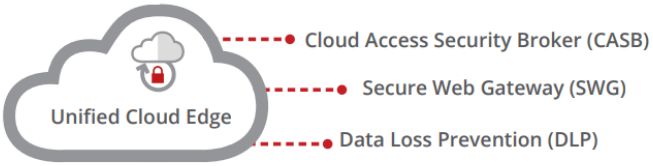
COMGUARD

Skyhigh Security

# Skyhigh Security Service Edge

## Ochrana bez perimetru

*Využívání veřejných cloudových služeb pro pracovní účely, práce z domova, nebo třeba i z kavárny či letiště. Nové možnosti pro zaměstnance s sebou však nesou nezanedbatelná bezpečnostní rizika. Díky holistickému přístupu společnosti Skyhigh dokážeme nyní zabezpečit firemní data od koncového zařízení až po cloud. Řešení Security Service Edge kombinuje technologie host DLP, Secure Web Gateway (SWG) a Cloud Access Security Broker (CASB), čímž zajišťuje ochranu uživatelských dat ve všech fázích jejich životního cyklu.*




### Skyhigh Security Service Edge

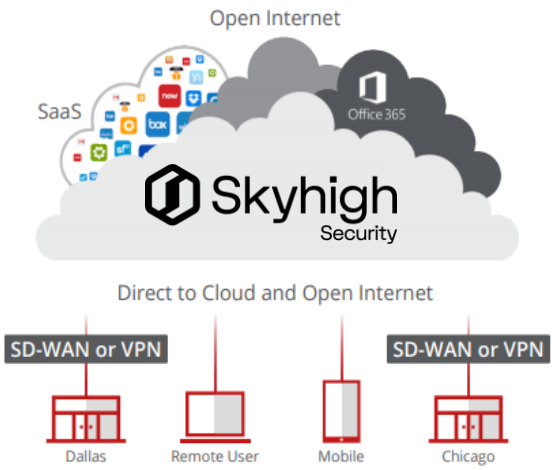
Společnost Skyhigh dokázala dokonale propojit tři pokrokové a spolu související technologie. Nový produkt Skyhigh Security Service Edge (SSE) poskytuje kompletní ochranu uživatelských dat nehledě na síťový perimetr. SSE se profiluje v nové oblasti Secure Access Service Edge (SASE), kterou společnost Gartner představila začátkem roku 2020. Díky SASE by firmy měly dosáhnout rychlé a bezpečné cloudové adaptace – tedy zajistit pro uživatele i zařízení zabezpečený přístup ke cloudovým službám kdykoliv a kdekoliv.

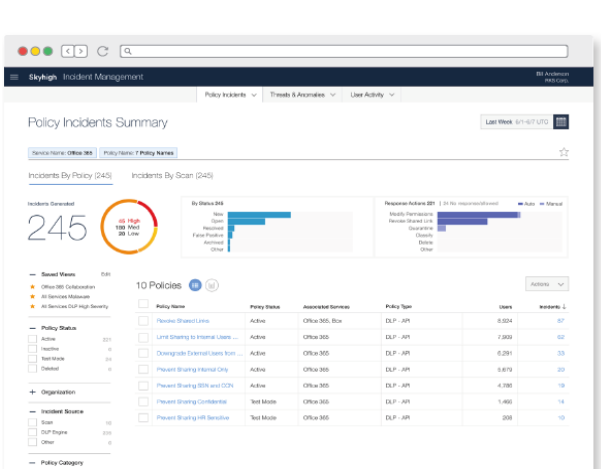
### Klíčové funkcionality

- **Jednotná nastavení** DLP politik pro CASB a host DLP
- Ochrana proti Zero-Day malware pomocí **Machine Learning algoritmů**
- Technologie **Remote browser** isolation, která zajišťuje zabezpečené prohlížení i rizikového webového prostoru
- Kontrola cloudových aplikací – možnost nahrávat či sdílet data
- Tenantní restrikce – rozpoznávají osobní cloudové účty a vynucují využití firemních (např. pro O365 atd..)

### Část I: Cloud Access Security Broker

CASB se dá přeložit také jako zprostředkování zabezpečeného přístupu do cloudu. Tato technologie vznikla jako odpověď na obavy bezpečnostních manažerů z migrace korporátních dat do cloudu. Průkopníkem CASB technologie a zároveň světovou jedničkou můžeme označit produkty **Skyhigh Security Cloud.** SH Security Cloud CASB poskytuje jednotné řešení zabezpečení, které umožňuje správcům týmů z jednoho místa detekovat rizika úniků dat, vynucovat bezpečnostní protokoly a nasazovat potřebná bezpečnostní opatření. Řešení CASB umožňuje zaměstnancům i nadále využívat cloudovou platformu, na kterou jsou již zvyklí, ale dává správcům potřebné prostředky pro sledování způsobu sdílení souborů. CASB zabraňuje úniku dat a zavádí vhled do cloudu ve smyslu detekce ukládání citlivého obsahu a evidence osob, které k tomuto obsahu mají přístup.




COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

COMGUARD

Skyhigh Security

# Skyhigh Security Service Edge

## Detekce – Ochrana – Náprava

**Funkcionality Skyhigh Security Cloud lze rozdělit do 3 kategorií:**

**Detekce** – řešení nabízí kompletní pohled do využívání cloudových služeb z pohledu nakládání s daty a přístupu uživatelů z konkrétních zařízení a lokalit, včetně podrobného auditu práce privilegovaných uživatelů.

**Ochrana** – řešení umožňuje spravovat oprávnění jednotlivých uživatelů při přístupu k datům uloženým v cloudu, chrání citlivá data pomocí šifrování a nabízí podrobný IRM (Information Rights Management).

**Náprava** – Skyhigh Security Cloud nabízí jednoduchou integraci s produkty třetích stran z oblastí DLP, SIEM, NGFW, Web Gateway, MDM a mnoho dalších. Provádí kontrolu na přítomnost malware, který má za cíl zcizení dat a podezřelé soubory umisťuje do karantény.

## Část II: Endpoint DLP

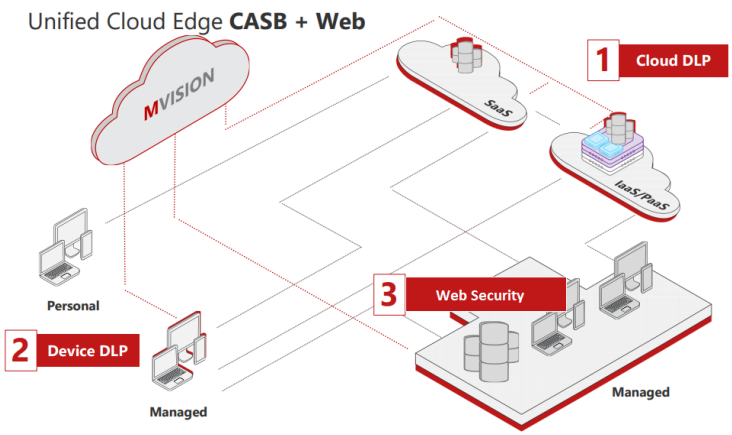
Skyhigh Data Loss Prevention Endpoint systematicky monitoruje a chrání informace před jejich neoprávněným užitím vlastními uživateli. Tímto způsobem pokrývá a zabezpečuje síťovou komunikaci (email, webmail, Instant Messaging, atd.), fyzická zařízení (tiskárny, USB zařízení aj.), peer-to-peer aplikace, trojské koně, červy, viry atp. Všechny pokusy o neautorizované přesunutí chráněných dat jsou monitorovány, reportovány a v případě potřeby blokovány – vždy na základě bezpečnostních politik společnosti. **Klasifikace citlivých dat** – řešení Data Loss Prevention Endpoint implementuje patentovaný algoritmus klasifikace obsahu, který analyzuje jak strukturovaná, tak nestrukturovaná data. Klasifikace může být například založena na umístění dokumentu na souborových serverech, dle klíčových slov a regulárních výrazů nebo dle aplikací, ve kterých byla data vytvořena.

| **Ztráta zákaznických & citlivých dat** | |
|---|---|
| • Záznamy o kreditních kartách<br>• Osobní data zaměstnanců a zákazníků<br>• Finanční data | |
| **Ztráty intelektuálního vlastnictví** | |
| • Patenty<br>• Zdrojové kódy<br>• Obchodní informace | |
| **Shoda se standardy** | |
| • ISO 27001<br>• EU Data Protection Directive | • SOX, HIPAA<br>• GLBA<br>• SB 1386<br>• Basel II |

## Část III: Secure Web Gateway

Skyhigh Web Gateway zaručí organizacím komplexní ochranu proti webovým nástrahám, poskytne patřičný vhled do využití webu v rámci organizace pomocí přehledných reportů a v neposlední řadě také zaručí vynucení organizační politiky. Díky možnosti využití cloudového nasazení mohou být uživatelé chráněni i mimo podnikovou síť.

### Architektura řešení UCE




Skyhigh uvedl nový standard proaktivní ochrany a napojil bezpečnostní brány na systém globální inteligence Skyhigh „Global Threat Intelligence" založeného na cloud computingu. Tento systém využívá patentované technologie a zpravodajské služby laboratoří Skyhigh Labs. Nejznámější je reputační technologiie Skyhigh TrustedSource s hodnocením obsahu webových stránek a zobrazující informace nejen o geografickém umístění jednotlivých webů (Geo-location).

Součástí je také nová generace skeneru, která provádí proaktivní kontrolu webového obsahu v reálném čase. Sofistikovaný Anti-malware engine dokáže odhalit jakékoli skryté útoky, viry, červy, trojské koně, přetečení zásobníku či jiné hrozby. Zároveň posuzuje chování mobilních kódů a hodnotí jejich potenciální škodlivé aktivity.

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz