Infradata

DIMsystem

Budujemy bezpieczną przyszłość

Infradata
DIMsystem

Grupa Infradata to międzynarodowy, niezależny dostawca nowoczesnych systemów cyberbezpieczeństwa, sieci krytycznych dla biznesu, rozwiązań chmurowych i usług zarządzanych. Wspieramy naszych klientów we wdrażaniu innowacji, dostarczając im najlepszych w swojej klasie technologii. W Infradata budujemy fundamenty pod bezpieczeństwo i rozwój gospodarki cyfrowej i społeczeństwa cyfrowego.

Łącząc technologie, procesy i fachową wiedzę tworzymy rozwiązania i usługi następnej generacji. Przez naszych klientów jesteśmy cenieni za wysokiej jakości usługi i doskonałość operacyjną. Nasi partnerzy strategiczni należą do wiodących dostawców technologii na świecie. Dzięki temu nasi klienci mają dostęp do najbardziej zaawansowanych rozwiązań sprzętowych i programowych dostępnych na rynku, które pomagają im poprawiać bezpieczeństwo i niezawodność sieci.

Legitymujemy się najwyższym statusem partnerskim u producentów większości oferowanych systemów. Nasi inżynierowie mogą pochwalić się nie tylko najwyższymi certyfikatami producenckimi, ale także szerokim doświadczeniem w zakresie tworzenia kompleksowych architektur.

Wspieramy również naszych klientów w zakresie zarządzania ich infrastrukturą sieciową i cyberbezpieczeństwa realizując usługi typu SOC i NOC.

GRUPA INFRADATA W LICZBACH

Wielokrotnie nagradzana firma
Nagrody branżowe i akredytacje

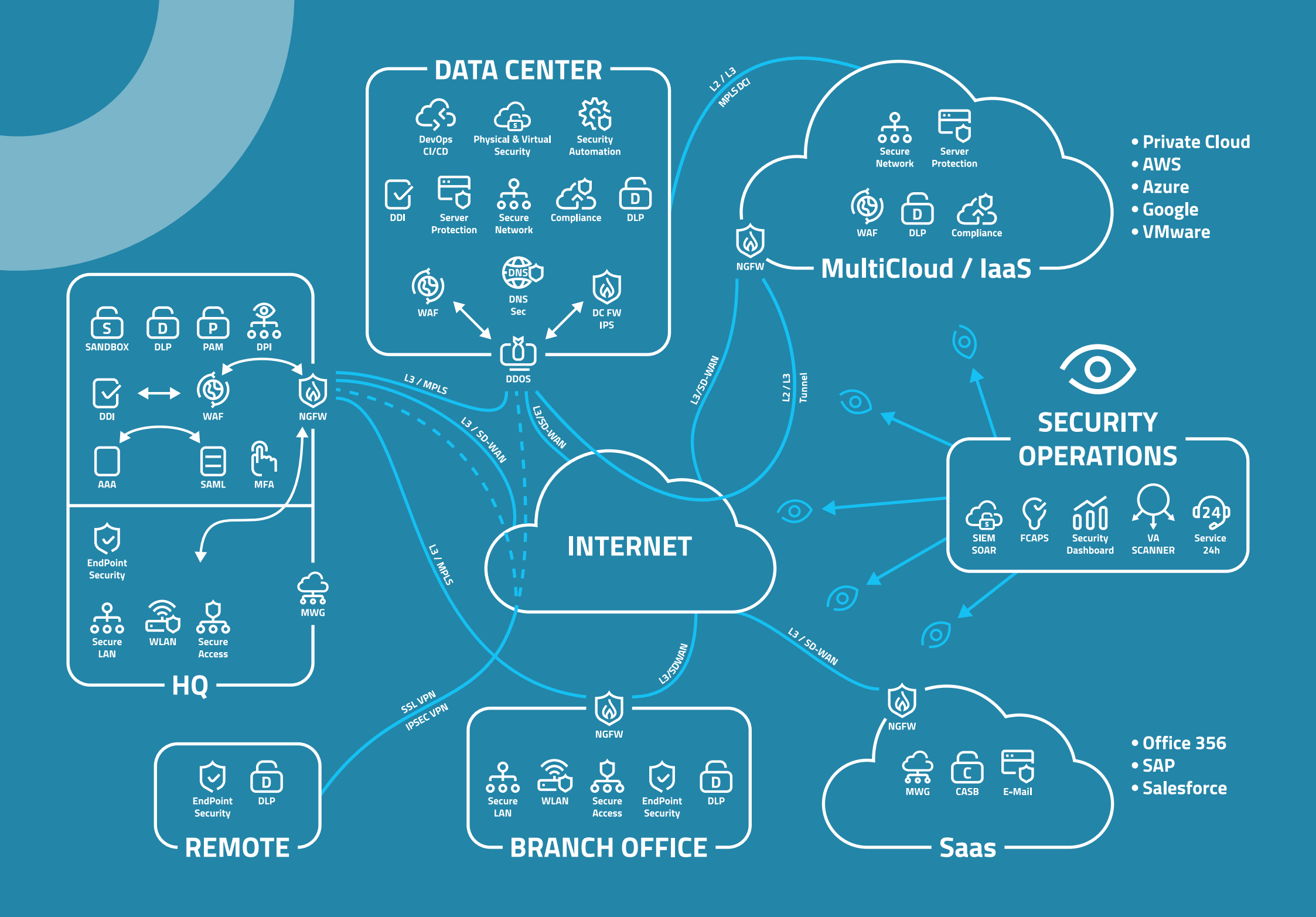
170+ certyfikowanych i doświadczonych inżynierów
Nasi specjaliści robią wielką różnicę

