EXCLUSIVE PORTFOLIO

Pojďme společně vytvořit bezpečný svět

EXCLUSIVE NETWORKS

Naše poslání a vize

Exclusive Networks je důvěryhodným specialistou na kybernetickou bezpečnost, který požadavky dnešní doby řeší pomocí cloudových služeb a služeb kybernetické bezpečnosti.

Jsme poháněni **vysoce výkonnou technologií,** podporováni **rozsáhlým partnerským ekosystémem** a **špičkovými talenty v oboru**, které sdílejí společnou filosofii **„služby na prvním místě“.**

Naší vizí je vytvořit zcela důvěryhodný digitální svět pro každého – jednotlivce i organizace. Rostoucí závislost na digitální infrastruktuře i zvyšující se hrozby kladou stále vyšší nároky na bezpečnost, přičemž odborných kapacit je nedostatek. Proto jsme tu my, abychom vám pomohli tyto výzvy zvládnout.

Na dalších stranách naleznete **přehled našich řešení** uspořádaný podle kategorií a technických oblastí. **Pro konzultaci se neváhejte obrátit na naše specialisty, kteří vám pomohou vybrat optimální variantu.**

Co nás odlišuje?

Jsme jedineční tím, že se specializujeme na kybernetickou bezpečnost v globálním měřítku. Naše odlišnost nespočívá jen v portfoliu, ale především v přístupu: **snažíme se neustále inovovat, hledat nové cesty a překračovat zavedené hranice.**

Nebojíme se být jiní. Díky tomu přinášíme našim partnerům vysokou přidanou hodnotu – propojujeme mezinárodní zkušenosti s lokální odborností a vytváříme řešení, která obstojí dnes i v budoucnu.

Jsme DŮVĚRYHODNÍ

Jsme RELEVANTNÍ

Jsme EXPERTI

Jsme GLOBÁLNÍ

Jsme UNIKÁTNÍ

Zastupujeme síť předních výrobců:

NOZOMI NETWORKS

Red Hat

elastic

HashiCorp
an IBM Company

docker

storware

Radiflow

Poskytujeme také rozsáhlou nabídku služeb:

- technické služby
- obchodní služby
- vzdělávací služby
- marketingové služby

Pro konzultaci jsme tu pro vás. Neváhejte se obrátit na naše specialisty – pomůžeme vám vybrat optimální řešení přesně podle vašich potřeb.

info@exclusive-networks.cz

Aplikační & e-mailová ochrana

Secure Email Gateways

Secure Email Gateways poskytují ochranu před e-mail-based hrozbami jako spam, phishing a malware. Implementují pokročilé threat protection techniky včetně sandboxing, URL rewriting a attachment analysis. Podporují Data Loss Prevention pro odchozí e-maily a šifrování pro citlivé komunikace. Moderní řešení využívají threat intelligence a machine learning pro detekci sofistikovaných attack vectors. Poskytují podrobný reporting a compliance funkce pro regulační požadavky.

FORTINET proofpoint. TREND MICRO

Web Application Firewall (WAF)

WAF poskytuje specializovanou ochranu pro webové aplikace proti běžným attack vectors jako SQL injection, cross-site scripting a DDoS. Implementuje filtrování na aplikační vrstvě založené na analýze HTTP/HTTPS provozu. Moderní WAF řešení využívají machine learning pro detekci nových attack patterns a zero-day exploits. Podporují pozitivní bezpečnostní model prostřednictvím application profiling a behavior analysis. Poskytují detailní logování a reporting pro compliance a forenzní analýzu.

FORTINET Progress Kemp LoadMaster

Síťová optimalizace & výkon

Secure Access Service Edge (SASE)

SASE spojuje síťové a bezpečnostní funkce do jednotné cloud-native platformy. Kombinuje SD-WAN capabilities s komplexními bezpečnostními službami jako firewall, CASB, DLP a Zero Trust Network Access. SASE poskytuje konzistentní bezpečnostní politiky bez ohledu na lokaci uživatelů nebo zdrojů. Umožňuje zabezpečené připojení pro vzdálené pracovníky a cloudové aplikace. Klíčové výhody zahrnují sníženou složitost, zlepšený výkon a zjednodušenou správu distribuovaných sítí.

