

# VPGC s.r.o.

Bezpečnost ● Datová centra ● Síťová infrastruktura ● Cloud ● Mobilita ● Služby

[www.vpgc.com](http://www.vpgc.com)

Karlovo náměstí 555/31,  
120 00 Praha 2  
Telefon: +420 212 243 062  
E-mail: office@vpgc.com

## ● OBCHODNÍ INFORMACE

IČ: 02869390  
DIČ: CZ02869390

Bankovní spojení (CZK): 5011260177/5500  
Bankovní spojení (EUR): 5011260193/5500  
Bankovní spojení (USD): 5011260185/5500

### Základní informace

Rok vzniku: 2014  
Partnerský program: ano  
Počet zaměstnanců: 7

### Podmínky pro zaslání zboží

Dopravci: DHL, Česká pošta  
Zaslání zboží na adresu koncového  
zákazníka: ano

### Značky v distribuci

Výhradní distribuce: A10 Networks, Bitglass,  
Mojo Networks  
Autorizovaná distribuce: Stormshield

### Služby s přidanou hodnotou

**Předprodejní a obchodní podpora** – vytváření nových obchodních případů pro partnery, konzultace u zákazníků, pomoc s návrhem řešení a ochrana marže.

**Poprodejní podpora** – pomoc s nasazením řešení a následným zajištěním SLA a technické podpory. Autorizována školení.

**Marketingové aktivity** – zajištění marketingové a PR komunikace, pořádání konferencí a společných akcí s partnery, pravidelné promoakce a další bonusové programy.

### Finanční služby

Pomoc při financování větších projektů (leasing, delší splatnost, speciální podmínky), možnost postoupení pohledávek.

### Další služby

Demolab a živé ukázky  
Bezplatné PoC, zápůjčky HW/SW



Produkty A10 Networks jsou dostupné jako hardwarové appliance, virtuální instance, v cloudu, ale i ve formě konteinerů. Konkurenční výhodou A10 Networks jsou zejména vysoký výkon na rackovou jednotku, velice jednoduchá all-in-one licenční politika a také otevřenost systému přes rozhraní API.

Řešení pro Application Delivery (ADC) zahrnuje funkce od tradičního load-balancingu přes pokročilý web application firewall (WAF) až po centralizovanou aplikační analytiku (APM) na úrovni jednotlivých aplikací díky Harmony Controlleru, který je možné provozovat jako SaaS nebo ve vlastním datovém centru.

Bezpečnostní oddělení musí mít přehled o provozu z a do internetu, proto rychlá a účinná analýza šifrovaného provozu (SSL insight) pomáhá k zajištění bezpečnosti ve velkých podnicích a státní správě.

AntiDDoS řešení (TPS) obsahuje jak detekci, tak mitigaci útoků na dedikovaném zařízení nebo v cloudu. Nabízí také rozsáhlé možnosti nasazení, ve vlastních datových centrech nebo u telekomunikačních operátorů.

Bezpečnostní řešení Bitglass je Cloud Access Security Broker (CASB), který zajišťuje komplexní zabezpečení moderních podnikových prostředí, na firemních a BYOD zařízeních. Poskytuje tak ochranu firmám, které používají cloudové aplikace, např. Office 365 nebo Salesforce.

Řešení dokáže v reálném čase sledovat a analyzovat aplikace, zařízení, identity a chování uživatelů napříč celým prostředím. Brání například před zneužitím přístupu nebo únikům dat (DLP) a poskytuje tzv. zero-day ochranu před novými cloudovými aplikacemi, a to díky ML a AI, které analyzují kód webových aplikací.

Bitglass dále slouží jako alternativní MDM řešení bez použití agenta na soukromých zařízeních zaměstnanců, a tím zajištění firemní bezpečnosti. Např. citlivá data budou v případě stažení na mobilní telefon zašifrována nebo maskována.

Kromě výše uvedených funkcí také pomáhá odhalovat šedé IT, tj. jaké neoficiální aplikace se ve firmě používají (př. Dropbox). U těchto aplikací je potom možné zakázat upload dat, a není tedy nutné je zcela blokovat, jak je to dnes obvyklé.

