ProjectX

IDENTITY & ACCESS · PILLAR OVERVIEW

One identity model for people, machines and agents.

Workforce, customer, machine and AI-agent identity in one directory, federated with the identity provider you already run and kept current from your HR system — and governed by the same policy engine that governs your tables, cameras and servers.

What it does

Phishing-resistant sign-in

Passkeys, FIDO2 security keys and push MFA with number matching, with SMS and email codes flagged as weak and restrictable by policy. People arrive by SCIM from your HR system and identity provider.

Single sign-on with what you already run

Sign in through Entra ID, Okta, Google Workspace, Ping, JumpCloud or any OIDC or SAML provider, or with an Active Directory or LDAP password. Each provider can be limited to your email domains.

Passwords and codes done properly

Passwords checked against tens of thousands of breached ones, with history and no composition rules, authenticator-app codes with backup codes, and OAuth flows for apps, services and CLIs — PKCE, client credentials, device codes, refresh and revocation.

One authorization decision point

Every permission question in every pillar goes to one engine. Write a rule once and it governs a table, a camera and a server identically — and there is no superuser flag, including for us.

Lifecycle automation

Joiners, movers and leavers driven from the directory. Offboarding produces one list across all five pillars, one approval, and a revocation certificate for your auditor.

Machine and agent identity

A service account and an AI agent are principals like anybody else — scoped, expiring, and audited under the same chain. Scopes narrow a key; they never widen the principal holding it.

How it works

01 **Sync the people you already manage** · Console
The directory fills from your HR system and identity provider over SCIM, so nobody types in a second list of people.

02 **Write each rule once** · Console
One policy engine answers every permission question across identity, data, video and cloud — a rule written once applies everywhere.

03 **Let the lifecycle run** · Audit trail
Joiners, movers and leavers flow from the directory: access is granted by role, removed on one approval, and evidenced for your auditor.

Products

Lifecycle
Day-one access. Day-zero offboarding.

Verify
Customer verification with consent, review and evidence.

Workplace
Every device managed. Every rollout pilot-first. No standing admin.

Questions buyers ask

Do we have to re-enter our people by hand?
No. The directory syncs from your HR system and your existing identity provider over SCIM 2.0, on a schedule and by delta, so the people you already manage arrive and stay current.

Does it work with Entra ID, Okta or our Active Directory?
Yes. People sign in through Entra ID, Okta, Google Workspace, Ping, JumpCloud or any OIDC or SAML provider, or with their Active Directory or LDAP password, and you can limit each provider to your own email domains.

Can services and AI agents have identities too?
Yes — a service account or an agent is a principal like anybody else: scoped, expiring, and audited on the same chain as every person.

How do we prove an access decision later?
Every permission question in every pillar goes through one policy decision point, and every answer — allow or deny — is on the append-only audit chain.

What does it cost?
The identity products carry published usage rates on the pricing page, drawing from the same credit balance as everything else.