

## Veracomp + Fortinet

# Fortinet Secure Access

**Technologie a trendy na trhu rychle mění způsob, jakým podniky zavádí místní sítě LAN, připojují koncová zařízení a provozují podnikové aplikace všech typů. Dopady těchto změn a následné trendy ovlivňují i způsob, jakým musí být sítě zabezpečené.**

Počet bezdrátových zařízení připojených k síti a jejich typů roste geometrickou řadou. Do podnikových sítí se připojují nejen notebooky, chytré telefony a tablety. Rozvoj internetu věcí (IoT) do nich vnáší nové typy zařízení. Analytická společnost Gartner předpovídá, že do roku 2020 bude připojených 33 miliard koncových bodů. Takovýto exponenciální nárůst počtu připojených zařízení přináší nové zranitelnosti a nové příležitosti k útoku. Zejména zařízení IoT (např. bezdrátové senzory, indikátory blízkosti a další malá zařízení) často nejsou vybavená tak, aby podporovala bezpečnostní řešení.

### Zranitelnosti bezdrátového připojení

Wi-Fi se pro mnoho takových síťových zařízení stává primárním přístupovým médiem. To vyvolává nikdy nekončící potřebu zvyšovat rychlost. Struktura zařízení se postupně přesunuje od podnikových k soukromým a připojení stále větší měrou k bezdrátovému. Na pořad dne proto přichází otázka zjevných zranitelností bezdrátových zařízení a sítí. Společnost Fortinet nedávno provedla průzkum, který ukazuje, že zranitelnost bezdrátových přístupových sítí vyvolává značné obavy u manažerů a správců IT.

Roste počet mobilních zařízení a s tím se zvyšuje i počet a míra využití mobilních aplikací. To znamená, že podniky čelí nejen problémům s podporou většího počtu podnikových aplikací, ale také se zranitelnostmi, které do sítí vnáší aplikace, které se v ní dříve nevykytovaly.

### Složitější provoz IT

Bez ohledu na nebyvalý růst rozmanitosti aplikací a zařízení uživatelé očekávají jednotný přístup do sítí – takový, který zajistí konzistentní bezpečnostní pravidla pro aplikace a zařízení v metalických i bezdrátových síťových prostředích. Nekonzistentnost a nesnadná správa pravidel značně ztěžují práci IT oddělením, která mají plné ruce práce se zaplňováním mezer v zabezpečení.

### Architektura Fortinet Secure Access

Kvůli těmto trendům a problémům je důležité zjednodušit zavádění a správu podnikových sítí, aplikací a zařízení. Přístupová vrstva sítě, která je nejen bezpečná, ale také jednoduchá na správu a nepřetržitě chráněná, brání důležité podnikové zdroje a uživatele před kybernetickými útoky.

Sítě Fortinet jsou proto jiné. Řešení společnosti Fortinet pro zabezpečení přístupu k síti nabízí schopnosti next-generation firewallů a ochranu přístupu k podnikovým zdrojům. Na rozdíl od tradičních bezdrátových řešení, která řeší pouze konektivitu, je jádrem řešení Fortinet pro bezpečný přístup účinné zabezpečení sítě, spolu s konektivitou. Řešení společnosti Fortinet poskytují pro bezpečný přístup stejně vysokou úroveň zabezpečení ve všech typech implementace, od samostatného přístupového bodu (AP) v izolované kanceláři přes soustavu několika AP v maloobchodní provozovně po tisíce AP v rozsáhlých průmyslových komplexech. Produktové nabídky umožňují každému podniku zvolit topologii a správu sítí podle svých preferencí, aniž by to bylo na úkor kvality zabezpečení.

Zabezpečení podnikové komunikace, soukromých informací, finančních transakcí a mobilních zařízení vyžaduje mnohem více než řízení přístupu do sítí. Nutné je sledování výskytu škodlivého

softwaru, prevence přístupu na nebezpečné internetové stránky, ověřování integrity koncových bodů a kontrola využití aplikací. Typická Wi-Fi řešení však těmto nárokům nevyhovují.

### Nabídka řešení Fortinet Secure Access

Nabídka společnosti Fortinet zahrnuje infrastrukturní, integrovaná a cloudová řešení a představuje ucelenou řadu implementačních možností, které vyhoví potřebám podniků a organizací všech velikostí a oborů činnosti. Tyto tři typy řešení slouží k rozšíření nebo nahrazení stávajících síťových systémů. Vysokou flexibilitu jim dodává i možnost lokálního nebo cloudového řízení.

### Nabídka pro bezdrátovou infrastrukturu

Nabídka společnosti Fortinet pro bezdrátovou infrastrukturu spojuje lokální správu s využitím kontrolérů, otevřená aplikační zařízení a řadu vysoce výkonných interiérových i venkovních AP. Tato nabídka je ideálním řešením pro podniky, které potřebují oddělit přístupovou infrastrukturu od hlavní síťové bezpečnostní infrastruktury. Mobilním uživatelům poskytuje maximální pohodlí díky síťově řízenému roamingu. Infrastrukturní řešení nabízí vysokou míru flexibility při konfiguraci kanálů a vrstev, čímž zjednodušuje implementaci a zároveň zvyšuje výkon, segmentaci provozu a kapacitu. Na vrcholku této infrastruktury je otevřená bezdrátová aplikační platforma, která pomáhá IT vybudovat přizpůsobitelnější a otevřenější síť. Tato řada produktů je vhodná pro nasazení v malých, středních i velkých podnicích všech typů.

Nabídka integrovaných řešení společnosti Fortinet zahrnuje řadu kontrolérem řízených AP, které fungují ve spolupráci se systémem FortiGate. Vedle konsolidace všech funkcí síťového firewallu, prevence průniku, ochrany proti škodlivému softwaru, VPN, optimalizace WAN, filtrování internetového provozu a řízení aplikací do jedné platformy, FortiGate obsahuje i integrovaný Wi-Fi kontrolér. Přístupové body Fortinet lze proto připojovat přímo k zařízení FortiGate a vytvořit kompletní bezdrátové pokrytí. FortiGate je k dispozici i s integrovaným AP pod označením FortiWiFi.

Cloudové řešení Fortinet je založené na službě pro poskytování a správu cloudových zdrojů FortiCloud a nové třídě přístupových bodů řady FortiAP-S. Spojuje prvky pokročilé firewallové ochrany na okraji sítě s jednoduchostí a pohodlím cloudové správy.

### Proč prodávat Fortinet Secure Access:

- spolupráce s jedním z předních výrobců na poli síťové bezpečnosti;
- lokální obchodní i technická podpora výrobce a VAD distributora Veracomp;
- registrace obchodních případů;
- atraktivní bonusový program VAD distributora Veracomp.

### Argumenty pro koncového zákazníka:

- komplexní ochrana proti rostoucímu počtu typů útoků a dostatečný výkon vyhovující požadavkům neohrazených sítí (dnešních i budoucích);
- řešení, která pokrývají každou část infrastruktury od internetu věcí po cloud;
- integrace s širokou škálou řešení jiných dodavatelů.

-bem-