24/7 obsługa klienta na całym świecie
Wskaźnik satysfakcji klienta na poziomie 8,9

Doświadczenie, któremu możesz zaufać
Od 2004 roku wspieramy naszych klientów we wdrażaniu najbardziej zaawansowanych rozwiązań IT

11 biur w 7 krajach
Obsługujemy klientów w ponad 50 krajach na świecie

50+ Partnerów technologicznych
Strategiczne partnerstwa z czołowymi producentami


DATA CENTER
DevOps CI/CD
Physical & Virtual Security
Security Automation
DDI
Server Protection
Secure Network
Compliance
DLP
WAF
DNS Sec
DC FW IPS
DDOS
L2 / L3 MPLS DCI
NGFW
MultiCloud / IaaS
Secure Network
Server Protection
WAF
DLP
Compliance
• Private Cloud
• AWS
• Azure
• Google
• VMware
SANDBOX
DLP
PAM
DPI
DDI
WAF
NGFW
AAA
SAML
MFA
EndPoint Security
Secure LAN
WLAN
Secure Access
MWG
HQ
L3 / MPLS
L3 / SD-WAN
L3/SD-WAN
L3/SD-WAN
L2 / L3 Tunnel
INTERNET
SECURITY OPERATIONS
SIEM SOAR
FCAPS
Security Dashboard
VA SCANNER
Service 24h
L3 / MPLS
L3/SDWAN
L3 / SD-WAN
SSL VPN
IPSEC VPN
NGFW
Secure LAN
WLAN
Secure Access
EndPoint Security
DLP
BRANCH OFFICE
NGFW
MWG
CASB
E-Mail
Saas
• Office 356
• SAP
• Salesforce
EndPoint Security
DLP
REMOTE

Juniper Networks

Nowoczesne rozwiązania sieciowe

Produkty firmy Juniper Networks adresują potrzeby klientów z zakresu budowy nowoczesnej infrastruktury sieciowej, zarówno przedsiębiorstw, jak i operatorów telekomunikacyjnych oraz dostawców usług. Szeroka rodzina przełączników serii EX i QFX pozwala na dobór optymalnych rozwiązań, od poziomu sieci oddziałowej, przez kampus, aż do Centrum Przetwarzania Danych (CPD). W przypadku CPD, rozwiązania typu fabric wspierane technologią EVPN/VXLAN, zapewniają sieć podkładową dla wirtualizacji i automatyzacji. W obszarze sieci oddziałowej i kampusowej uzupełnieniem jest rozwiązanie WiFi MIST.

