



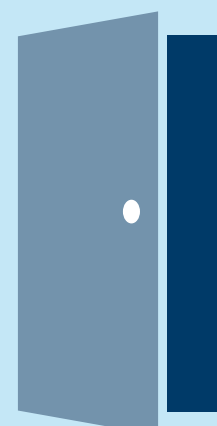
Zabezpečení Cisco Spark

Kdo má klíče od vašich dat v cloudu?

Přístupuje váš poskytovatel řešení pro spolupráci k vašim datům, brzdí vás, nebo vám dává kontrolu?

Typické firemní aplikace pro zasílání zpráv – příliš otevřené

Typické firemní aplikace pro zasílání zpráv ohrožují bezpečnost tím, že přímo přistupují k vašemu obsahu, aby mohly nabízet funkce jako vyhledávání zpráv, změna kódování obsahu nebo integrace s aplikacemi třetích stran.



Spotřebitelské aplikace pro chatování – příliš omezující

Komplexní spotřebitelské aplikace pro chatování se obvykle zaměřují na ochranu soukromí uživatelů tím, že nabízejí kompletní šifrování na úkor rozšiřitelnosti a funkcí s přidanou hodnotou.

Cisco Spark – to pravé

Cisco Spark™ nabízí to nejlepší z obojího: ucelenou, šifrovanou platformu pro spolupráci v cloudu, která umožňuje IT oddělení přistupovat k obsahu a vybírat, jaká oprávnění budou případně poskytnuta společnosti Cisco a třetím stranám.



Které řešení se hodí pro váš model zabezpečení?



Klíče máte v rukou vy.

Kompletní šifrování a zákaznická kontrola

Cisco Spark využívá otevřenou architekturu pro zabezpečenou distribuci šifrovacích klíčů, což zákazníkům umožňuje získat výhradní kontrolu nad správou šifrovacích klíčů a důvěrností jejich dat. To znamená, že obsah je šifrován na klientu uživatele a zůstává šifrován až do okamžiku, kdy se dostane k příjemci, aniž by měli nějaký prostředníci přístup ke klíčům pro dešifrování obsahu, pokud se firma výslovně nerozhodne, že takový přístup poskytne.



[Další informace >](#)

