OAuth 2.0: What Is It and How Does It Work?

BY DAVE WALLEN

CATEGORIES: CLOUD AND DATA SECURITY

It's no secret that data breaches can bring down businesses of any size. But what you may not know is that many of the most devastating breaches began with a single, vulnerable privileged account. According to a Black Hat survey, 32% of hackers stated that accessing a privileged account is the easiest and fastest way to steal critical data.

This is where software or SaaS solutions that use service accounts to access applications come under the scanner. These accounts entail the risky practice of storing privileged credentials, generally without multi-factor authentication (MFA). Essentially, one hack of your service account is all it takes for a data breach to occur. Despite the obvious risks involved, many vendors still use service accounts because they feel the reduced development costs outweighs the risk of customer data loss.

To avoid any chance of compromising a privileged account, security-focused applications like Spanning will provide application-level authorization leveraging the industry-standard OAuth 2.0 protocol.

What is OAuth?

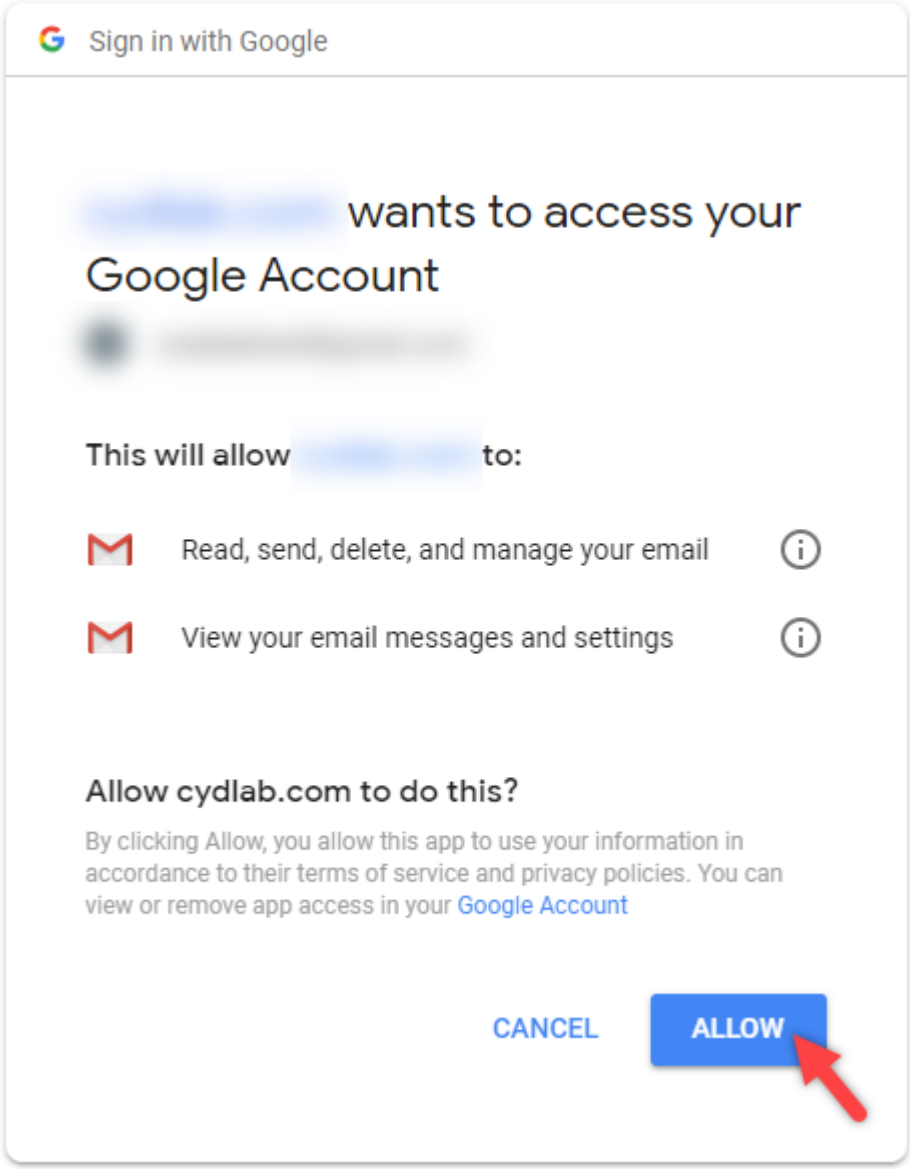


Image courtesy of ELEX.