Juniper Networks zapewnia również produkty do budowy nowoczesnych sieci międzyoddziałowych, tzw. Software Defined WAN (Contrail SD-WAN). Pozwalają one na łatwe i elastyczne łączenie oddziałów firm, z wykorzystaniem różnych dostępnych łączy (Internet, MPLS VPN, itp.) przy zachowaniu jakości i bezpieczeństwa.

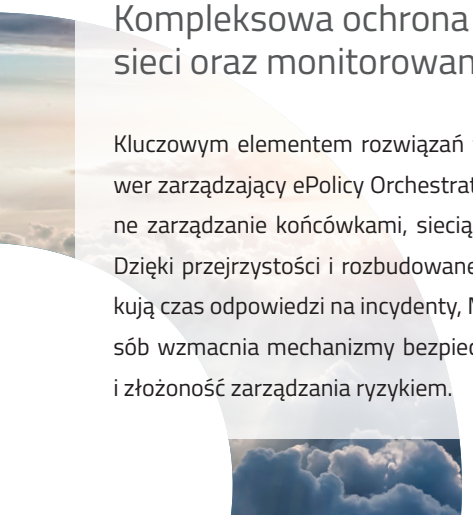
Firma Juniper Networks jest również liderem w obszarze rutingu, z uznawanymi przez wielu klientów i specjalistów za najlepsze w klasie routerami serii MX, (zastosowanie: styk BGP, WAN/MPLS/VXLAN/EVPN/SD-WAN, CGNAT), oraz oddziałowymi ruterami z serii SRX.

W zakresie bezpieczeństwa, firma oferuje kompleksowe rozwiązania do ochrony ruchu na styku sieci firmowych i Internetu oraz w CPD. Platformy z rodziny SRX to systemy klasy NG Firewall, cenione za ich wysoką wydajność i szerokość zastosowań. Całości dopełniają rozwiązania Sky ATP(sandbox chmurowy) i JATP (sandbox lokalny). Juniper Networks posiada również ciekawą ofertę dotyczącą sieci SDN (Contrail Networking/Enterprise Multicloud) dla Data Center.

McAfee

Kompleksowa ochrona stacji, serwerów, sieci oraz monitorowanie bezpieczeństwa

Kluczowym elementem rozwiązań firmy Intel Security jest serwer zarządzający ePolicy Orchestrator (ePO), zapewniający spójne zarządzanie końcówkami, siecią i bezpieczeństwem danych. Dzięki przejrzystości i rozbudowanej automatyzacji, które redukują czas odpowiedzi na incydenty, McAfee ePO w znaczący sposób wzmacnia mechanizmy bezpieczeństwa oraz obniża koszty i złożoność zarządzania ryzykiem.



Firma McAfee udostępnia bardzo szerokie portfolio rozwiązań bezpieczeństwa, w związku z czym – dla łatwiejszego ich przedstawienia – dobrze jest je pogrupować ze względu na obszar zastosowania oraz funkcjonalność.

Produkty wchodzące w skład McAfee Data Protection chronią krytyczne dane i pomagają zapewnić zgodność z regulacjami. W ich skład wchodzą między innymi systemy szyfrujące oraz zapobiegające wyciekom danych (DLP), zapewniające wielowarstwowe bezpieczeństwo danych bez względu na to, gdzie się znajdują – w zasobach lokalnych, czy sieciowych.

McAfee Web Security integruje w sobie zabezpieczenia przed złośliwym oprogramowaniem, kontrolę treści oraz serwisy reputacyjne, chroniąc użytkowników, aplikacje, dane i sieci przed wszystkimi formami zagrożeń przenoszonych poprzez pocztę elektroniczną i Internet.

