



# McAfee Skyhigh Security Cloud

## Ucelený vhled do korporátních cloudových aktivit

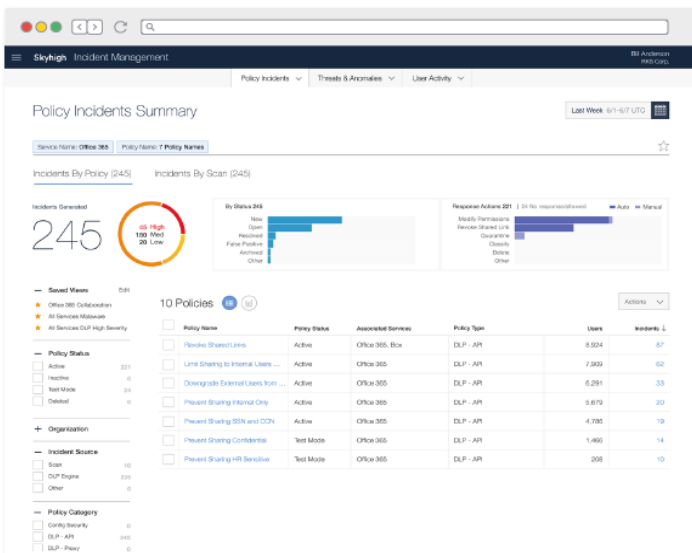
Probíhající cloudová transformace je trnem v oku celému zástupu bezpečnostních manažerů. S migrací firemních dat, nebo dokonce celé infrastruktury do cloudu je spojena řada rizik jako např. ztráta přehledu o datových tocích, nedostatečné uplatnění korporátních politik, neautorizované sdílení citlivých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

### 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 **McAfee 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 lidem.
- Blokace synchronizace nebo stažení korporátních dat směrem 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 McAfee 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** – McAfee 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 umísťuje do karantény.

### Další klíčové funkcionality McAfee Skyhigh:

#### Guided Learning

Technologie na bázi **AI machine learning** obohacena o lidský faktor – poskytuje v reálném čase přehled o anomáliích detekovaných v systému.

#### Cloud Registry

McAfee Skyhigh disponuje světově nejrozsáhlejším registrem cloudových služeb s hodnocením **CloudTrust**, které se zakládá na 261 bodech rizikovosti.

#### Unified Policy Engine

Aplikuje jednotné politiky na všechna data (statická i v pohybu) pro zvolené cloudové služby. Politiky lze importovat z již zavedených systémů nebo nastavit nové.

#### Pre-Built Policy Templates

Součástí jsou přednastavené šablony politik rozdělené dle: **obchodního zaměření, shody s regulacemi, typu cloudových služeb.**



# McAfee Skyhigh Security Cloud

## Technologie pro všechny druhy cloudových služeb

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

**McAfee Skyhigh for Sanctioned IT** (Office365, ServiceNow, Slack, Salesforce, Box, Dropbox, ..) - 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 vysoko nastavené korporátní standardy. Právě pro dosažení shody s mnoha bezpečnostními nařízeními a regulacemi slouží McAfee Skyhigh for Sanctioned IT, který vystuží nativní ochranu a poskytne větší kontrolovatelnost.

**McAfee 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 které se staly pro zaměstnance nutným standardem pro zvládání každodenního života.

**McAfee 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, nebo umožní vytvářet alerty pro bezpečnostní incidenty v případě vadných konfigurací (např. S3 uložště s veřejným přístupem).

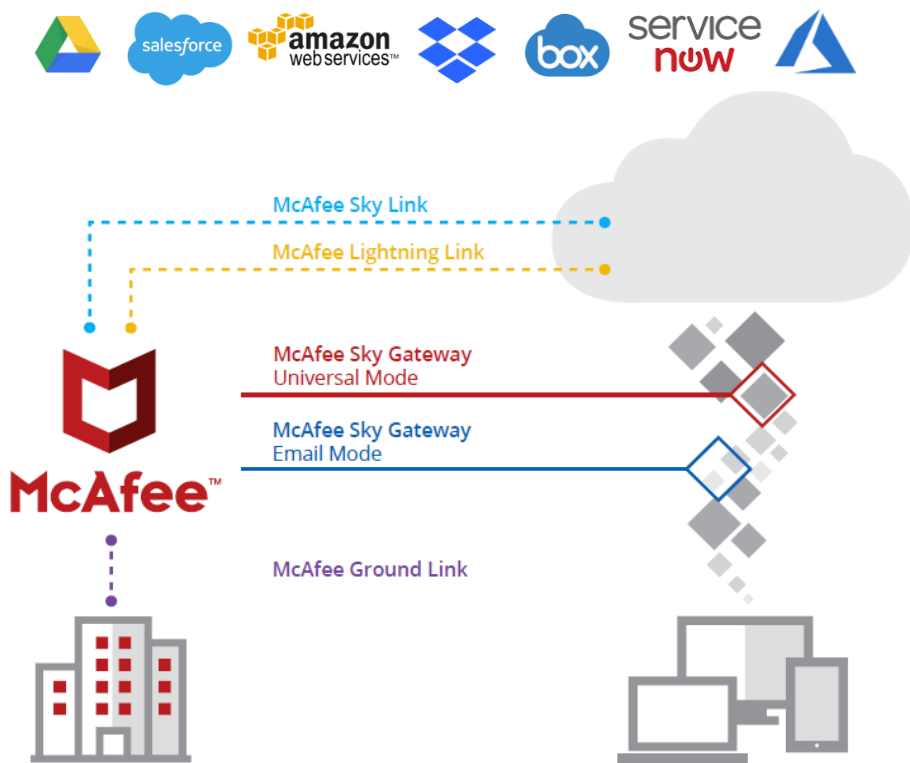
## Architektura řešení

**McAfee 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, kdy 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.

**McAfee Sky Link** – připojuje se k API cloudové služby pro získání přístupu k datům, uživatelské aktivitě. Slouží pro vynucení politik téměř v reálném čase pro data, která jsou nahrávána nebo sdílána.

**McAfee Lightning Link** – vynucuje politiky v reálném čase v rámci cloudových služeb

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



### 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)

### Ocenění:

