

# HPE Aruba Networking Security Service Edge\*

## Příloha II: Popis způsobu zpracování

1. Popis způsobu zpracování	<p>Síťové produkty HPE Aruba Networking Security Service Edge (SSE) zpracovatele umožňuje firmám lépe podporovat moderní pracoviště prostřednictvím zabezpečeného připojení v rámci své cloudové platformy Atmos. Atmos je zkratka pro <b>Atmosphere</b>, což je platforma SSE (Security Service Edge), která nabízí moderní alternativu k tradičním technologiím zabezpečení sítě. Díky více než 350 globálním lokalitám umožňuje Atmos IT týmům snadno poskytovat koncovým uživatelům granulární přístup založený na „nulové důvěře“ k privátním aplikacím, aplikacím SaaS a internetu všude tam, kde potřebují pracovat a kde mohou pracovat, a to na základě definovaných zásad, které zohledňují roli uživatele, oprávnění, zeměpisnou polohu a další parametry.</p> <p>Platforma bezproblémově integruje řešení Atmos ZTNA, Atmos SWG, Atmos CASB a Atmos Experience do jedné cloudové platformy, která je uživatelsky přívětivá a umožňuje správu z jediného rozhraní.</p> <p>Platforma Atmos sama zajišťuje zpracování dat, neboť poskytuje uživatelům také možnost filtrování obsahu pomocí funkce prevence úniku dat a služeb ochrany proti malwaru.</p>
2. Druhy zpracovávaných osobních údajů	<p>Osobní údaje shromážděné v rámci správy sítě a souvisejících aplikací zahrnují:</p> <ul style="list-style-type: none"><li>a. MAC adresa zařízení</li><li>b. IP adresa zařízení</li><li>c. Operační systém zařízení</li><li>d. Model zařízení</li><li>e. Typ zařízení</li><li>f. Název hostitele zařízení</li><li>g. Uživatelské jméno</li><li>h. ID uživatele</li><li>i. E-mail (pokud je použit jako ID uživatele)</li><li>j. Umístění uživatele</li><li>k. Geografické umístění</li><li>l. Zobrazované jméno / členství ve skupině / titul</li></ul>

\* Řešení HPE Aruba Networking SSE bylo dříve známé a prodávané pod názvem Axis Security.

3.	Kategorie zpracovávaných osobních údajů	Správce koncoví uživatelé, zaměstnanci, dodavatelé a dočasní pracovníci.
4.	Doba zpracování	Informace shromažďované a ukládané produktem jsou minimem potřebným k zajištění bezpečného přístupu k portálu a jsou nezbytné pro plnění jeho funkce. Všechny protokoly relací o uživateli se automaticky vymažou po 90 dnech. Samotný obsah se vymaže ihned po zpracování.
5.	Technická a organizační opatření	Zpracovatel dodržuje program informační bezpečnosti pro ochranu osobních údajů správce, jak je podrobně uvedeno v příloze III níže.

## Příloha III: Technická a organizační opatření včetně technických a organizačních opatření k zajištění bezpečnosti údajů

### 1. Bezpečnostní funkce produktu:

**a. Fyzické zabezpečení:** Síťové produkty HPE Aruba Networking SSE jsou hostovány na nejrozšířenější platformě IaaS – Amazon Web Services (AWS) – která nabízí nejkomplexnější funkce zabezpečení a dodržování předpisů. AWS zavedla bezpečnostní opatření ve všech kritických oblastech včetně perimetru, infrastruktury, dat a prostředí.

**V rámci našeho programu zabezpečení cloudů každých 6 měsíců kontrolujeme příslušné zprávy od poskytovatele cloudových služeb (CSP), abychom se ujistili, že úroveň zabezpečení zůstává stejná.**

**b. Zabezpečení sítě:** Zabezpečení sítě zpracovatele zajišťuje bezpečnost fyzické a virtuální sítě, v níž se aplikace a data nacházejí. Využíváme služby a nástroje, které nabízí poskytovatel IaaS, a některá řešení třetích stran, abychom zajistili maximální zabezpečení našeho produkčního prostředí před vnějšími hrozbami a vnitřními zranitelnostmi. Zpracovatel provozuje oddělené instance interních a produkčních prostředí. Interní prostředí je zaměřeno na vývoj a testování, zatímco produkční prostředí je vyhrazeno výhradně pro naše zákazníky (Správce). Toto fyzické a logické oddělení našeho produkčního prostředí od ostatních běžících instancí nám pomáhá nabízet co nejkvalitnější nasazení softwaru pro naše zákazníky (Správce) a pomáhá zajistit, aby jejich data byla vždy omezena na jedno prostředí.

**c. Architektura a zabezpečení aplikace:** Veškerý provoz, který se vyměňuje mezi centrální aplikací a okolním světem, probíhá pomocí protokolu HTTPS přes SSL. Veškerý tok dat je šifrován pomocí šifrovací technologie AES. Různé úrovně aplikace, jako je web, aplikace a databáze, jsou navrženy tak, aby fungovaly v rámci povoleného seznamu. Mezi úrovněmi jsou povoleny pouze nezbytné a požadované komunikační cesty. Každá instance v rámci úrovně je chráněna pravidly brány firewall, aby se zabránilo neoprávněnému nebo škodlivému přístupu.

**d. Zabezpečení dat:** Veškerá výměna dat mezi aplikací a zařízeními a uživateli probíhá pomocí protokolu HTTPS. Data v klidovém stavu jsou šifrována a ukládána. Doba uchování dat je navíc přísně sledována s požadavky smlouvy a pohybuje se od okamžitého vymazání po dobu 90 dní. Data jsou pravidelně zálohována a záložní data jsou ukládána redundantně. Z organizačního hlediska máme k dispozici tým DevOps, který spravuje všechny bezpečnostní a provozní aspekty aplikace.

