Use Application Attributes in the Umbrella App Discovery Report

Contents

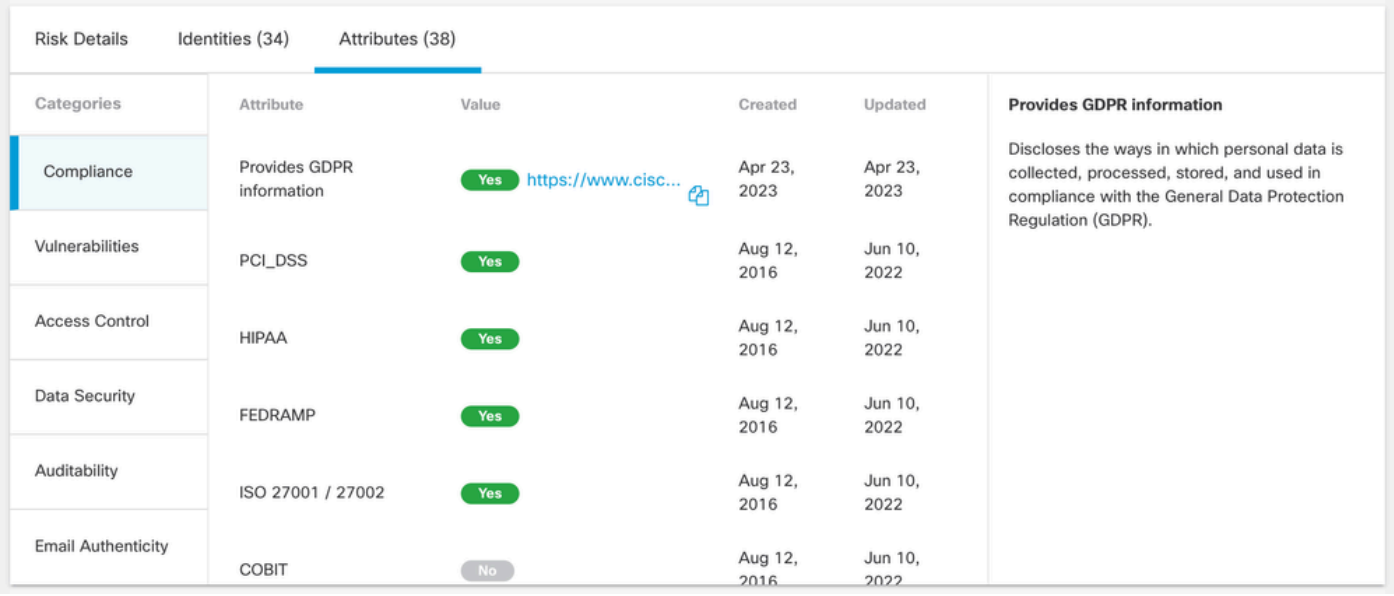
Introduction

This document describes how to use the Application Attributes feature in the Cisco Umbrella App Discovery Report.

Overview

The Application Attributes feature in the Cisco Umbrella App Discovery Report assists with risk assessment capabilities.

Application attributes significantly broaden the contextual information delivered by Cisco Umbrella for every identified app, empowering Cisco Umbrella customers to make well-informed policy decisions that align with their needs.



18263606083476

With these application attributes, Cisco Umbrella admins can build additional context on newly-discovered applications in their environment while significantly reducing the time to decide and block risky applications.

Using up to thirty-eight application attributes across six categories, Cisco Umbrella administrators possess an extensive array of supplementary insights about applications, complementing the existing risk classification. These insights encompass:

- **Compliance:** Existence of certifications like PCI-DSS, GDPR, HIPPA, and FEDRAMP for both the vendor and the application.
- **Vulnerabilities:** Known TLS/SSL vulnerabilities linked with the Application like PODDLE and BEAST.
- **Access Control:** Supported Access control mechanisms like SSO and MFA.
- **Data Security:** Data in-transit specifications like TLS version support, weak ciphers, and more.
- **Auditability:** Auditing availability.
- **Email Authenticity:** Measures to control email authenticity.

How Do I Determine if the Attributes Information Is Updated?

Each application attribute has both creation and update dates to help admins determine whether the information is relevant to their decision-making.

How Do I Access this Feature?

You can access the application attributes by navigating to **Reporting > Core Reports > App Discovery > [Application] > Attributes**.

Additional Information

Cisco Umbrella SIG Guide

Cisco Umbrella DNS Guide