COMGUARD

Skyhigh Security

Skyhigh Security Cloud

Ucelený vhled do korporátních cloudových aktivit

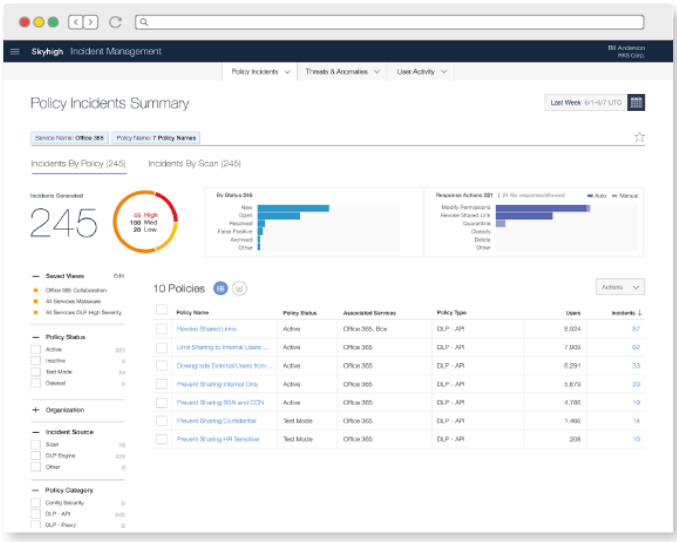
Probíhající cloudová transformace je trnem v oku celému zástupu bezpečnostních manažerů. S migrací firemních dat, nebo dokonce celé infrastruktury do cloudu je spojena řada rizik. Mezi tato rizika se řadí: ztráta přehledu o datových tocích, nedostatečné uplatnění korporátních politik, neautorizované sdílení citlivých dat, nebo kompromitace uživatelských účtů. Odpověď na tento problém nabízí Skyhigh – kompletní řešení zabezpečeného přístupu do cloudu.

Cloud Access Security Broker

CASB se dá přeložit také jako zprostředkování zabezpečeného přístupu do cloudu. Průkopníkem CASB technologie a zároveň světovou jedničkou jsou produkty **Skyhigh.** Skyhigh 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.

Klíčové možnosti využití

- Uplatnění Data Loss Prevention (DLP) politik na data uložena v cloudových platformách
- Prevence neautorizovaného šíření citlivých dat neoprávněným uživatelům
- Blokace synchronizace nebo stažení korporátních dat do soukromých zařízení
- Detekce kompromitovaných účtů, Insider Threats a malwaru
- Šifrování dat v cloudu pomocí unikátních šifrovacích klíčů
- Revize a zesílení bezpečnostního nastavení cloudových služeb
- Hodnocení rizikovosti využívaných cloudových služeb dle GDPR perspektivy (GDPR risk skóre)



Detekce – Ochrana – Náprava

Funkcionality Skyhigh lze rozdělit do 3 kategorií:

Detekce – řešení nabízí kompletní pohled do využívání cloudových služeb ať už z pohledu nakládání s daty, 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 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.

Další klíčové funkcionality Skyhigh

Guided Learning	Cloud Registry	Unified Policy Engine	Pre-Built Policy Templates
Technologie na bázi **AI machine learning** obohacena o lidský faktor poskytuje v reálném čase přehled o anomáliích detekovaných v systému.	Skyhigh disponuje světově nejrozsáhlejším registrem cloudových služeb s hodnocním **CloudTrust**, které se zakládá na 261 bodech rizikovosti.	Aplikuje jednotné politiky na všechna data (statická i v pohybu) pro zvolené cloudové služby. Politiky lze importovat z již zavedených systémů nebo nastavit nové.	Součástí jsou přednastavené šablony politik rozdělené dle: **obchodního zaměření, shody s regulacemi, typu cloudových služeb**.

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 Cloud

Technologie pro všechny druhy cloudových služeb

Skyhigh for Shadow-IT (4Shared, leteckaposta, ulozto aj.) – díky analýze proxy a firewall logů umožňuje zákazníkům získat kompletní viditelnost využití tzv. shadow-IT (cloudové služby, jejíž využití není v souladu s firemní politikou).

