Cisco Webex Control Hub Extended Security Pack

Contents

Product overview 3

Data Loss Prevention (DLP) 3

Key functionality highlights 4

Anti-malware capabilities 5

Summary of features 6

Ordering information 7

Frequently Asked Questions 7

Cisco Capital 8

Product overview

Cisco Webex® connects people with each other and their work, whether you are collaborating with partners or working with your own customers. Webex delivers highly secure world-class messaging, meetings, and calling experiences from your pocket to the boardroom, to optimize and modernize employee and customer experiences.

Enterprises require controls to ensure their employees don't accidentally or intentionally send sensitive and critical information via collaboration tools. Examples of such information include intellectual property, patient records, credit card numbers, and social security numbers.

IT administrators also need to protect against malware and ransomware that may get distributed when sharing files externally or when using devices that aren't managed by their corporate IT teams.

The Extended Security Pack for Cisco® Webex Control Hub can help you protect your company's data, your partners, and your customers by bundling data loss prevention and anti-malware capabilities in an add-on Cisco Flex collaboration offer.

The Extended Security Pack provides collaboration administrators with agility and peace of mind so they can more securely deploy Webex in their enterprises by addressing all information security concerns in one tightly integrated solution.

Data Loss Prevention (DLP)

The Extended Security Pack includes the full set of functionalities from Cisco Cloudlock® for Webex Teams™. Cloudlock enables organizations to more securely adopt Cisco Webex Teams by providing full visibility and control over sensitive data stored in Webex Teams. Cloudlock identifies critical information such as Personally Identifiable Information (PII), Personal Health Information (PHI), and Payment Card Information (PCI) as well as other proprietary information to adhere to regulatory compliance and internal data protection mandates. When sensitive information is detected in violation of customer policies, Cloudlock triggers incidents and automatically takes risk-appropriate actions such as notifying end users and admins of violations and deleting violating content (file or message) from a Webex Teams space. Figure 1 is a screenshot of an incident view within Cloudlock.

