Symantec

Solution Brief

CloudSOC CASB
Security for Webex Teams

previously known as Cisco spark

Safely use Webex Teams and protect your organization and data from threats and loss.

- Are you sure your Webex Teams accounts are secure?
- How do you prevent confidential data from being broadly shared?
- Do you have protections in place to prevent the spread of malware via messages?

DID YOU KNOW?

in 2017:

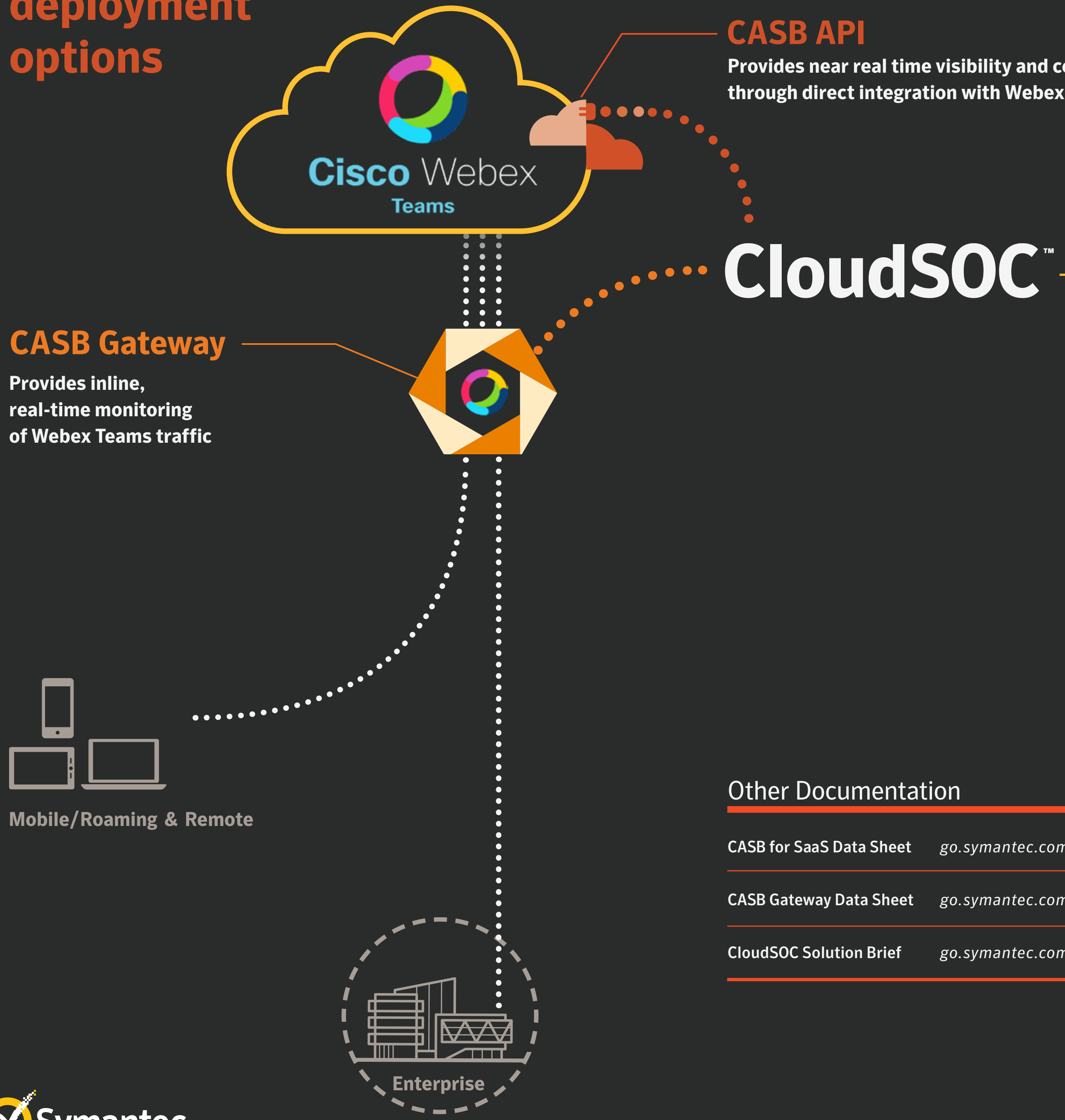
49% of cloud hacks and exploits came from messaging, file sharing, and email