Systemy wchodzące w skład McAfee Endpoint Security oferują ciągłe, zaktualizowane i silne zabezpieczenia przeciwko całemu spektrum zagrożeń. McAfee dostarcza ochronę dla wszystkich końcówek, w tym dla urządzeń mobilnych i środowisk wirtualnych, gwarantując bezpieczny, bezproblemowy dostęp do aplikacji biznesowych i danych korporacyjnych.

Rodzina rozwiązań McAfee Network Security zawiera m.in. zaawansowaną analizę bahawioralną oraz silniki detekcji zagrożeń sieciowych (IPS). Wykorzystywane w nich mechanizmy Network Security Framework oferują maksymalną dostępność, bezpieczeństwo, integralność, elastyczność, łatwość zarządzania w połączeniu z minimalnymi narzutami wydajnościowymi i ryzykiem. Rozwiązanie to można także zintegrować z systemem klasy sandbox, zapewniającym analizę oraz wykrywanie nieznanych zagrożeń w danych przesyłanych siecią.

Rozwiązania klasy SIEM (Security Information and Event Management) pozwalają łączyć logi dotyczące zdarzeń, zagrożeń i ryzyka oferując błyskawiczne reakcje na incydenty, bezproblemowe zarządzanie logami i zaawansowane mechanizmy raportowania. Umożliwiają konsolidowanie, korelowanie, ocenę i priorytetyzację zdarzeń dotyczących bezpieczeństwa pochodzących zarówno z systemów McAfee, jak i produktów firm trzecich.

Firma McAfee wychodząc naprzeciw potrzebom zapewnienia bezpieczeństwo, działającym systemom w oparciu o platformy chmurowe. Udostępnia także stale rozszerzany katalog rozwiązań dostosowanych do specyfiki takich środowisk. Systemy te chronią przed zaawansowanymi zagrożeniami, wyciekiem danych oraz pozwalają na monitorowanie wykorzystywania aplikacji chmurowych przez użytkowników.

Istotnym elementem ekosystemu bezpieczeństwa McAfee jest także szyna danych (Data Exchange Layer/DXL) zapewniająca wymianę informacji pomiędzy poszczególnymi komponentami ochrony firmy McAfee oraz – co szczególnie istotne – także innych producentów.

IBM

Monitorowanie i zarządzanie bezpieczeństwem

IBM QRadar SIEM stanowi kompleksowe rozwiązanie do analizy bezpieczeństwa informatycznego, zapewniające integrację z różnorodnymi źródłami zdarzeń i przepływów sieciowych oraz możliwość automatyzacji procesów obsługi incydentów. IBM QRadar SIEM pozwala widzieć to, co dzieje się w sieci, w centrum przetwarzania danych i w środowisku aplikacyjnym, a dzięki temu też lepiej chronić zasoby informatyczne i spełniać wymogi formalno-prawne.

Rapid7

Zarządzanie podatnościami

Zarządzanie podatnościami (ang. Vulnerability Management) jest kluczowym elementem systemu bezpieczeństwa każdej firmy, której działalność biznesowa jest wspomagana przez systemy informatyczne. W infrastrukturze IT, w której brakuje dobrej jakości narzędzi do identyfikacji podatności, szybko dochodzi do naruszeń bezpieczeństwa, a komputery i inne urządzenia dostają się w ręce przestępców.

Rapid7 Nexpose/InsightVM zapewnia identyfikację podatności oraz ocenę implikowanego przez nie ryzyka dla wszystkich elementów systemu informatycznego firmy. Dostępne w Nexpose rozbudowane narzędzia raportowania pozwalają na prezentowanie informacji w sposób zrozumiały dla osób decyzyjnych oraz sprawne planowanie działań naprawczych.

Rapid7 AppSpider/InsighAppSec wykrywa podatności aplikacji internetowych (web), ułatwiając szybkie minimalizowanie ryzyka związanego z wypływem danych lub niedostępnością serwisów biznesowych. Opcjonalnie system ten można zintegrować z rozwiązaniami klasy WAF (Web Application Firewall), uniemożliwiając wykorzystanie podatności do czasu wprowadzenia stosownych poprawek.