FORTINET TREND MICRO

Edge Management

Edge Management představuje strategický přístup k řízení distribuovaných IT prostředí, kde se výpočetní výkon, bezpečnost a správa infrastruktury přesouvají blíže ke zdroji dat – tedy na „edge“ sítě. Tento model umožňuje zpracování dat v reálném čase, snižuje latenci, zvyšuje provozní efektivitu a zároveň zajišťuje vyšší úroveň zabezpečení v decentralizovaných prostředích.

FORTINET Progress Chef

Cloud Access Security Brokers (CASB)

CASB jsou bezpečnostní nástroje, které poskytují viditelnost a kontrolu nad používáním cloudových služeb v organizaci. Fungují jako prostředník mezi uživateli a cloudovými aplikacemi, kde monitorují a kontrolují přístup k datům. Klíčové funkce zahrnují Data Loss Prevention (DLP), detekci anomálií a vynucování bezpečnostních politik. CASB řešení pomáhají organizacím udržet kontrolu nad citlivými daty uloženými v cloudových službách. Podporují compliance požadavky a poskytují audit trail pro cloudové aktivity.

FORTINET proofpoint. TREND MICRO

Middleware a aplikační platformy

Middleware a aplikační platformy představují sadu nástrojů a produktů pro vývoj, integraci a správu podnikových aplikací. Umožňují propojení různých systémů, podporují messaging, API management, business rules i procesní automatizaci. Poskytují stabilní základ pro provoz moderních i tradičních aplikací a usnadňují jejich škálování a správu v komplexním prostředí.

Red Hat

Platformy pro kontejnery a orchestraci

Platformy pro správu kontejnerů usnadňují práci se Kubernetes díky integrovaným nástrojům a podporují rychlé nasazení aplikací prostřednictvím automatizovaných CI/CD pipeline. Poskytují podnikové zabezpečení, škálovatelnost, vysokou dostupnost a portabilitu aplikací mezi on-premises, hybridním i multi-cloud prostředím. Díky podpoře kontejnerů, mikroslužeb a rozsáhlému ekosystému jsou ideálním řešením pro moderní, flexibilní vývoj a provoz aplikací.

docker Progress Chef

Red Hat

Cloudová infrastruktura a virtualizace

Platformy pro cloudovou infrastrukturu umožňují budování flexibilních privátních i hybridních cloudů s integrovanou správou výpočetních zdrojů, úložišť a sítí. Nabízejí stabilitu na podnikové úrovni, dlouhodobou podporu, bezpečnostní aktualizace a certifikace pro široké spektrum hardwaru a softwaru. Díky podpoře automatizace a orchestrace zjednodušují správu cloudu a zajišťují efektivní využití zdrojů podle potřeb organizace.

Red Hat

Endpoint Detection and Response (EDR/XDR)

EDR jsou pokročilé bezpečnostní nástroje, které monitorují a analyzují aktivity na koncových zařízeních. Poskytují real-time detekci hrozeb, forenzní analýzu a automatizované odpovědi na bezpečnostní incidenty. XDR rozšiřuje EDR konceptem o korelaci dat z více bezpečnostních vrstev včetně sítě, cloudu a aplikací. Tato řešení využívají machine learning a behavioral analytics pro identifikaci pokročilých hrozeb. Umožňují rychlou izolaci napadených systémů a poskytují detailní forenzní informace pro incident response.

CROWDSTRIKE
CYBERARK
FORTINET
TREND MICRO

Vulnerability Management

Vulnerability Management představuje systematický přístup pro identifikaci, hodnocení a řešení bezpečnostních zranitelností. Zahrnuje pravidelný vulnerability scanning, penetrační testování a bezpečnostní hodnocení. Vulnerability scanning se přitom uplatňuje nejen v IT prostředí, ale i v oblasti OT. Poskytuje rámce pro stanovení priorit založené na risk scoring a threat intelligence. Implementuje patch management procesy pro včasné řešení kritických zranitelností. Moderní řešení integrují s DevOps workflows pro kontinuální bezpečnostní testování. Klíčové metriky zahrnují průměrný čas do detekce, průměrný čas do řešení a celkové snížení rizika.