18% of all PII in the cloud was overexposed

$2.8M average cost of a data breach per company

Source: Symantec 2H2017 Shadow Data Report

Multiple deployment options



CASB API

Provides near real time visibility and control through direct integration with Webex Teams

CASB Gateway

Provides inline, real-time monitoring of Webex Teams traffic

Other Documentation

CASB for SaaS Data Sheet	*go.symantec.com/casb-saas-ds*
CASB Gateway Data Sheet	*go.symantec.com/casb-gw-ds*
CloudSOC Solution Brief	*go.symantec.com/casb-sb*

Integrated Cyber Defense

CloudSOC is an integral part of the Symantec Integrated Cyber Defense Platform, which delivers multichannel protection across cloud, web, email, and endpoints—backed by the Symantec Global Intelligence Network, aggregated and distilled from Symantec products and technologies.

Data Loss Prevention

Industry-leading DLP helps protect sensitive data from loss with comprehensive detection and unified policies for cloud, web, endpoint, and data center

Malware Protection

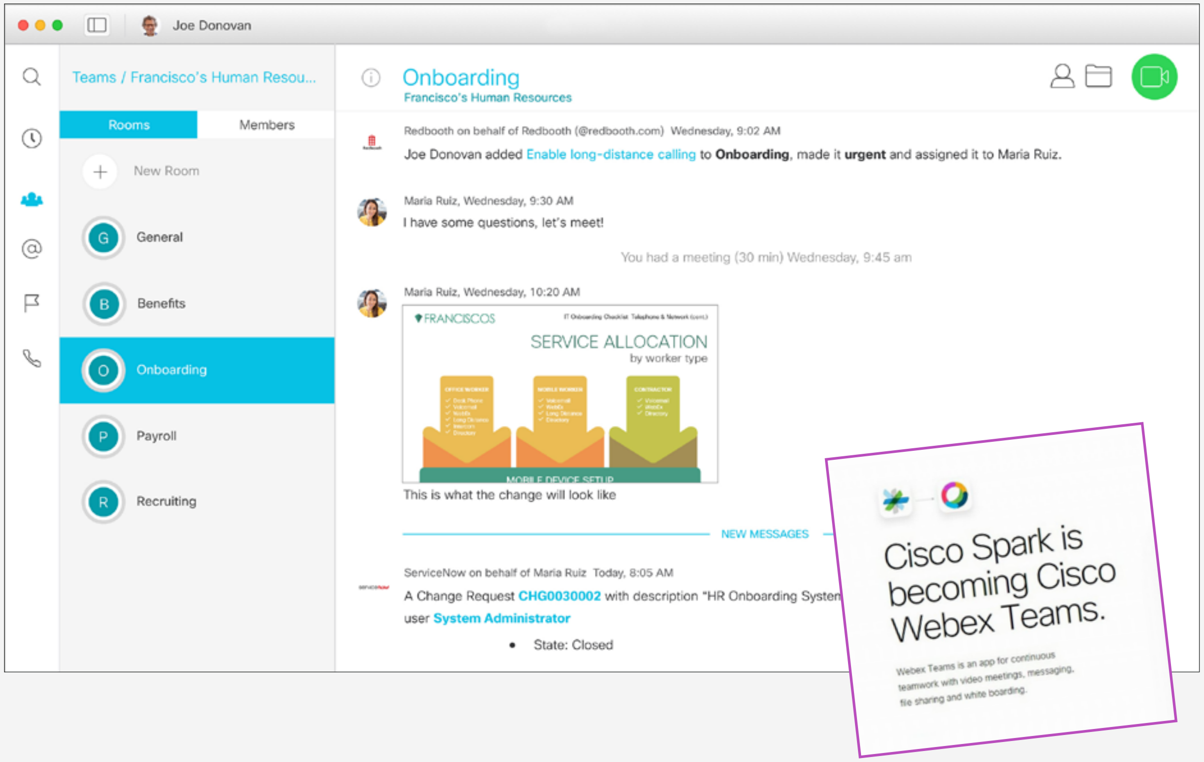
Advanced malware defense using reputation, machine learning, behavior analysis, and virtual machine-aware sandboxing

Encryption

Information Centric Encryption (ICE) enables end-to-end digital rights management

Safely use Webex Teams

With Symantec CloudSOC, you gain visibility and control over the messages, content, and actions performed in Webex Teams in spaces and by people and teams with an industry-leading cloud access security broker (CASB) solution. In CloudSOC, you can detect sensitive data and malware and use policies to automatically mitigate your risk of data loss or malware proliferation by monitoring and controlling message content and file sharing by your employees, contractors, vendors, and systems. CloudSOC is optimized to efficiently leverage Cisco Webex Teams API integration and inline controls to provide extensive and integrated security, so you can safely take full advantage of the Webex Teams platform.



