0pass

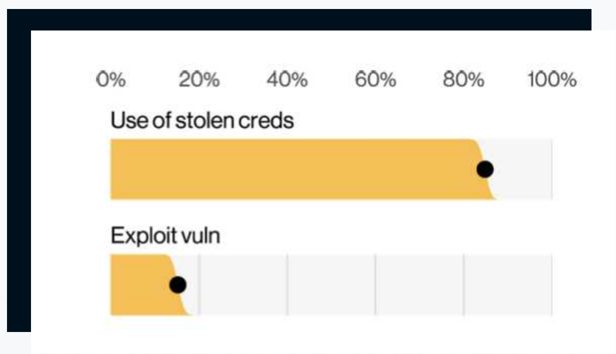
Platform Overview

Strong authentication that ends the #1 source of breaches

Stolen credentials account for over 80% of breaches[1]. Any MFA method that pushes prompts to an app or uses 6 digit codes is also vulnerable. Attackers consistently breach MFA-protected systems by stealing codes or tricking employees into verifying their MFA.

Only authentication methods like Windows Hello, Apple Face ID and Touch ID, or YubiKeys can effectively seal the front door of an account. They use private keys stored in specialized hardware modules and are compatible with phishing-resistant authentication frameworks like FIDO2 and PIV. When implemented correctly, these are impervious to theft or interception by remote attackers.

The problem is, how do you tie every system and device to these authentication methods? How do you enroll your users and integrate the management into your internal workflows?



[1] Verizon 2022 Data Breach Investigation Report

Introducing 0pass Citadel

Citadel allows you to manage biometrics and security keys for phishing and theft resistant authentication. Secure access to every app, server, and workstation with strong authentication tied to a corporate chain of trust.

Platform modules

Citadel Web

Citadel Web plugs into leading identity providers to handle authentication for web apps. Every login meets FIDO2 standards for phishing resistance and uses Windows Hello, Face ID, Touch ID, or YubiKeys.

Citadel SSH

Citadel SSH ties strong MFA to a corporate chain of trust with managed Public Key Infrastructure (PKI). It enables SSH access without deploying or managing public keys. All secrets are locked within the YubiKey's secure processor.

Citadel Workstation

Citadel Workstation brings the strongest form of multifactor authentication for OS logins that is supported natively by Windows, Mac, and Linux operating systems. Tie security keys to a corporate chain of trust with managed PKI.

Key Benefits

Employee identity tied to PKI

Managed certificates ties user identity to the private key on the YubiKey, so the right users get access to the right systems.

Zero-touch key management at scale

The entire company can implement the strongest authentication while letting 0pass handle user enrollment, certificate renewals, and managed PKI.

A smooth user experience

End users follow an easy flow to enroll their key and biometrics, update certificates when needed, and enjoy a consistent login experience that takes seconds.

Configurable integrations

Integrate with your enterprise applications to get strong authentication and proof-of-identity across your entire business.

About 0pass

0pass powers authentication that stops breaches and lateral movement. We deliver identity-centric management for strong authentication using security keys and biometrics.

0pass.com
sales@0pass.com

Key features for YubiKey authentication

An app for smooth enrollment

The 0pass App gives an easy enrollment flow for every employee—whether they're in HR or engineering. The App runs on Mac, Windows, and Linux, tying the key to the account and a corporate chain of trust.

| Citadel Web | Citadel Workstation | Citadel SSH

Users and security keys management

Manage users, their keys, and their access to enroll in different levels of trust. Admins can also configure security options like lockout thresholds for incorrect PIN attempts.

| Citadel Web | Citadel Workstation | Citadel SSH

Handles the certificate lifecycle

We do the heavy lifting for certificate issuing, management, and revocation. A security key signed by a trusted certificate authority creates a cryptographic trust between it and the accounts that it unlocks.

| Citadel SSH | Citadel Workstation

Integrates with OS subsystems

Your security key works with the smart card support inherent in Windows, Mac, and Linux to authenticate the user. This ensures compatibility across all OS versions; no need for additional software for OS logins.

| Citadel Workstation

No public keys on servers

The 0pass SSH Plugin runs when authentication is initiated. It enables the server to communicate directly with Citadel and the YubiKey.

| Citadel SSH

Tie PKI to corporate identity

When a user enrolls a YubiKey, Citadel installs a signed certificate onto the YubiKey and derives a public SSH key from it. SSH servers will check Citadel for allowed keys.

| Citadel SSH

Manage users and their access

Define the authorization for each user or user group, managing server access like you manage application access with your identity provider.

| Citadel SSH

Key features for biometrics authentication

Use a touch or a look

To access any website behind single sign-on, employees simply enter a username and use Face ID, Touch ID, Windows Hello, or a YubiKey to authenticate.

| Citadel Web

Plugs into your identity provider

Plug Citadel neatly into your identity provider, keeping all your identity management in place. Citadel does the authentication. They handle the access.

| Citadel Web

Take control of your authentication

Decide what employees can use to authenticate into corporate resources; authenticators can be added or deleted. All methods use FIDO2 standards.