CROWDSTRIKE
Radiflow
tenable
TREND MICRO

Network Detection and Response (NDR)

NDR technologie monitorují síťový provoz v real-time pro detekci bezpečnostních hrozeb a anomálií. Využívají behavioral analytics a machine learning pro identifikaci suspicious aktivit, které mohou indikovat kompromitaci. NDR poskytuje deep visibility do síťové komunikace včetně šifrovaného provozu prostřednictvím metadata analysis. Automatizované response capabilities umožňují rychlou izolaci napadených systémů nebo blokování malicious komunikace. Integruje se s SIEM a SOAR platformami pro komplexní security operations.

Extreme networks
Gigamon
Progress Flowmon
tenable

Security Information and Event Management (SIEM)

SIEM platformy agregují a analyzují bezpečnostní události z celé IT infrastruktury. Poskytují centralizovanou viditelnost do bezpečnostního stavu organizace prostřednictvím log managementu a correlation rules. Pokročilé analytické capabilities umožňují detekci složitých attack patterns a insider threats. SIEM podporuje compliance reporting a forenzní analýzu pro incident response. Moderní řešení integrují threat intelligence feeds a poskytují automatizované alertování pro kritické bezpečnostní události.

CROWDSTRIKE
FORTINET
elastic
TREND MICRO

Compliance and Governance

Oblast Security Automation / Policy-as-Code představuje zásadní komponentu moderního přístupu k zabezpečení IT prostředí, kde jsou bezpečnostní politiky definovány, spravovány a prosazovány pomocí strojově čitelného kódu. Tento přístup umožňuje automatizované ověřování souladu s bezpečnostními standardy, jako jsou PCI-DSS, ISO27001 nebo CIS benchmarky, a zároveň zajišťuje auditovatelnost, verzování a opakovatelnost bezpečnostních kontrol napříč celým životním cyklem infrastruktury.

Progress Chef

Patch Management and Remediace

Patch Management and Remediace představuje zásadní součást moderní kybernetické bezpečnosti, jejímž cílem je minimalizovat rizika vyplývající ze známých zranitelností prostřednictvím efektivního nasazování záplat a nápravných opatření. V prostředí, kde se hrozby neustále vyvíjejí, je nutné přejít od reaktivního přístupu k proaktivnímu modelu, který umožňuje rychlou identifikaci, prioritizaci a automatizovanou aplikaci bezpečnostních aktualizací.

Progress Chef TREND MICRO

DNS bezpečnost

DNS Security prezentuje systematický přístup k ochraně jednoho z klíčových pilířů internetové infrastruktury – systému doménových jmen. Zahrnuje detekci a mitigaci DNS útoků, jako jsou DNS spoofing, cache poisoning, exfiltrace dat přes DNS tunneling či DDoS útoky na DNS servery.

infoblox

CROWDSTRIKE FORTINET

NOZOMI NETWORKS Radiflow

tenable TREND MICRO

IOT / IOT-OT

Internet of Things (IoT) a Operational Technology (OT) představují síťové připojení fyzických zařízení a průmyslových systémů. IoT zahrnuje širokou škálu smart devices od senzorů po connected vehicles. OT se zaměřuje na průmyslové řídicí systémy jako SCADA, PLC a HMI. Bezpečnost IoT/OT vyžaduje specifické přístupy kvůli omezeným výpočetním zdrojům a legacy systémům. Klíčové aspekty zahrnují device management, network segmentation, pravidelný vulnerability scanning a monitoring anomálií.

Operační systémy

Podnikové operační systémy jsou navrženy jako stabilní, bezpečné a spolehlivé prostředí s dlouhodobou podporou a certifikacemi pro různé typy nasazení. Nabízejí vysokou úroveň zabezpečení, profesionální podporu a širokou kompatibilitu s hardwarem i softwarem. Díky modularitě a integraci s moderními technologiemi, jako jsou cloudová řešení, virtualizace či kontejnery, dodávají flexibilitu a škálovatelnost potřebnou pro provoz v různorodých podnikových prostředích.

