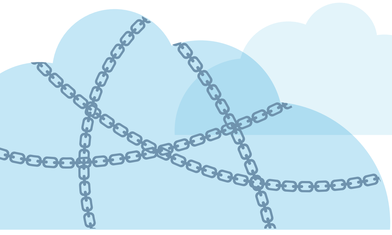
Cisco Spark

Cisco Spark security

Who holds the keys to your cloud data?
Does your collaboration provider access your content, hold you back, or give you control?

Typical business messaging apps—too open

Typical business messaging apps compromise security by directly accessing your content in order to offer features like message search, content transcoding, or integration with third-party applications.



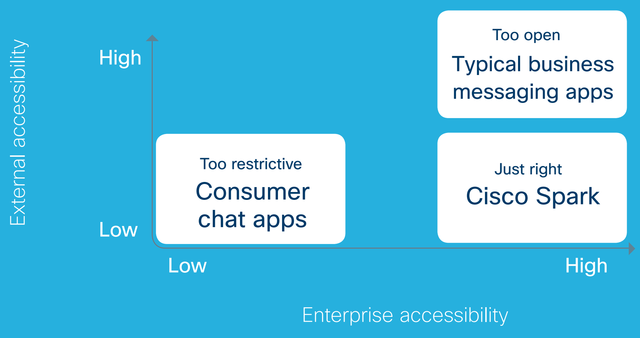
Consumer chat apps—too restrictive

End-to-end consumer chat apps tend to be geared toward protecting consumer privacy by offering end-to-end encryption at the expense of extensibility and value-add features.

Cisco Spark—just right

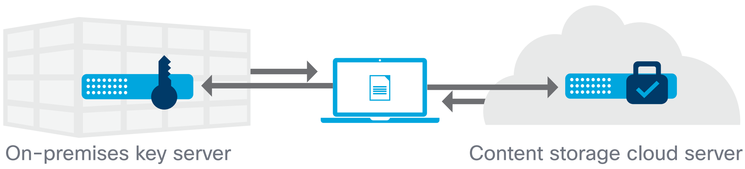
Cisco Spark™ is the best of both worlds: an end-to-end, encrypted cloud collaboration platform that gives IT the ability to access content and choose what, if any, permission is provided to Cisco and third parties.

Which fits your security model?



You hold the keys.
End-to-end encryption and customer control

Cisco Spark makes use of an open architecture for the secure distribution of encryption keys, allowing our customers to gain exclusive control over the management of their encryption keys and the confidentiality of their data. This means that content is encrypted on the user's client and stays encrypted until it reaches the recipient, with no intermediaries having access to decryption keys for content unless the enterprise explicitly chooses to grant such access.



On-premises key server

Content storage cloud server

Learn more >

CISCO