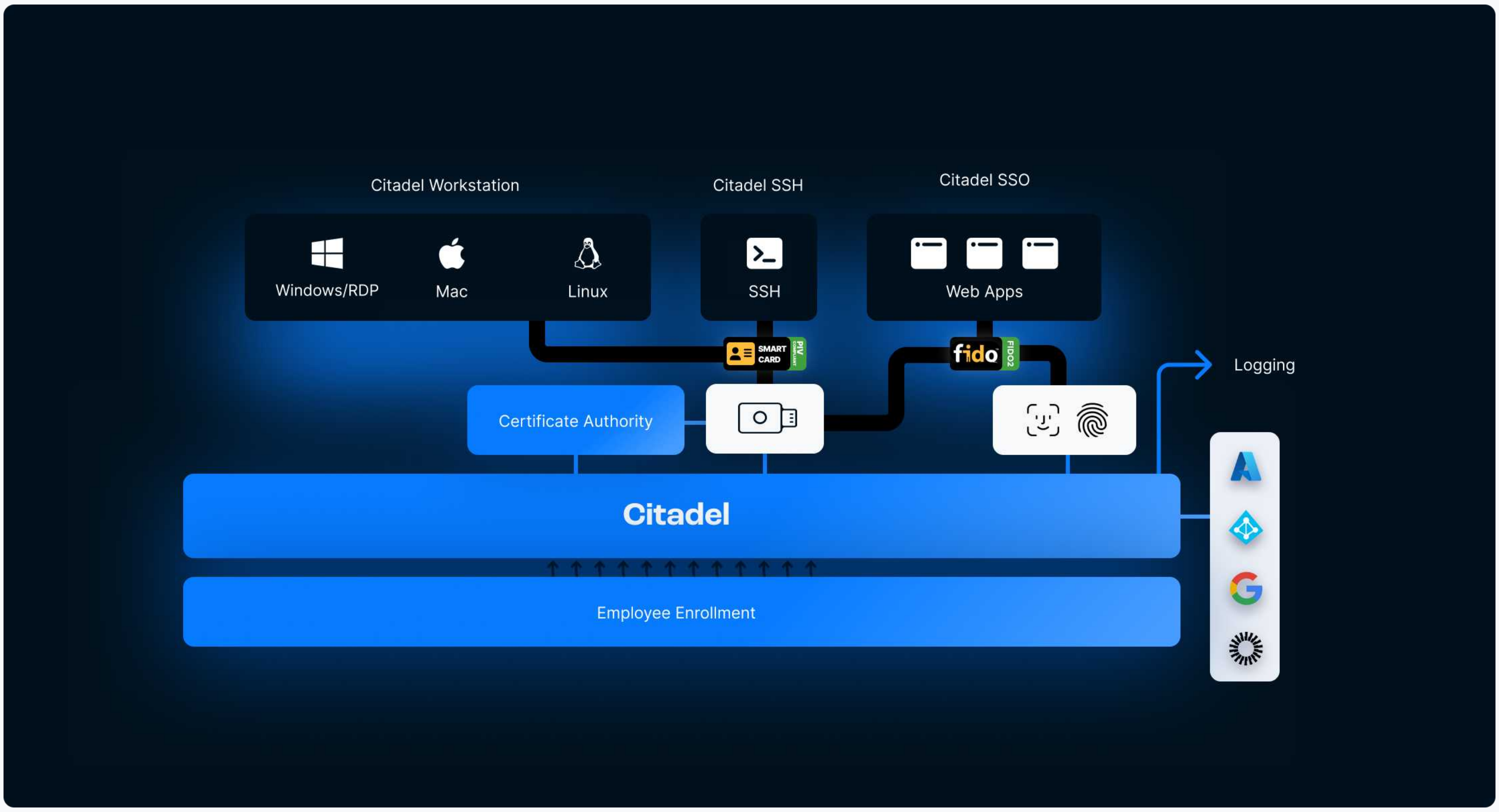
| Citadel Web

No agent, no app, no hassle

Users can easily enroll their authenticators directly in the Citadel web app. After that, they can use biometrics or a YubiKey. No additional software on devices to maintain.

| Citadel Web

0pass Citadel Platform


Citadel Workstation
Citadel SSH
Citadel SSO
Windows/RDP
Mac
Linux
SSH
Web Apps
SMART CARD
PIV
fido
FIDO2
Certificate Authority
Logging
Citadel
Employee Enrollment