**e. Geografická dostupnost:** Síťové produkty HPE Aruba Networking SSE jsou dostupné na několika místech po celém světě, takže si správce může vybrat, ve kterém regionu si založí účet. Toto rozhodnutí může záviset na mnoha faktorech. Organizace může například vyžadovat, aby byla všechna data uložena v určitém regionu, nebo může stanovit regulační omezení týkající se způsobu zpracování a ukládání dat.

**Síťové produkty HPE Aruba Networking SSE jsou nasazeny v clusterech v několika regionech, které slouží především k ukládání a zpracování dat.**

Cluster pro HPE Aruba Networking SSE	Region AWS (město, kde se cluster nachází)
EU (Londýn)	Londýn, Anglie, Spojené království (eu-west-2)
Východ USA (Severní Virginie)	Severní Virginie, USA (us-east-1)
EU (Frankfurt)	Frankfurt, Německo (eu-central-1)

**Vedle toho HPE Aruba Networking SSE provozuje po celém světě několik přístupových bodů (PoP), které plní funkci prostředníků mezi vybraným regionem a aplikacemi. Tyto body PoP jsou určeny pouze pro směrování přenášených dat a neukládají žádná data. PoP je vybrán automaticky a lze jej změnit na přání zákazníka.**

HPE Aruba Networking SSE Point of Presence (PoP)	Region AWS (Město, kde se cluster nachází)
EU (Londýn)	Londýn, Anglie, Spojené království (eu-west-2)
Asie a Tichomoří (Hongkong)	Hongkong (ap-east-1)
EU (Španělsko)	Španělsko (eu-south-2)
Izrael (Tel Aviv)	Tel-Aviv (il-central-1)
Asie a Tichomoří (Sydney)	Sydney, Austrálie (ap-southeast-2)
Východ USA (Severní Virginie)	Severní Virginie, USA (us-east-1)
Asie a Tichomoří (Singapur)	Singapur (ap-southeast-1)
Asie a Tichomoří (Bombaj)	Bombaj, Indie (ap-south-1)
Jižní Amerika (São Paulo)	São Paulo, Brazílie (sa-east-1)
EU (Frankfurt)	Frankfurt, Německo (eu-central-1)
Afrika (Kapské Město)	Kapské Město, Jihoafrická republika (af-south-1)
Západ USA (severní Kalifornie)	Severní Kalifornie, USA (us-west-1)
Asie a Tichomoří (Tokio)	Tokio, Japonsko (ap-northeast-1)
Asie a Tichomoří (Jakarta)	Jakarta, Indonésie (ap-southeast-2)
Blízký východ (SAE)	SAE (me-central-1)
Milán (Itálie)	Milán, Itálie (eu-south-1)
Paříž (Francie)	Paříž, Francie (eu-west-3)
Asie a Tichomoří (Soul)	Soul, Jižní Korea (ap-northeast-2)

Texas (jižní a střední USA)	Jižní a střední USA
Iowa (střední USA)	Střední USA
Toronto (střední Kanada)	Střední Kanada

Veškeré aktivity související s konvergencí ovladače ve vybraném clusteru, včetně síťových statistik a telemetrických dat odesílaných prostřednictvím připojení HTTPS.

Veškerá data (včetně osobních údajů) odpovídající síťovým aktivitám zákazníka (tj. protokoly přístupu k webu) a veškerá další uživatelská data jsou uložena v databázích ve stejném clusteru.

— Bezpečnostní opatření:

- Zpracovatel dodržuje následující program informační a fyzické bezpečnosti pro ochranu osobních údajů správce („**bezpečnostní program zpracovatele**“):
  - Zaměstnanci a smluvní partneři jsou proškoleni o zásadách ochrany osobních údajů a zabezpečení zpracovatele a jsou seznámeni se svými povinnostmi v oblasti ochrany osobních údajů a zabezpečení. Zaměstnanci a smluvní partneři zpracovatele jsou smluvně zavázáni zachovávat důvěrnost osobních údajů správce a dodržovat příslušné zásady, normy nebo požadavky zpracovatele v souvislosti se zpracováním osobních údajů správce. Nedodržení těchto zásad, standardů nebo požadavků bude předmětem vyšetřování, které může vyústit v disciplinární opatření až do ukončení pracovního poměru nebo angažmá u zpracovatele.
- Pokud se správce dozví o incidentu narušení bezpečnosti osobních údajů, který má vliv na služby, neprodleně o tom informuje zpracovatele a sdělí mu rozsah narušení bezpečnosti osobních údajů. Oznámení se odešle centru bezpečnostních operací zpracovatele e-mailem na adresu [cloudops@axissecurity.com](mailto:cloudops@axissecurity.com)

Navštivte HPE.com

### [Zahájit chat](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Informace obsažené v tomto dokumentu se mohou změnit bez předchozího upozornění. Jediné záruky na produkty a služby společnosti Hewlett Packard Enterprise jsou uvedeny v přesně vymezených prohlášeních týkajících se záruk, která jsou dodávána s těmito produkty a službami. Ze žádných zde uvedených informací nelze vyvodit existenci dalších záruk. Společnost Hewlett Packard Enterprise není zodpovědná za technické nebo redakční chyby ani za opomenutí vyskytující se v tomto dokumentu.

Azure je registrovaná ochranná známka nebo ochranná známka společnosti Microsoft Corporation ve Spojených státech nebo dalších zemích. Všechny známky třetích stran jsou majetkem příslušných vlastníků.

a00138898CSE, Rev. 3

HEWLETT PACKARD ENTERPRISE

[hpe.com](http://hpe.com)