Onboarding
Francisco's Human Resources

Redbooth on behalf of Redbooth (@redbooth.com) Wednesday, 9:02 AM
Joe Donovan added Enable long-distance calling to **Onboarding**, made it **urgent** and assigned it to Maria Ruiz.

Maria Ruiz, Wednesday, 9:30 AM
I have some questions, let's meet!

You had a meeting (30 min) Wednesday, 9:45 am

Maria Ruiz, Wednesday, 10:20 AM
This is what the change will look like

ServiceNow on behalf of Maria Ruiz Today, 8:05 AM
A Change Request **CHG0030002** with description "HR Onboarding System
user **System Administrator**

- State: Closed

Cisco Spark is becoming Cisco Webex Teams.

Webex Teams is an app for continuous teamwork with video meetings, messaging, file sharing and white boarding.

Detect security issues

Detect and analyze risky activity and content exposures to quickly investigate security incidents and monitor the security status of your people, teams, and spaces.

Govern sensitive data

Enforce DLP on data shared in messages and spaces in Webex Teams to protect confidential content and mitigate the risk of exposure, loss, and breach.

Protect against threats

Scan messages and content for malware, ransomware, and APTs. Dynamically identify suspicious user behavior to alert, quarantine, or block high risk actions and accounts.

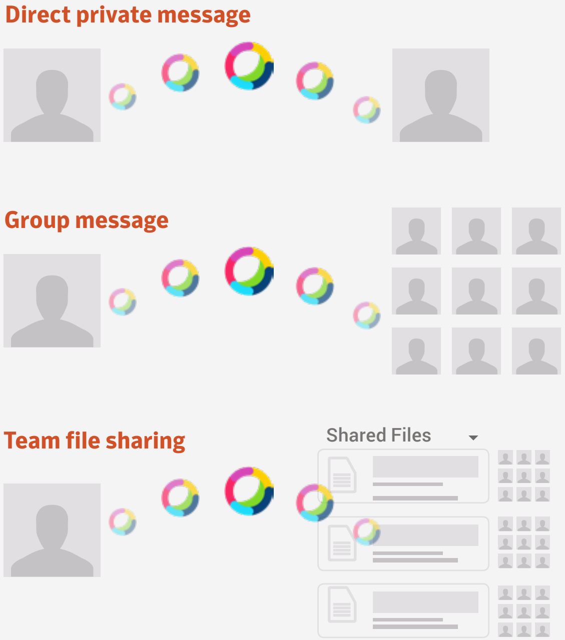
Automate policy controls

Automatically enforce security controls to quarantine or block high risk user actions, coach users, or alert admins with content-based and context-based policies.

Quickly investigate and respond to security incidents

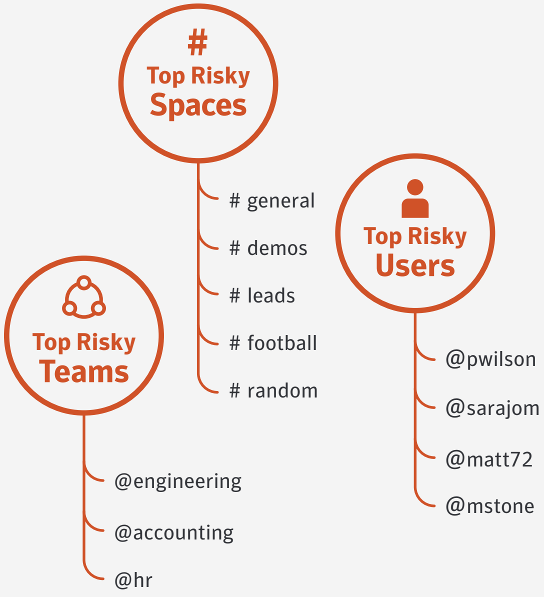
Track granular people, teams, and spaces activity and events within Webex Teams, and provide critical insights to your compliance, audit, and other internal stakeholder teams when you have a security incident. Quickly investigate a specific user or activity, correlate events across apps and accounts, and discover what really happened with powerful search and data visualization tools and dashboards or export detailed incident log files to your SIEM system for analysis.