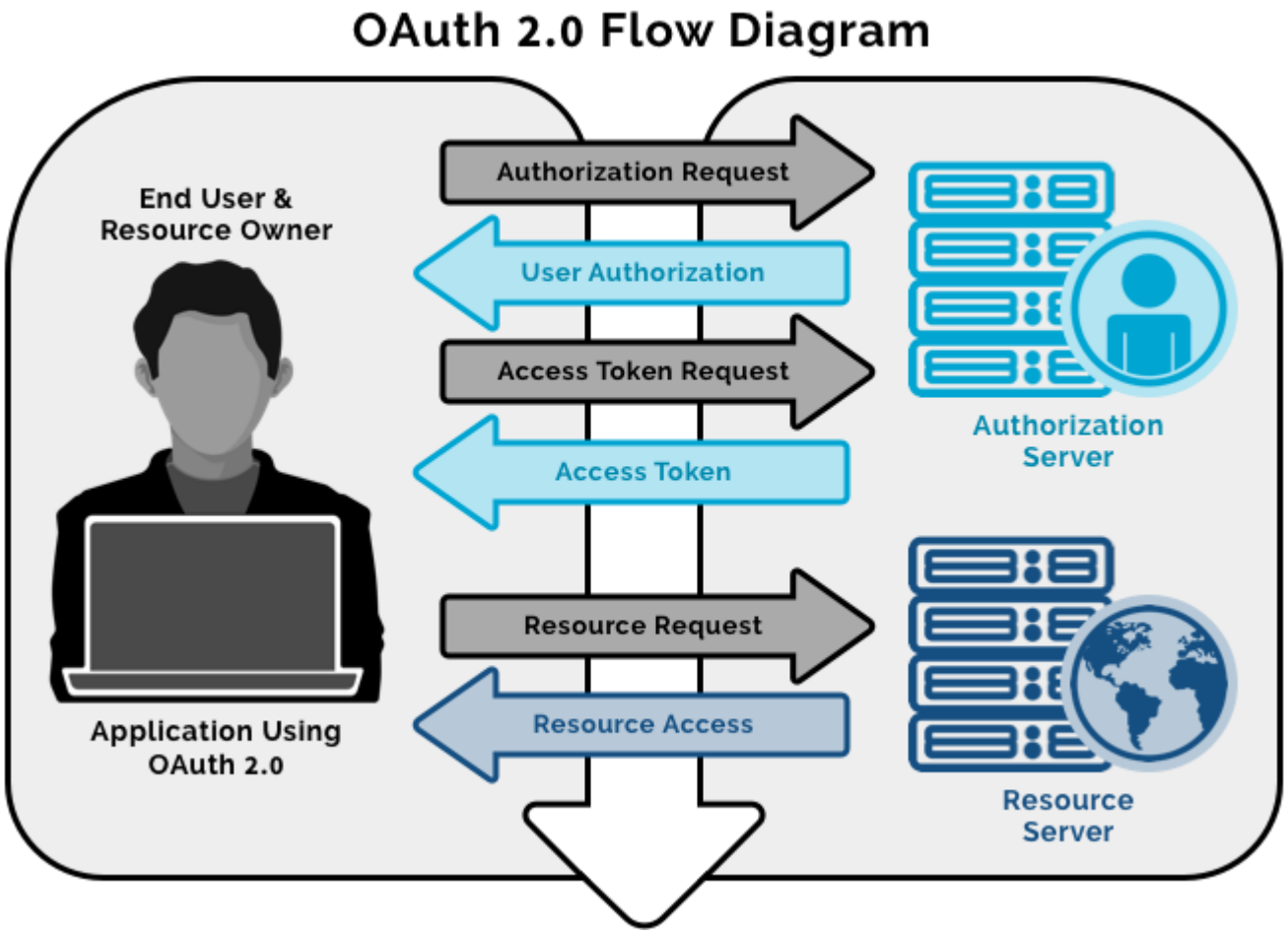
***Above**: A splash page for a Google partner service requests the user permission to use Google authentication for application access. That's OAuth 2.0 in action.*

The OAuth (open authorization) protocol was developed by the Internet Engineering Task Force and enables secure delegated access. It lets an application access a resource that is controlled by someone else (end user). This kind of access requires **Tokens,** which represent delegated right of access. That's why applications get access without impersonating the user who controls the resource.

How does OAuth work?

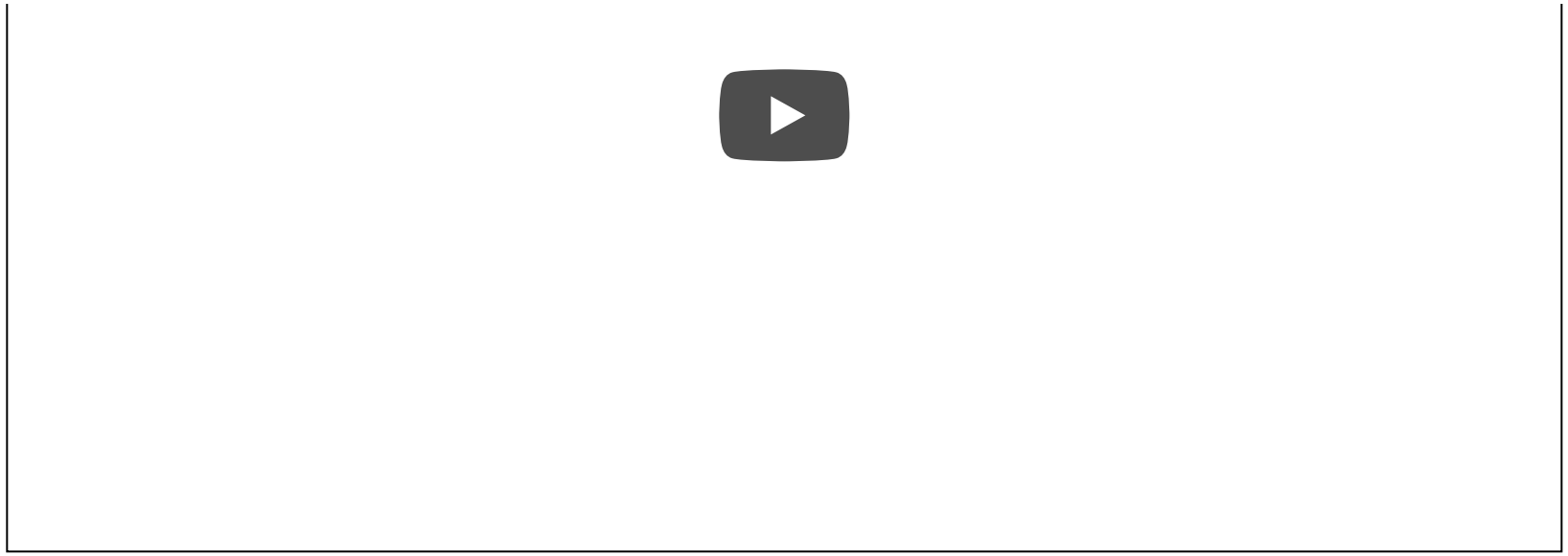
An OAuth Access Token transaction requires three players: the end user, the application (API), and the resource (service provider that has stored your privileged credentials). The transaction begins once the user expresses intent to access the API.

- **Application asks permission:** The application or the API (application program interface) asks for authorization from the resource by providing the user's verified identity as proof.
- **Application requests Access Token:** After the authorization has been authenticated, the resource grants an Access Token to the API, without having to divulge usernames or passwords.
- **Application accesses resource:** Tokens come with access permission for the API. These permissions are called scopes and each token will have an authorized scope for every API. The application gets access to the resource only to the extent the scope allows.



Watch the video below to learn more about OAuth 2.0 Access Tokens:

OAuth 2.0 access tokens explained



Why Your Backup Should Have OAuth 2.0

Many Office 365 and G Suite backup solutions use service accounts that require administrator rights and privileged credentials to access these systems.

However, a good backup solution enables OAuth data transfers to take place in Secure Sockets Layer (SSL) to ensure that the most trusted cryptography industry protocols are being used to keep your credentials secure.

While it's clear that the right backup solution keeps privileged credentials out of the reach of hackers, finding the right backup solution for your business needs can be an overwhelming task.

To help you make an informed decision before purchasing a backup solution, download our whitepaper Securing Your SaaS Backup.

Ask the right questions – find the right answers – choose the right SaaS backup.

GET THE WHITEPAPER

< PREVIOUS POST

NEXT POST >

GOT SOMETHING TO SAY?

Name

Email

Comments

SUBMIT

STAY CONNECTED

SUBSCRIBE TO BLOG

Business Email: * Email Address

*Required: The information you provide will be used in accordance with the terms of our Privacy Policy.

SUBSCRIBE

SEARCH

Search

CATEGORIES

BACKUP

CLOUD AND DATA SECURITY

CLOUD TECHNOLOGY

COMPANY NEWS

COMPLIANCE

CUSTOMERS

EDUCATION

ENGINEERING

EVENTS

G SUITE

GDPR

HEALTHCARE

INDUSTRY

OFFICE 365

PRODUCTS & NEWS FEATURES

RANSOMWARE

SALESFORCE

MOST POPULAR

OneDrive vs. Google Drive: Which Cloud Storage is Better?

READ MORE >

Google Takeout: Is It a Good Backup Option?

READ MORE >

Gmail Recovery Made Easy: Get Lost Gmail Back in Just a Few Clicks

READ MORE >

PRODUCTS

Backup for G Suite

Backup for Office 365

Backup for Salesforce

Backup for MSP

RESOURCES

G Suite

Office 365

Salesforce

Videos

GDPR

COMPANY

Careers

Contact Us

Customers

SUPPORT

Knowledge Base

Email Support

Email Security

PARTNERS

BLOG

LOGIN

Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, protecting more than 10,000 organizations from data loss due to user error, malicious activity and more.

5323 Levander Loop, Austin Texas 78702