skryptami • Wykrywanie trojanów • Wykrywanie połączeń interaktywanych (botnet, Command & Control) • Ochrona przed data evasion • Zaawansowane zarządzanie fragmentacją • Automatyczna reagowanie na ataki (powiadomienia, kwarantanna, blokada, QoS, zrzut ruchu) • Antyspam i antyphishing: analiza reputacji, silnik heurystyczny • Wbudowany antywirus (HTTP, SMTP, POP3, FTP) • Analiza i inspekcja ruchu szyfrowanego (SSL) • Ochrona VoIP (SIP) • Współpraca bezpieczeństwa: reputacja IP, Sanboxing oparty na chmurze na terenie Europy (opcja)

Poufność

Tunele IPSec VPN Site-to-site lub client-to-site • Odporność postkwantowa • Dostęp zdalny za pomocą SSL VPN dla wielu systemów (Windows, Android, iOS, itd.) • Agent SSL VPN z automatyczną opcja konfiguracji (Windows) • Wsparcie IPSec VPN dla Android/iPhone

Sieciowa - integracja

IPv6 • NAT, PAT, tryb transparentny (bridge)/routera/hybrydowy • Dynamiczny routing (RIP - OSPF - BGP) • Multicast • Zarządzanie wieloma łączami (równoważenie, failover) • Wielopoziomowe wewnętrzne lub zewnętrzne PKI • Uwierzytelnianie wielu domen (w tym wewnętrzny LDAP) • Routing oparty na regułach (PBR) • Zarządzenia QoS • Serwer/klient/relay DHCP • Klient NTP • DNS proxy-cache • HTTP proxy • Agregacja linków (LACP, tryb Broadcast oraz redundancja) • Spanning-tree management (RSTP/MSTP) • SD-WAN • Wieloskładnikowe uwierzytelniania (MFA)

Zarządzanie

Zarządzanie stronami Web • Interfejs webowy z anonimizacja logów (zgodność z RODO) • Obiektowe zarządzanie politykami • Kontekstowe reguły bezpieczeństwa • Analizator poprawności reguł • Licznik użycia reguł • Aktualizacje zabezpieczeń online lub offline • Globalna/Lokalna polityka bezpieczeństwa • Wbudowane narzędzia do raportowania i analizy logów • Interaktywne i konfigurowalne raporty • Wsparcie dla wielu serwerów syslog UDP/TCP/TLS • Agent SNMP v1, v2, v3 • IPFIX • Automatycznie konfigurowana kopia zapasowa • Open API • Nagrywanie skryptów • Klaster wysokiej dostępności (HA)

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ[1]	SNi50
Przepustowość firewalla (UDP 1518 bajtów)	**20 Gbps**
Przepustowość firewalla (IMIX)	**9,1 Gbps**
Przepustowość IPS (UDP 1518 bajtów)	**15 Gbps**
Przepustowość IPS (IMIX)	**4 Gbps**
Ochrona przed zagrożeniami*	**1,3 Gbps**
Opóźnienie (średnie, µs przy 80% obciążenia)	**83 µs**

** Pomiar ochrony przed zagrożeniami obejmuje firewall, IPS, antywirus, reputację IP oraz bezpieczeństwo aplikacji webowych, w realistycznych warunkach ruchu i z włączonym logowaniem.*

VPN	SNi50
Przepustowość IPsec – AES-GCM256 (1408 bajtów)	**5,7 Gbps**
IPSec - AES-GCM256 (IMIX)	**2,7 Gbps**
Maksymalna liczba tuneli IPsec VPN (1024 kb/s na tunel)	**750**
Liczba klientów SSL VPN	**500**

ŁĄCZNOŚĆ SIECIOWA	SNi50
Maksymalna liczba jednoczesnych sesji	**600 000**
Liczba nowych sesji na sekundę	**80 000**

INTERFEJSY	SNi50
2,5Gb Interfejsy miedziane	**8**
10Gb SFP+	**2**
Pary bypass (na portach miedzianych)	**2**

REDUNDANCJA	SNi50
Wysoka dostępność / Bypass (safety mode)	**Tak**

PROTOKOŁY - DEEP PACKET INSPECTION (DPI)	SNi50
Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV), S7+ & IT	

SPRZĘT	SNi50
Pamięć	**85 GB**
TPM chip	**Tak**
MTBF przy 25°C (lata)	**108,5**
Montaż	**Szyna DIN UTA 159 (35 mm, IEC/EN 60715:2017)**
Wysokość x szerokość x głębokość (mm)	**160 x 78 x 127**
Waga	**2,23 kg (4,92 lb)**
Podwójne zasilanie (DC)	**2 x 12-48 VDC 6A-1,5A**
Pobór mocy (w spoczynku/ średni / maks. w W)	**20 / 29 / 31**
Odprowadzanie ciepła (maks., BTU/h)	**68 / 99 / 106**
Poziom hałasu	**Bez wentylatorów (fanless)**
Stopień ochrony (IP)	**IP40**
Środowisko pracy	Temperatura: **-40° do +70°C (-40° do +167°F)** Wilgotność: **0% to 95%**
Środowisko przechowywania	Temperatura: **-40° do +85°C (-40° do +185°F)** Wilgotność: **5% to 95%**

CERTYFIKATY	SNi50
CE/UKCA/FCC/ICES-003/RCM/CB, EN 61000-6-2, EN 61000-6-4, IEC 61000-4-18, IEC 60068-2, IEC 61850-3, IEEE 1613, EN 50121-1, EN 50121-4, IEC 60529	

1 Wydajność mierzona w środowisku laboratoryjnym w idealnych warunkach dla wersji 5.x. Wyniki mogą się różnić w zależności od warunków testowych i wersji oprogramowania.