Red Hat

Monitoring

Monitoring infrastruktury poskytuje ucelený pohled na výkon a dostupnost síťových prvků, serverů, aplikací i cloudových služeb. Umožňuje rychle odhalit výpadky, úzká místa nebo neobvyklé chování a tím zkracuje dobu potřebnou k řešení incidentů. Díky vizualizaci topologie a centralizovanému dohledu mají IT týmy kontrolu nad celým prostředím z jednoho místa. Moderní řešení přinášejí flexibilní škálování, přehledné dashboardy, alerting a reporty, které podporují jak každodenní provoz, tak strategické plánování kapacity.

FORTINET

Progress WhatsUp Gold

Data and Log Management

Data and Log Management představuje systematický přístup ke sběru, ukládání, analýze a správě datových záznamů a logů z různých systémů, aplikací a síťových prvků. Zajišťuje centralizované ukládání logů pro účely provozního dohledu, bezpečnostní analýzy i plnění regulačních požadavků. Podporuje detekci anomálií a korelaci událostí napříč prostředím, což umožňuje rychlejší odhalení incidentů a jejich efektivní řešení. Součástí je správa životního cyklu dat, včetně nastavení retence, archivace a bezpečné likvidace. Moderní řešení integrují pokročilou analytiku, strojové učení a automatizaci pro proaktivní identifikaci hrozeb a optimalizaci provozu. Klíčové metriky zahrnují objem zpracovaných dat, dobu uchování, rychlost vyhledávání a úroveň detekovaných bezpečnostních událostí.

CROWDSTRIKE

elastic

FORTINET

Logmanager

Automatizace

Automatizační platforma zjednodušuje správu IT procesů díky agentless přístupu a rozsáhlým knihovnám modulů pro infrastrukturu, aplikace i bezpečnost. Umožňuje rychlé vytváření, nasazování a škálování automatizačních řešení, zvyšuje efektivitu, minimalizuje riziko chyb a podporuje spolupráci napříč týmy prostřednictvím centralizované správy a nástrojů pro orchestraci.

Red Hat Progress Chef

Security Orchestration, Automation and Response (SOAR)

SOAR platformy automatizují bezpečnostní procesy a orchestrují response aktivity napříč security tools. Umožňují tvorbu playbooks pro standardizované incident response postupy. Poskytují case management capabilities pro sledování a dokumentaci bezpečnostních incidentů. SOAR se integruje s existující bezpečnostní infrastrukturou prostřednictvím API a konektorů. Klíčové výhody zahrnují zkrácení reakčních časů, zlepšenou konzistenci a uvolnění kapacity bezpečnostních analytiků pro složité úkoly.

FORTINET CROWDSTRIKE

TREND MICRO

Business Process Management

Platformy pro správu a automatizaci podnikových procesů dovolují modelování, optimalizaci a sledování firemních postupů s cílem zvýšit efektivitu a flexibilitu organizace. Díky vizuálním nástrojům, integraci s podnikovými systémy a podpoře analytiky usnadňují spolupráci mezi IT a byznysem a pomáhají rychle reagovat na měnící se potřeby trhu.

Red Hat

Backup and Recovery

Backup & Recovery je oblast, která zahrnuje strategie a technologie pro zálohování dat a jejich obnovení v případě ztráty nebo poškození. Moderní řešení kombinují tradiční zálohování s pokročilými funkcemi jako deduplikace, komprese a cloudové úložiště. Klíčové aspekty zahrnují RTO (Recovery Time Objective) a RPO (Recovery Point Objective) pro definování požadavků na obnovení. Řešení zahrnují různé typy záloh od plných přes inkrementální až po kontinuální replikaci dat. Disaster Recovery plány jsou nezbytnou součástí pro zajištění kontinuity podnikání při výpadcích.

storware

Storage

Softwarově definovaná úložiště umožňují škálovatelné blokové, objektové i souborové ukládání dat s vysokou dostupností a odolností vůči výpadkům. Hodí se nejen pro náročná datová centra, ale i pro jednodušší sdílení souborů, přičemž konkrétní řešení se liší architekturou a vhodností podle typu aplikací a workloads.