Skyhigh for Sanctioned IT (Office365, ServiceNow, Slack, Salesforce, Box, Dropbox aj.) – je zaměřeno na korporátně orientované cloudové služby, které jsou implementovány, nebo schváleny IT oddělením. I když tyto služby již většinou disponují nativním zabezpečením (např. MS Office 365), mnohdy tato úroveň není dostatečná pro vysoké korporátní standardy. Právě pro dosažení shody s mnoha bezpečnostními nařízeními slouží Skyhigh for Sanctioned IT, který vystuží nativní ochranu a poskytně větší kontrolovatelnost.

Skyhigh for Permitted Services (Gmail, seznam.cz, GDrive aj.) – je spolehlivá technologie určená pro kontrolu a zabezpečení všech cloudových služeb, které nejsou impelmentovány IT oddělením, ale staly se pro zaměstnance nutným standardem pro zvládání každodenních pracovních činností.

Skyhigh for Custom Apps and IAAS Services (Amazon, Azure, Google) – umožňuje zákazníkům aktivovat bezpečnostní opatření na profesionálních cloudových platformách provozující také IaaS a PaaS, (např. AWS nebo MS Azure), zákazník tak může mj. kontrolovat třeba administrátorské aktivity. Umožní i vytvářet alerty pro bezpečnostní incidenty v případě vadných konfigurací (např. S3 uložiště s veřejným přístupem).

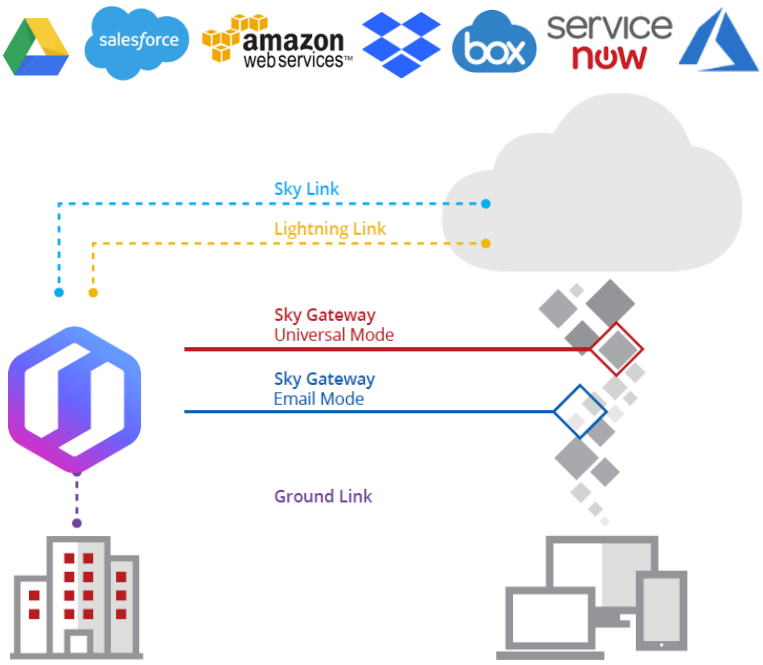
Architekura řešení

Skyhigh Sky Gateway – slouží pro vynucení politik, je nasazena v inline módu a využívá se pro tzv data-in-motion. Má dva módy, Universal a Email mód. Univerzální mód slouží k řízení provozu a pokrývá veškeré uživatele a zařízení bez nutnosti agentů. Email mód slouží buď k aktivnímu řízení nebo pasivnímu monitoringu veškerého emailového provozu, který jde přes Exchange Online.

Skyhigh Sky Link – připojuje se k API cloudové službě pro získání přístupu k datům a k uživatelské aktivitě. Slouží pro vynucení politik téměř v reálném čase pro data, která jsou nahrávána nebo sdílena.

Skyhigh Lightning Link – vynucuje politiky v reálném čase v rámci cloudových služeb

Skyhigh Ground Link – zprostředkuje spojení mezi Skyhigh a on-premise službami typu LDAP, řešení DLP, proxy, brány, firewall a služby pro správy klíčů.



Ocenění

Možnosti Integrace

- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Web Security Gateway (WSG)
- Next generation firewall (NGFW)
- Key management service (KMS)
- Access management (IDaaS)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)
- Directory services (LDAP)

COMGUARD
communication security

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