



## Secure Access Starts with Zero Trust

As you digitize your business, you enable employees, vendors, and contractors to access any app hosted on-premises or in the cloud from their devices (managed or unmanaged).

How do you provide secure access to all users? How do you prevent attackers from using compromised credentials to access sensitive data? How do you minimize impact to user productivity when implementing additional access controls?

Organizations need secure access to all applications and data, no matter where your users are - on any device. Furthermore, managing the lifecycle of an employee's identity and the growing number of applications that an employee needs to access increases the risk of a security breach. From provisioning and deprovisioning accounts, protecting and controlling access to key functionality in the identity governance lifecycle has never been more instrumental.



# 80%

**of breaches are caused by compromised credentials and an organization must protect key assets like identity access for their employees.**

Verizon 2019 Data Breach Investigations Report

### Duo + SailPoint

With the combination of Duo and SailPoint, organizations can adopt a zero-trust methodology to securely manage, control and protect identity access by using strong authentication, device insights,

and setting access policies at the application level. This enables organizations to achieve a higher level of security posture and the peace of mind to perform their core business functions.

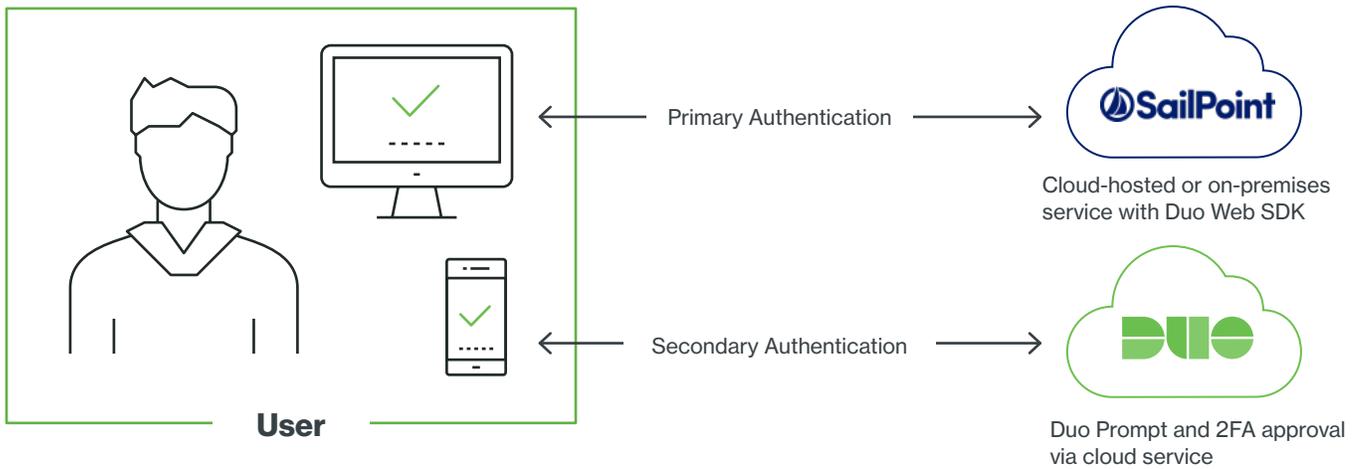
### Joint Solution Highlights

**+** Grant users secure access to all protected applications (cloud-based or on-premises) through a uniform, frictionless interface accessible from anywhere

**+** Provide the broadest, secure access across all users, devices, applications and files

**+** Improve efficiencies and lower TCO through reduced licensing costs, ease of deployment and quick time to value for employee day-one access

**+** Enforce policies to demonstrate compliance with confidence and ease



**Together, Duo and SailPoint enable organizations to securely manage and govern all users' application and data access throughout their lifecycle, from onboarding through off-boarding.**

## Features & Use Cases

- + Protect sensitive workflows and tasks by invoking step up authentication
- + Enforce additional authentication when performing password resets
- + Lifecycle management and provisioning of Duo users including administrators and end users
- + Process access requests based on organizational approval policies
- + Secure key functionality such as password reset within SailPoint
- + Device insights into identity using device posturing



**cisco** Duo Security is now part of Cisco.



Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and Zero Trust for the Workforce provider. Duo's zero-trust security platform, Duo Beyond, enables organizations to provide secure access to all of their critical applications - for any user, from anywhere, and with any device. Duo is a trusted partner to more than 15,000 customers globally, including Dresser-Rand, Etsy, Facebook, Paramount Pictures, Random House, Zillow and more. Founded in Ann Arbor, Michigan, Duo has offices in growing hubs in Detroit; Austin, Texas; San Francisco, California; and London.

Start your free 30-day trial at [duo.com](https://duo.com).

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

Visit [sailpoint.com](https://sailpoint.com)