Red Hat

Data Encryption and Protection

Šifrovací technologie zajišťují ochranu citlivých informací jak při uložení, tak při přenosu dat. Poskytují bezpečnostní vrstvu proti neoprávněnému přístupu, ztrátě či zneužití dat a podporují splnění regulačních a compliance požadavků. V kombinaci s řízením přístupu, auditem a dalšími bezpečnostními mechanismy tvoří základní prvek strategie ochrany informací v moderních IT prostředích.

HashiCorp
an IBM Company

Identity and Access Management (IAM)

IAM systémy spravují digitální identity a jejich přístupová práva k podnikovým zdrojům. Klíčové funkce zahrnují single sign-on (SSO), multi-factor authentication (MFA) a role-based access control (RBAC). IAM implementuje principy least privilege a zero trust pro minimalizaci bezpečnostních rizik. Moderní řešení podporují federované identity a integraci s cloudovými službami. Lifecycle management zajišťuje správný provisioning a deprovisioning uživatelských účtů při změnách v organizaci.

FORTINET CROWDSTRIKE

CYBERARK Red Hat TREND MICRO

Identity Management (IDM)

IDM řešení spravují digitální identity uživatelů a jejich životní cyklus v rámci organizace. Umožňují centrální řízení uživatelů, skupin a oprávnění napříč aplikacemi i prostředími a zajišťují konzistentní a bezpečnou správu přístupů. Klíčové funkce zahrnují provisioning a deprovisioning účtů, správu atributů identity a integraci s adresářovými službami. Moderní IDM systémy podporují škálovatelnost, integraci s cloudem, kontejnery i hybridními infrastrukturami a usnadňují napojení na autentizační a autorizační platformy (např. IAM, SSO, MFA).

Red Hat CYBERARK

Progress Kemp LoadMaster

Privileged Access Management (PAM)

PAM řešení spravují a monitorují přístup k privilegovaným účtům a kritickým systémům. Implementují principy least privilege a just-in-time access pro minimalizaci bezpečnostních rizik. Klíčové funkce zahrnují password vaulting, session recording a privileged task automation. PAM poskytuje detailní audit trail všech privilegovaných aktivit a umožňuje rychlé odvolání přístupů. Moderní PAM řešení podporují cloudovou integraci a dodávají analytiky pro risk assessment privilegovaných uživatelů.

CYBERARK CROWDSTRIKE

FORTINET

Secret Management

Nástroje pro správu tajemství a citlivých dat zabezpečují ukládání, šifrování a centralizovanou kontrolu přístupu k heslům, klíčům, certifikátům či tokenům. Umožňují automatizaci bezpečnostních procesů, detailní audit a integraci s moderními IT prostředími včetně cloudu, kontejnerů a hybridní infrastruktury. Díky tomu posilují ochranu kritických dat a zjednodušují dodržování bezpečnostních standardů i regulací.

HashiCorp an IBM Company

Data Centre Networking (SDN)

Software-Defined Networking představuje paradigma, kde je síťová kontrola oddělena od fyzické infrastruktury. Umožňuje centralizované řízení síťového provozu prostřednictvím softwarových kontrolerů. SDN nabízí flexibilitu, programovatelnost a dynamické přizpůsobení síťových politik dle potřeb aplikací. Klíčové výhody zahrnují snížení komplexity správy, rychlejší nasazování služeb a lepší využití síťových zdrojů. V datových centrech SDN umožňuje virtualizaci síťových funkcí a podporuje agilní provoz.

Extreme networks FORTINET Red Hat

Wired and Wireless LAN Access

Naše řešení pro LAN infrastrukturu dodává spolehlivou konektivitu pro datová centra, enterprise zákazníky i segment SMB.

Drátová část je založena na moderním ethernet switchingu s podporou logické segmentace sítě, řízení kvality přenosu a napájení koncových zařízení prostřednictvím datové infrastruktury (PoE).

Bezdrátový přístup je zajištěn nejnovějšími wi-fi standardy, které nabízejí vysoký výkon, flexibilitu a pokročilé funkce.

Díky jednotné platformě pro centralizovaný management je možné celou síť efektivně spravovat z jednoho místa.

Samozřejmostí je také pokročilá ochrana – 802.1X autentizace, síťová segmentace a detekce neautorizovaných přístupových bodů chrání prostředí před bezpečnostními hrozbami.