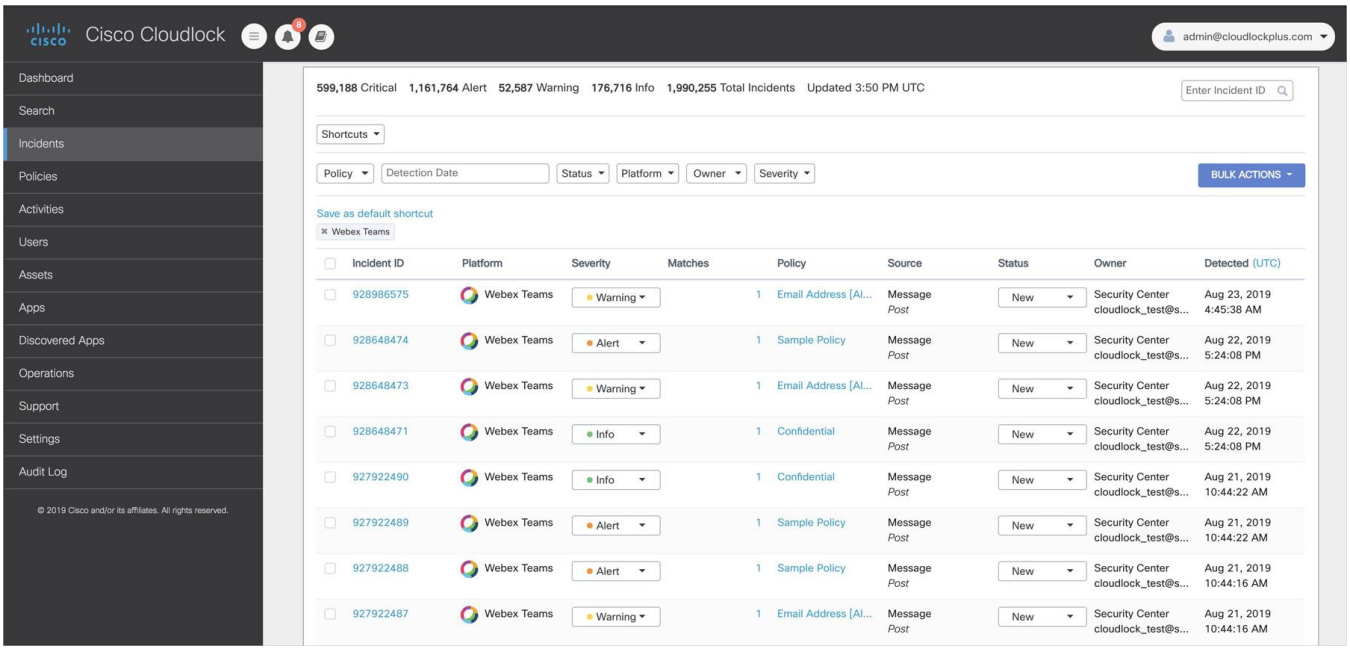

Figure 1.
Cisco Cloudlock for Webex Teams – Incident View

Key functionality highlights

Mitigate increased risk of data exposure in cloud applications

Combating data leakage in the cloud can be challenging given the collaborative nature of cloud environments and the ease with which they enable users to access, create, and share sensitive information. Organizations struggle to bridge the gap between legacy data protection tools and the limited level of visibility and control they provide within cloud environments. This is particularly true when cloud applications are being accessed by external users or remote and roaming employees who are not on the corporate network.

Identify sensitive data in cloud environments

Cloudlock continuously monitors Webex Teams environments with a powerful cloud Data Loss Prevention (DLP) engine that can identify when sensitive information stored in cloud environments is in violation of policy. With Cloudlock, security professionals enforce out-of-the-box policies focused on common sensitive information sets, such as Payment Card Industry Data Security Standard (PCI-DSS) and HIPAA compliance, as well as custom policies to identify proprietary data such as intellectual property. Advanced capabilities such as custom Regular Expression (RegEx) input, threshold settings, and proximity controls help to ensure high true positive and low false positive rates.

Mitigate risk through automated responses

Cloudlock takes cloud DLP beyond discovery by offering configurable, cross-platform, automated response actions. Through an API-driven Cloud Access Security Broker (CASB) architecture, Cloudlock supports deep, integrated response workflows that leverage the native capabilities of Webex Teams—from end user and admin notifications to the automated deletion of sensitive data. Figure 2 shows the web interface of Cloudlock's Automated Response.