Fudo Security

Monitorowanie, rejestracja, kontrola i audyt zdalnych sesji administracyjnych

Sztandarowym produktem firmy Fudo Security jest rozwiązanie FUDO, dedykowane do monitoringu, kontroli, rejestracji i audytu zdalnych sesji administracyjnych. Pozwala ono podsłuchiwać i nagrywać sesje SSH, RDP, VNC, umożliwiając analizę zarówno sesji archiwalnych, jak i obecnie trwających, a także zakończenie, wstrzymanie lub włączenie się w prace zdalnych konsultantów czy pracowników.

ProofPoint

Ochrona poczty elektronicznej

Rozwiązania dostępne w ramach platformy ProofPoint Enterprise Protection Suite, takie jak Targeted Attack Protection zapewniają kompleksową ochronę przed zagrożeniami poczty elektronicznej, włączając w to ochronę przed złośliwym oprogramowaniem (malware), wyłudzaniem informacji (phishing) oraz innymi formami niepożądanych lub niebezpiecznych treści.

Dodatkowo w ramach ProofPoint Enterprise Privacy Suite dostępne są funkcjonalności zapewniające ochronę informacji wrażliwych oraz prywatnych, zapobiegające wyciekom informacji poufnych wysyłanych z wykorzystaniem poczty elektronicznej (DLP) oraz zapewniające zgodność z powszechnie stosowanymi międzynarodowymi i branżowymi regulacjami w zakresie ochrony danych. Całość dopełnia moduł ProofPoint Encryption, automatycznie szyfrujący wskazane polityką wiadomości email, zmniejszając ryzyko powiązane z naruszeniami przepisów, utratą danych i złamaniem polityki korporacyjnej. Wiadomości mogą być szyfrowane z wykorzystaniem technologii S/MIME, PGP lub mogą być publikowane w bezpiecznym portalu, zapewniającym szyfrowany dostęp do informacji.

F5 Networks

Programowalne rozwiązania bezpieczeństwa oraz wysokiej dostępności dla aplikacji

F5 Networks jest liderem rynku w klasie rozwiązań ADC (Application Delivery Controller). Produkty F5 zapewniają mechanizmy inteligentnego kierowania ruchem danych w sieci, lokalnie (LTM),

oraz pomiędzy rozproszonymi Centrami Przetwarzania Danych (GSLB). Zapewniają również ochronę, zarówno w warstwie sieciowej (AFM), jak i aplikacyjnej (AWAF), oraz mechanizmy kontroli dostępu (APM). Dodatkowo, dzięki zastosowanemu wsparciu sprzętowemu, pozwalają na wysokowydajną inspekcję ruchu szyfrowanego (SSL Orchestrator, TLS/SSL Offload) oraz łagodzenie skutków ataków DDoS, zarówno wolumetrycznych (AFM), jak i aplikacyjnych (ASM).

O wyjątkowej elastyczności platformy decydują ogromne możliwości programowania i wręcz dowolnej modyfikacji ruchu przechodzącego przez urządzenia. Programowalność dotyczy zarówno warstwy danych, jak i warstwy kontrolnej. Dzięki temu F5 staje się wyjątkową platformą dla tworzenia własnych, dostosowanych do potrzeb, mechanizmów optymalizacji i automatyzacji usług aplikacyjnych (BIG-IQ, AS3, iRule).

InfoBlox

Ochrona ruchu DNS oraz zarządzanie siecią

Infoblox jest jednym z liderów w technologiach zarządzania DNS, DHCP i adresami IP (IPAM) oraz Secure DNS. Infoblox zapewnia blokowanie wycieków danych w zapytaniach DNS oraz komunikacji Command&Control over DNS oraz blokuje zapytania dotyczące domen powiązane z malware i ransomware. Umożliwia integrację z innymi narzędziami bezpieczeństwa (np. NAC, NGFW, End-Point Protection, skanery podatności), zapewniając ochronę publicznych serwerów DNS przed atakami DDoS, próbami amplifikacji, exploitami, czy DNS hijackingiem.