Extreme networks FORTINET

Visibility WAN Edge Infrastructure (SD-WAN)

Software-Defined WAN transformuje tradiční WAN konektivitu prostřednictvím centralizovaného řízení a správy politik. Umožňuje inteligentní výběr cest přes více typů připojení včetně MPLS, broadband a LTE. SD-WAN poskytuje application-aware routing pro optimalizaci výkonu kritických aplikací. Klíčové výhody zahrnují snížené náklady, zlepšenou agilitu a zjednodušenou správu distribuovaných sítí.

Extreme networks FORTINET

DDI (DNS, DHCP, IPAM) a DNS bezpečnost

DDI představuje integrované řízení klíčových síťových služeb – DNS, DHCP a IP Address Management. DNS zajišťuje spolehlivý překlad doménových jmen, DHCP automatizuje přidělování síťových konfigurací a IPAM centralizovaně spravuje adresní prostor. Spojení těchto služeb do jednoho řešení zjednodušuje administraci, zvyšuje efektivitu a minimalizuje chyby.

infoblox

Wi-Fi Planning, Design and Optimization

Naše řešení s využitím platformy Ekahau přináší profesionální přístup k návrhu, plánování a optimalizaci bezdrátových sítí. Díky přesnému modelování pokrytí, simulaci výkonu a detailní analýze v reálném prostředí pomáháme budovat wi-fi infrastrukturu, která splňuje nejvyšší požadavky na spolehlivost, kapacitu i bezpečnost. Výsledkem je efektivně navržená a snadno spravovatelná bezdrátová síť připravená na současné i budoucí potřeby vašeho podnikání.

ekahau

Network Packet Brokers

Network Packet Brokers jsou specializovaná síťová zařízení, která agregují, filtrují a distribuují síťový provoz k monitoring a security nástrojům. Umožňují efektivní využití monitoring infrastruktury prostřednictvím inteligentní distribuce paketů. Poskytují pokročilé možnosti filtrování založené na různých kritériích jako protokoly, IP adresy nebo aplikace. Podporují load balancing pro monitoring tools a eliminují duplicitní pakety. Jsou klíčové pro viditelnost do vysokorychlostních sítí a optimalizaci výkonu bezpečnostních a monitoring systémů.

Gigamon®

Application Delivery Controllers (ADC) (Load Balancing)

ADC jsou síťová zařízení, která optimalizují distribuci síťového provozu mezi více servery nebo aplikacemi. Hlavní funkcí je load balancing, který zajišťuje rovnoměrné rozložení zátěže a zvyšuje dostupnost služeb. ADC také poskytují funkcionality jako SSL offloading, komprese dat a cache pro zrychlení odezvy aplikací. Moderní ADC řešení zahrnují pokročilé algoritmy pro směrování provozu na základě zdravotního stavu serverů. Tyto technologie jsou klíčové pro zajištění vysoké dostupnosti a výkonu webových aplikací a služeb.

FORTINET Progress® Kemp® LoadMaster®

Enterprise Network Firewalls (NGFW)

Next-Generation Firewalls představují pokročilé síťové bezpečnostní zařízení, které kombinuje tradiční firewall funkcionalitu s dalšími bezpečnostními funkcemi. NGFW poskytují deep packet inspection, application awareness a integrovanou intrusion prevention. Zahrnují pokročilé funkce jako SSL/TLS inspection, sandboxing a threat intelligence integration. Moderní NGFW podporují centralizované řízení politik a poskytují detailní reporting a monitoring. Jsou klíčovou součástí defense-in-depth strategie pro ochranu podnikových sítí.

FORTINET

Network Access Controllers (NAC)

NAC řešení kontrolují přístup zařízení k podnikové síti na základě jejich identity, compliance stavu a bezpečnostních politik. Implementují authentication, authorization a accounting (AAA) pro všechna připojená zařízení. NAC může vynucovat security policies před povolením síťového přístupu včetně patch management a antivirus kontroly. Podporuje různé deployment modely od in-line po out-of-band monitoring. Poskytuje detailní audit trail síťových připojení a umožňuje dynamické přeřazení zařízení do příslušných síťových segmentů.