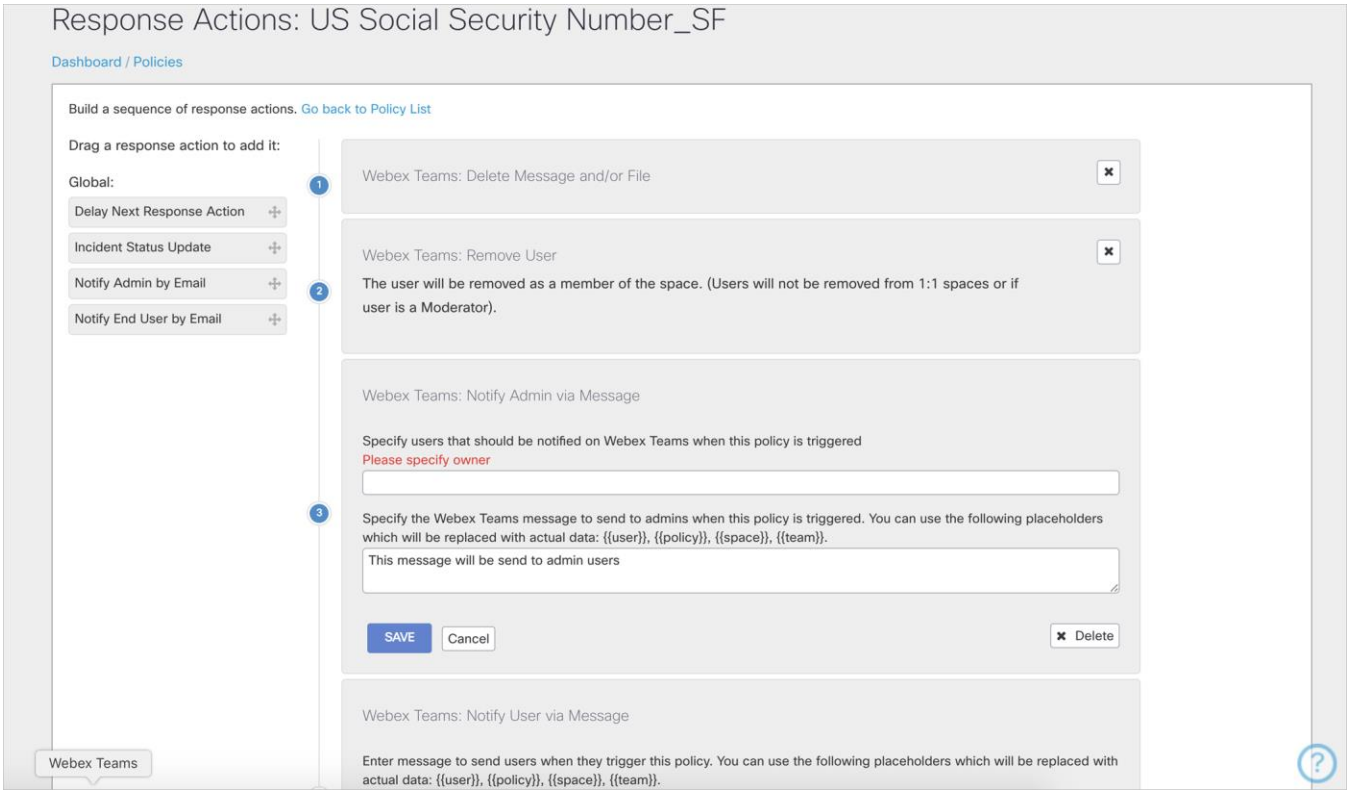

Figure 2.
Cisco Cloudlock for Webex Teams – Automated Response

Anti-malware capabilities

The Extended Security Pack includes a built-in anti-malware engine in Webex Cloud that scans all file uploads for Trojan attacks, viruses, malware, and other malicious threats. All files in spaces that you designate will be scanned and remediated, even if they are uploaded by external users. Infected files will be marked clearly and end users will not be able to download them on both corporate-managed and personally managed devices.

There is no limit on the number of files that can be scanned as part of this Extended Security Pack subscription. Figure 3 shows an instance of the Extended Security Pack blocking a file.