Radware

Ochrona przed atakami DDoSFirma

Radware jest, obok firmy F5, globalnym liderem w zakresie rozwiązań bezpieczeństwa aplikacyjnego dla centrów danych w modelach wirtualnych i w chmurze. Rozwiązania Radware sprawdzają się m.in. w takich obszarach, jak: ochrona przed atakami DDoS, ataki wolumetryczne oraz ataki aplikacyjne. Ciekawym i bardzo dobrze ocenianym przez klientów mechanizmem jest behawioralna ochrona przed atakami DDoS (DefensePro), która jest jednym z elementów autorskiej referencyjnej architektury Infradata, dotyczącej bezpiecznego brzegu w datacenter.

Tufin

Zarządzanie rozwiązaniami sieciowymi

Tufin Orchestration Suite umożliwia firmom usprawnienie procesów zarządzania politykami bezpieczeństwa w obrębie złożonych, zróżnicowanych środowisk. Tufin automatyzuje procesy projektowania i wprowadzania zmian konfiguracji sieci, obejmując także ich analizę i kontrolę – od warstwy aplikacji do warstwy sieci. Rozwiązanie to umożliwia definiowanie zasad zabezpieczeń organizacji, obejmujących segmentację i wizualizację sieci. Zapewnia także zarządzanie ryzykiem, jego analizę oraz wgląd we właściwości reguł bezpieczeństwa oraz planowanie i ocenę w oparciu o dobre praktyki, czy regulacje.

Flowmon

Monitorowanie ruchu sieciowego

Flowmon dostarcza narzędzia do monitorowania oraz analizowania ruchu sieciowego w czasie rzeczywistym. Umożliwia to administratorom sieci szybki wgląd w bieżący stan sieci, komunikację urządzeń, identyfikację hostów, aplikacji i użytkowników oraz szybkie eliminowanie usterek i optymalizację sieci. Dodatkowe moduły zapewniają wykrywanie anomalii sieciowych (mechanizm wykorzystujący machine learning), analizę wydajności usług, zbieranie statystyk z ruchu sieciowego w celu wykrywania ataków DDoS i zainicjowania automatycznych działań obronnych oraz nagrywanie ruchu sieciowego do późniejszej analizy.

Fortinet

Rozwiązania do budowy i ochrony sieci

Firma Fortinet jest dostawcą wysokowydajnych informatycznych rozwiązań zabezpieczających, które umożliwiają klientom ochronę i kontrolę używanej infrastruktury informatycznej. Jej specjalnie opracowane, zintegrowane technologie zabezpieczeń wraz z badającymi zagrożenia usługami FortiGuard, zapewniają klientom niezwykle skuteczną ochronę treści, dotrzymującą kroku nieustannie rozwijającym się zagrożeniom. Fortinet dostarcza szerokie portfolio produktów bezpieczeństwa sieci i organizacji, zawierające między innymi rozwiązania typu Firewall NGFW (SSL/IPSec VPN, SD-WAN), systemy uwierzytelniania wieloskładnikowego, komponenty sieci bezprzewodowych, Web Application Firewall, sandbox oraz ochronę stacji końcowych.

Wallix

Kontrola i rejestracja zdalnych sesji dostępu do sieci (PIM, PAM)

Rozwiązanie firmy Wallix pozwala na zarządzanie dostępem użytkowników uprzywilejowanych do kluczowych systemów, wraz z możliwością obserwacji poszczególnych sesji w czasie rzeczywistym. Każda sesja może być także nagrywana do późniejszej analizy. System umożliwia między innymi wymuszenie zmiany haseł dla użytkowników po każdym zalogowaniu do systemu docelowego. Dzięki temu użytkownik uprzywilejowany nie zna danych uwierzytelniania do poszczególnych systemów, a tym samym ryzyko kradzieży haseł do zasobów krytycznych jest znacząco zredukowane.