FORTINET Extreme networks

Služby

Kromě rozsáhlého produktového portfolia nabízíme služby zaměřené na to, aby vám jako partnerovi usnadnily cestu k úspěchu u vašich zákazníků.

Technické služby

Technická pre-sales podpora
Odpovíme na vaše technické dotazy v rámci pre-sales podpory nebo vás doprovodíme ke klientovi s odborným poradenstvím.

Technická podpora
Ve spolupráci s našimi globálními týmy ulevíme vašemu týmu technické podpory a nabídneme flexibilní kapacity, abychom zajistili dostupnost služeb vašemu koncovému zákazníkovi.

Konzultační služby
Naši experti vám rádi pomohou s různorodými úkoly – od řešení konkrétních problémů až po realizaci celého projektu.

Vybavení pro Demo, Pilot a PoC
Můžeme vám poskytnout testovací zařízení pro účely demonstrace, pilotních projektů nebo Proof of Concept (PoC).

Wireless Site Survey
Před zahájením bezdrátového projektu doporučujeme provést průzkum lokality (Site Survey), abyste přesně věděli, kolik přístupových bodů je potřeba a kam je umístit pro optimální pokrytí a zajištění potřebné kvality komunikace.

Služby instalace a konfigurace
Exclusive Networks bude vaší oporou při implementaci a konfiguraci řešení v rámci projektu.

Pre–staging
Exclusive Networks vás plně podpoří v rámci pre-stagingu: nabízíme předkonfigurace, testování a označení zařízení před dodávkou, včetně zajištění logistického procesu na globální úrovni.

Globální služby
Podporujeme naše partnery od A do Z při realizaci mezinárodních projektů – včetně poradenství, podpory a logistických služeb.

Deployment as a Service (DepaaS)
Ve 150+ zemích nabízíme kompletní instalaci na místě. V kombinaci s pre-stagingem a logistickými službami zajistíme celý proces od A do Z.

Služby na míru
Nenašli jste, co hledáte? Rádi s vámi probereme možnosti a navrhneme řešení na míru.

Obchodní služby

Komerční pre-sales podpora

Náš obchodní tým má rozsáhlé znalosti o dodavatelích, zodpoví vaše komerční pre-sales dotazy a pomůže s přípravou nabídky.

Renewals

Specializovaný tým sleduje termíny končících smluv, licencí i služeb a zajistí jejich hladkou obnovu bez přerušení.

Vzdělávací služby

Školení

Jsme lokálním akreditovaným training centrem (ATC) společnosti Fortinet. K dispozici máme dva certifikované Fortinet trenéry. Nabízíme jak oficiální školení s pevně danými termíny, tak individuální vzdělávání s možností přizpůsobení obsahu i harmonogramu.

Marketingové služby

Nabízíme širokou škálu marketingových služeb k posílení podporu vašich aktivit a pro udržení přehledu o trhu i dodavatelích.

Formy podpory: on-line marketing, newslettery, eventy, semináře, veletrhy, kulaté stoly, onboarding boxy, marketingové kampaně apod. Rádi s vámi probereme konkrétní možnosti.

Pronájem prostor pro workshopy a školení

Exclusive Networks nabízí také možnost pronájmu plně vybavených prostor pro konání školení, workshopů nebo seminářů. Naše zázemí je ideální pro technické akce – nabízíme moderní konferenční místnosti, prezentační techniku, připojení k internetu a možnost občerstvení. Rádi vám pomůžeme s organizací celé akce dle vašich potřeb.

Partner Portál

Registrujte se do našeho nového **Partner Portálu** a získejte snadný a bezpečný přístup k objednávkám v reálném čase, přehledným statistikám a reportům, klíčovým dokumentům i licencím – to vše na jednom místě. Portál šetří čas díky automatizaci procesů, zjednodušuje administrativu a poskytuje vždy aktuální informace a novinky, které potřebujete pro svůj byznys.

https://portal.exclusive-networks.cz/

Stáhněte si brožuru níže

Pomáháme při přechodu do zcela důvěryhodného digitálního světa.

Ozvěte se nám

Exclusive Networks Czechia s.r.o.
Argentinská 1610/4, 170 00 Praha

+420 724 647 785

info@exclusive-networks.cz
www.exclusive-networks.com/cz/

Sledujte nás