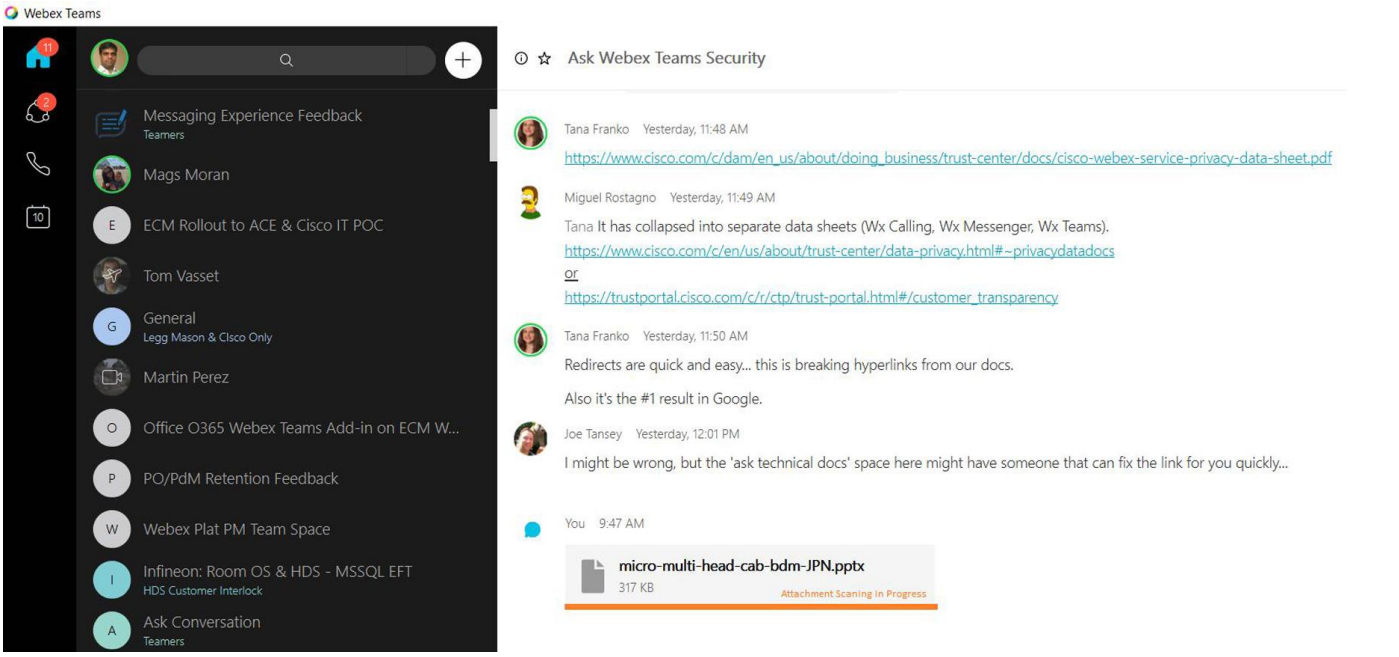

Figure 3.
Blocking an infected file

Summary of features

Table 1 summarizes the compliance features of Webex Teams.

Table 1. Compliance features

Feature	Description
Data loss prevention	Use Cisco Cloudlock to: • Gain visibility into and control over sensitive information stored in Cisco Webex Teams. Admins can leverage 80+ existing policies or create new custom policies • Mitigate the risk of cloud data leakage through powerful, automated response actions when sensitive data is discovered. When policies are violated, Cloudlock will automatically delete files or messages, notify users or admins, and remove users from spaces • Support adherence to compliance regulations within your cloud applications' security incident lifecycle directly from SIEM systems
Anti-malware	The built-in, high-performance anti-malware engine in Webex Cloud scans all file uploads for Trojans, viruses, malware, and other malicious threats. Infected files will be marked and cannot be downloaded by end users

Ordering information

The Webex Teams Extended Security Pack can be purchased within the Collaboration Flex Plan subscription (A-FLEX). See the Collaboration Flex Plan Ordering Guide for details on how to add this feature to a Collaboration Calling and/or Meetings subscription.

Table 2. Product SKUs and descriptions

PID	PID description
A-FLEX-NU-SEC-PK	Extended Security Pack NU add-on
A-FLEX-EA1-SEC-PK	Extended Security Pack EntW add-on for 250-1,999 KWs
A-FLEX-EA2-SEC-PK	Extended Security Pack EntW add-on for 2,000-9,999 KWs
A-FLEX-EA3-SEC-PK	Extended Security Pack EntW add-on for 10,000+ KWs
A-FLEX-AU1-SEC-PK	Extended Security Pack Active User add-on for 250-1,999 KWs
A-FLEX-AU2-SEC-PK	Extended Security Pack Active User add-on for 2,000-9,999 KWs
A-FLEX-AU3-SEC-PK	Extended Security Pack Active User add-on for 10,000+ KWs
A-FLEX-SEC-PK-ENT	Extended Security Pack Entitlement

Frequently Asked Questions

Q. Are Cloudlock functionality limitations in the Extended Security Pack?

A. No, the full functionality of Cisco Cloudlock is packaged in the Extended Security Pack. All you need to do is provision a compliance officer user in Webex Control Hub and have that user authorize Cloudlock for Webex Teams.

Q. If I like Cloudlock for Webex Teams, can I use it to protect my other SaaS and cloud services such as Box?

A. Yes, you can buy additional licenses for Box and other SaaS services by contacting your account team or partner. Management for all application will be done via a single console.

Q. Can I only enable DLP capabilities because I already have a malware scanner on my devices?

A. Yes, there is a Control Hub setting to enable and disable malware scans.

Q. Will malware scanning delay my file uploads and impact user experience?

A. No, the anti-malware engine has high performance and files will be scanned within a few seconds. The files will be uploaded to spaces instantly, but they cannot be downloaded or previewed until the malware scan is complete. There is no visible difference to the end-user experience.

Q. Will administrators have the option to disable and enable malware scanning for their organization?

A. Yes, administrators will have option to disable malware scanning for their organization in Control Hub.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-742773-01 12/19