PAKIETY LICENCYJNE

INDUSTRIAL SECURITY PACK

Firmy poszukujące ochrony dla swojej infrastruktury przemysłowej mogą wybrać ten pakiet. Jest on dostosowany do **precyzyjnego filtrowania i zarządzania dostępem do sieci operacyjnej, przy jednoczesnym zapewnieniu dogłębnej inspekcji protokołów przemysłowych**. Funkcja połączenia VPN (zarówno IPsec, jak i SSL) zapewnia bezpieczny punkt dostępu do zdalnych operacji serwisowych.

PREMIUM SECURITY PACK

Pakiet ten jest przeznaczony dla przedsiębiorstw o rygorystycznych wymaganiach bezpieczeństwa, **oferując najlepsze technologie do zwalczania nawet najbardziej zaawansowanych ataków. Zaawansowany system antymalware z technologią emulacji oraz filtrowanie URL w trybie chmurowym, oparte na ponad 70 kategoriach (Extended Web Control)**, podnoszą poziom ochrony do poziomu nieosiągalnego dla konkurencji.

	Industrial Security Pack	Premium Security Pack
Next-Generation Firewall		
Firewall warstwy 7	✓	✓
Geolokalizacja	✓	✓
Usługi internetowe	✓	✓
Uwierzytelnienie użytkowników, MFA oraz SSO	✓	✓
SD-WAN i ZTNA		
IPsec VPN	✓	✓
Szyfrowanie postkwantowe	✓	✓
SSL VPN	✓	✓
Ocena bezpieczeństwa urządzenia	✓	✓
Ochrona przed zagrożeniami		
IPS/IDS	✓	✓
Zaufane certyfikaty publiczne	✓	✓
Antyspam	Opcja	✓
Threat intelligence (IP i domeny)	✓	✓
Ochrona protokołów przemysłowych	✓	✓
Antywirus	Opcja	✓
Breach Fighter (Sandboxing wykorzystujący AI)	Opcja	✓
Chmurowa baza URL (Filtrowanie URL)	Opcja	✓
Serwisy		
Aktualizacja oprogramowania	✓	✓
Wymiana w razie awarii	✓	✓
Standardowe wsparcie techniczne	✓	✓
Automatyczna kopia konfiguracji	✓	✓
Dostęp do wsparcia technicznego 24x7	Opcja	Opcja
Ekspresowa wymiana	Opcja	Opcja
Bezpieczny zwrot	Opcja	Opcja

WYMIANA SPRZĘTU

Wszystkie pakiety bezpieczeństwa obejmują wymianę sprzętu, aby zapewnić ciągłość działania w przypadku awarii. Urządzenie zostanie po prostu wymienione na podobny produkt. Dostępne są trzy poziomy tej usługi.

Standardowa wymiana
Twoje urządzenie zostanie wymienione po otrzymaniu przez nasze centrum obsługi klienta we Francji wadliwego urządzenia.

Ekspresowa wymiana
Twoje urządzenie zostanie wymienione z wyprzedzeniem. Gdy tylko nasze wsparcie zdiagnozuje awarie sprzętu, wyślemy produkt zastępczy, który otrzymasz następnego dnia roboczego[1].

Spokój dla wszystkich
W ramach tej usługi możesz samodzielnie wymienić sprzęt po zdiagnozowaniu przez nasze wsparcie techniczne usterki [2].

[1] Skontaktuj się z nami w sprawie kwalifikujących się krajów i miast. Dotyczy diagnozy postawionej przed godziną 13:00.

[2] Aby skorzystać z tej usługi należy wcześniej nabyć produkty zamienne.

DLA OPTYMALNEJ OCHRONY

Stormshield oferuje opcje, które pokryją Twoje dodatkowe potrzeby w zakresie cyberbezpieczeństwa.

Neutralizuj najbardziej zaawansowane zagrożenia dzięki Stormshield Network Advanced Antivirus.

Korzystaj z zaawansowanego i niezawodnego rozwiązania filtrującego dzięki Stormshield Extended Web Control.

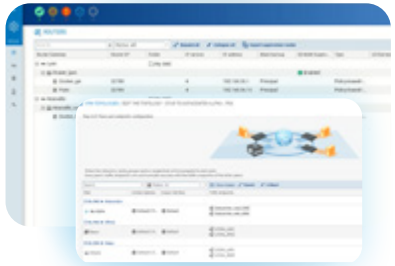
Rozszerz swoje biuro domowe dzięki wysoce bezpiecznemu zdalnemu dostępowi z klientem Stormshield VPN.

ZARZĄDZAJ BEZPIECZEŃSTWEM ZA POMOCĄ SKUTECZNYCH NARZĘDZI

Narzędzie podejmujące decyzje

ze Stormshield Log Supervisor

Optymalizuj swoje działania związane z analizą i reakcją na incydenty. Dzięki szybkiemu podglądowi efektywności systemu zyskujesz pewność, że Twoje inwestycje w bezpieczeństwo są uzasadnione.



Zarządzanie dużymi infrastrukturami

ze Stormshield Management Center

Stormshield Management Center wymienia konfigurację zapór SNS i dane monitorujące w czasie rzeczywistym, jednocześnie zapewniając ich poufność i integralność. Jego intuicyjny interfejs graficzny minimalizuje błędy konfiguracji, a jego globalne zarządzanie zasadami bezpieczeństwa i filtrowania eliminuje powtarzające się zadania.

EUROPEJSKI WYBÓR
W CYBERBEZPIECZEŃSTWIE

www.stormshield.pl