TrendMicro

Ochrona infrastruktury DataCenter

Rozwiązania TrendMicro z grupy Deep Security zostały zaprojektowane we współpracy z czołowymi światowymi dostawcami technologii chmurowych, kontenerowych i środowisk wirtualnych m.in: AWS, Azure, Google Cloud, Vmware, Docker, Kubernetes. Dzięki temu jeden produkt zapewnia scentralizowaną ochronę we wszystkich środowiskach: serwerach fizycznych, wirtualnych i działających w chmurze oraz kontenerowych. Do najważniejszych modułów funkcjonalnych można zaliczyć: monitorowanie integralności, kontrolę uruchamianych aplikacji oraz ochronę przed szkodliwym oprogramowaniem i włamaniami. Dodatkowo dzięki funkcji Virtual Patching możliwe jest zabezpieczanie podatności „inline" zanim pojawi się oficjalna łatka producenta chronionego systemu lub usługi. Dostępna w portfolio TrendMicro grupa rozwiązań

Deep Discovery wykorzystuje wyspecjalizowane mechanizmy wykrywania zagrożeń (np. symulacje w pełni konfigurowalnym sandboxie) oraz globalne dane analityczne o zagrożeniach pochodzące z sieci Smart Protection Network.

Pulse Secure

Bezpieczny dostęp do sieci firmowej

Pulse Secure jest jednym z liderów dostarczających mechanizmy bezpiecznego dostępu do sieci firmowej: NAC oraz SSLVPN. Rozwiązanie Network Access Cotrol (NAC), współpracujące z większością dostawców infrastruktury sieciowej, zapewnia szczegółową wiedzę o tym, w jaki sposób oraz przez kogo sieć jest wykorzystywana, które urządzenia lub/i użytkownicy wykorzystują sieć w sposób zgodny z polityką firmy. Mając wgląd i widoczność w to jak funkcjonują urządzenia w sieci, możliwe jest wdrażanie właściwych reguł kontrolnych, zgodnych z polityką bezpieczeństwa firmy, dzięki temu tylko uwierzytelnieni oraz autoryzowani użytkownicy i urządzenia będą mieli dostęp do sieci firmy. Dzięki integracji systemu NAC z firewallami, możliwe staje się m.in. budowanie reguł filtrowania na bazie tożsamości konkretnego użytkownika lub grup użytkowników, np. Active Directory oraz szczegółowe śledzenie aktywności danej osoby w sieci tzw. user awareness.

Pulse Secure dostarcza także rozwiązania zdalnego dostępu do zasobów (Data Center, Cloud) z wykorzystaniem SSL VPN, wspierające wiele platform systemowych oraz przeglądarek internetowych.

VMware

Platforma wirtualizacji oraz rozwiązania dla zarządzania i automatyzacji środowisk wirtualnych

Współczesna architektura Centrum Przetwarzania Danych (SDDC – Software Defined Data Center) opiera się na wirtualizacji i automatyzacji wszystkich jej komponentów – zasobów obliczeniowych, dyskowych i sieci.

Celem jest uzyskanie jak najbardziej elastycznych środowisk, w których warstwa sprzętowa nie jest już przedmiotem codziennej konfiguracji. VMware zapewnia narzędzia do wirtualizacji serwerów (VMware vSphere), macierzy dyskowych (VMware vSAN), oraz infrastruktury sieciowej (NSX V/T). Pozwala również na poprawę bezpieczeństwa w SDDC poprzez mechanizmy mikrosegmentacji (NSX V/T).

W nowoczesnych Centrach Przetwarzania Danych zaczynają wieść prym technologie kontenerowe, dla których warto zastanowić się nad spójnym zarządzaniem wszystkimi komponentami, także w środowiskach MultiCloud (NSX-T, PKS, PKS Essentials, VMware Cloud AWS).

Zastosowanie automatyzacji sprawia, że istotnym staje się zapewnienie odpowiedniej widoczności, narzędzi do planowania i optymalizacji procesów, co dostarczają produkty z rodziny vRealize.

Infradata
DIMsystem

Infradata Polska Sp. z o.o.

ul. Puławska 537
02-844 Warszawa

www.infradata.pl

t. +48 22 567 17 40
info@infradata.pl