## ● PROFIL DISTRIBUTORA

### DISTINCT

Nevyhledáváme obchodní příležitosti, ale vytváříme je poradenstvím. Poskytujeme prémiovou péči a budujeme silné vztahy se zákazníky. Nebojíme se neúspěchu, každá prohra nás posiluje. Jsme proaktivní. Rosteme díky neustálému technickému vzdělávání a osobnímu rozvoji. Zastáváme názor, že uspějí pouze ti, kteří se dokážou přizpůsobit. Vážíme si naší konkurence.

### SMART

Máme velmi dobrou znalost IT trhu a rozumíme konkurenčním IT řešením. Jsme flexibilní a neustále se udržujeme mimo zónu komfortu. Každý krok si pečlivě připravíme a vyhodnotíme rizika. Naše go-to-market strategie jsou promyšleny do posledního detailu. Zaměřujeme se na nejúspěšnější systémové IT integrátory na trhu. Vzájemná důvěra s partnery patří mezi naše hlavní hodnoty.

### INNOVATIVE

Firma vznikla od nuly v době digitální transformace a nebrzdí nás staré procesy. Používáme nejnovější cloudové technologie. Jsme provozně efektivní. Korporátní zkušenosti zaměstnanců firmy, disciplína a pokora z nás dělají nejrychleji rostoucího a nejprogresivnějšího VAD na CZ/SK trhu. Neustále sledujeme trendy na globálním trhu a na základě požadavků a potřeb zákazníků rozšiřujeme portfolio výrobců.



Více se o historii společnosti dočtete v ChannelWorldu 1-2018



Mojo Networks využívá sílu cloudu, analytiky a otevřených standardů pro doručování tzv. kognitivní Wi-Fi sítě, která si zachovává vlastnosti snadné správy, vysoké škálovatelnosti, spolehlivosti z pohledu správce, nízkých nákladů z pohledu vlastníka a vysoké kvality služby z pohledu uživatele.

Kognitivní Wi-Fi vizualizuje kvalitu provozu každého uživatele a automatizuje analýzu příčin pro snadné odhalování potenciálních problémů v síti. Díky třetímu rádiu v AP je možné testovat skutečný stav Wi-Fi bez výjezdu na pobočku a také bez dalších dedikovaných testovacích zařízení.

Mojo AirTight (WIPS) zajišťuje prostřednictvím třetího rádia v AP (senzoru) rychlou a efektivní ochranu proti podvrženým AP nebo neautorizovaným klientům, např. blokadí nežádoucího provozu. Integrací s bezpečnostním systémem je možné okamžitě reagovat na nově vzniklý incident.

Správa Wi-Fi i WIPS je možná nejen z cloudu, ale i na lokální instanci, což je požadováno pro vysoce zabezpečené instalace. Samotné řízení provozu i bezpečnosti probíhá na úrovni AP, takže je controller-less a v případě výpadku spojení funguje samostatně bez managementu.



## STORMSHIELD

Evropský výrobce (bezpečnostní divize Airbus Defense & Space) zabezpečení infrastruktury vyvíjí řešení pro ochranu průmyslových podniků, IT sítí, serverů, pracovních stanic a zabezpečení dat. Přístup tzv. vícevrstvého zabezpečení zajišťuje propojenou ochranu napříč produktovým portfoliem.

Nabídka hardwarových boxů zahrnuje UTM s propustnostmi od megabitů do stovek gigabitů. Přímou v kernelu integrovaná IPS ochrana, antivírus, antimalware nebo vulnerability manager poskytují komplexní zajištění firemních centrálních i jednotlivých poboček.

Produktová řada industry UTM analyzuje průmyslové protokoly a zabezpečuje komunikaci pouze s povolenými servery a stanicemi, ostatní provoz je blokován a reportován. Toto je vlastnost, kterou oceňují hlavně průmyslové podniky i dodavatelé energií.

Technologie Stormshield drží nejvyšší evropské certifikace (EU Restricted, NATO, ANSSI EAL3+/EAL4+) a poskytuje vysoce šifrovanou VPN komunikaci mezi lokalitami, proto je vhodná nejen pro firmy všech velikostí, ale i pro veřejnou správu s důrazem na kritickou infrastrukturu státu.