Umbrella Cloud Malware Detection General Availability

Contents

Introduction

This document describes the general availability of the Umbrella Cloud Malware Detection.

Background Information

As Cisco Umbrella continues to execute on its CASB vision, Cisco is excited to announce general availability of Umbrella Cloud Malware Detection!

Malware can infiltrate organizations in many ways, a gap in existing securitysolutions in the market is cloud platforms. While files that contain malwarecannot perform actual damage in the cloud, they can once they are downloaded to the endpoint of an user.

What is Cloud Malware Detection?

The ability to detect and remediate malicious files in your sanctioned cloud applications. With the addition of this feature, security admins can investigate the reported malware - at-rest found by Cisco AMP and other Umbrella AV tools, and secure their environment by choosing to quarantine or delete those files.

Cloud Malware Detection allows organizations to:

- Safely share and support cloud transformation
- Prevent the spread of cloud malware infections
- Report on cloud malware incidents

Supported Applications

Office365, Box, Dropbox, Webex Teams, and Google (coming soon) are the supported applications.

Where in the product will I see Cloud Malware Detection?

The Cloud Malware Detection can be found in:

Reporting > Cloud Malware

Admin > Authentication (self onboarding flow)

Related Information

- Reporting documentation
- Onboarding documentation
- Demo video
- Cisco Technical Support & Downloads