Protect your confidential data in Webex Teams messages and attachments



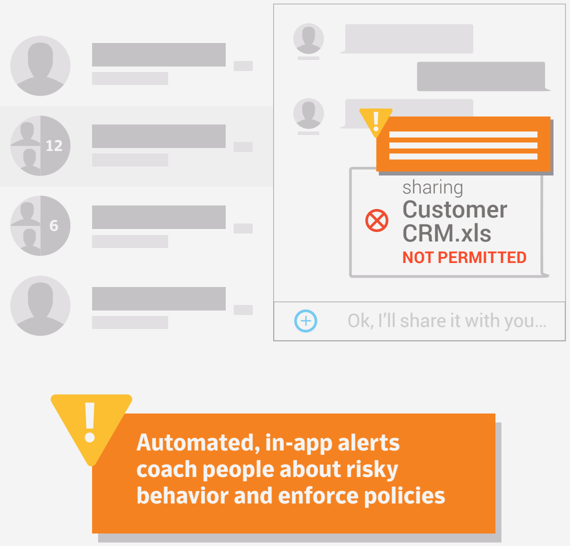
Quickly identify and mitigate risky data exposures in Webex Teams with highly accurate DLP in the cloud that scans and automatically classifies message content and attachments. Use Symantec's data science powered ContentIQ™ engine to prevent data exposures with content-aware and context-aware cloud DLP. Use event-driven policies to automate data security enforcement activities such as quarantining content for inspection, notifying users, and enforcing actions that control how sensitive data can be shared. Extend your enterprise DLP to Webex Teams by using CloudSOC integration with Symantec DLP to enforce your centralized DLP policies and workflows.

Safeguard your organization against high risk people, teams, and spaces



Automatically identify high risk people, teams, and spaces; compromised accounts; and insider threats with CloudSOC's unique data science driven User Behavior Analytics (UBA). Alert, quarantine, or block users from sharing corporate content based on their dynamic ThreatScore™. Enforce granular policies that target specific Teams or spaces. Detect elaborate data exfiltration sequences, such as a pattern of downloading content from a corporate Webex Teams space and then uploading that content to a personal collaboration app, or anomalous and repetitive messages followed by deletes of sensitive files.

Automate user coaching for safer behavior



Automated, in-app alerts coach people about risky behavior and enforce policies

Automatically alert admins and educate users on safe practices directly in Webex Teams with policy-driven CloudSOC notifications. A prompt response with coaching appearing directly in the app after a user takes a risky action can be more effective at modifying user behavior than traditional email-based notifications. CloudSOC can automatically notify users if content is quarantined for review by DLP and the result of that DLP scan. The same automated in-app notification capability can be used as a policy response to alert admins of policy violations.

Secure your Webex Teams accounts against attacks and malware

Continuously scan Webex Teams message content and attachments to remediate and prevent the proliferation of ransomware, macros, APTs, and other malware threats. CloudSOC finds threats by inspecting content and analyzing user behavior with machine learning, UBA, and industry-leading Symantec threat protection that includes advanced anti-malware and file insight reputation technologies. Effectively protect your organization from emerging threats with dynamic analysis of files using integrated Symantec cloud sandboxing.

Always know the state of your security with intuitive dashboards and reports

Easily keep track of your Webex Teams security status through an intuitive user interface that provides default and fully customizable dashboards that can show content risks and exposures in messages aggregated at people, team, and spaces views. Gain deep insights into Webex Teams activity through detailed pivot tables, charts, and graphs to visualize risks over time. Role based access controls provide admins just the right level of visibility and control. Management, compliance officers, and other stakeholders can be kept informed with regularly scheduled, customizable reports.

About CloudSOC

The Data Science Powered™ Symantec CloudSOC platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC platform deliver the full life cycle of cloud application security, including auditing of Shadow IT, real-time detection of intrusions and threats, protection against data loss and compliance violations, and investigation of historical account activity for post-incident analysis. CloudSOC provides cloud access security broker protection for a wide range of Saas, PaaS, and laaS solutions.

go.symantec.com/casb

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Where to start?

free shadow data risk assessment

Take a big step towards securing your organization's cloud usage and request a no-commitment Shadow Data Risk Assessment to uncover and classify all Shadow Data stored and shared within your team's preferred cloud apps. You'll receive access to the CloudSOC dashboard for an opportunity to see your cloud risk profile in detail and learn how to take action to stay safe and compliant.

go.symantec.com/shadow-data

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com