The Path to Zero Trust — With JumpCloud

 jumpcloud ™

Zero Trust is a process, not a feature. With JumpCloud, you can build a path toward a Zero Trust security framework with a centralized solution for verifying everything from identities to networks. Read on to learn how JumpCloud offers the path of least resistance toward Zero Trust implementation — without a stack of invoices from multiple vendors.

jumpcloud ™ | **Disparate Solutions**

GO! | GO!

Verify Identity

With JumpCloud, you can create a single source of truth for identities in your organization. Enable SSO and push MFA to reduce the use of passwords and protect critical resources. Leverage conditional access to judge the security of a login and prevent unwarranted access.

- MFA
- SSH/Password
- Biometrics

Disparate: MFA — DUO, RSA, Secret Double Octopus, Idaptive, SecureAuth

Verify Device

Visualize the devices in your IT environment, regardless of where they and their users are located, with cloud-based directory + device management. Utilize JumpCloud patch management to close vulnerability gaps on schedule and ensure that your entire fleet is on the correct software version.

- MFA
- Security management policies
- Certificates

Disparate: Security management policies — Addigy, ManageEngine, Hexnode, Jamf, Kandji, Intune

Certificates — Microsoft Intune, Jamf

Verify Network

Get better visibility into your infrastructure as people come back to the office. Capture event logging and directory telemetry while making user access seamless and secure.

- Location approval/denial
- IP allow/Deny list

Disparate: Location approval/denial

IP allow/Deny list — Zscaler, Barracuda, NinjaOne

Authenticate

JumpCloud supports SAML 2.0, SCIM, and OIDC, so you can choose the protocol most relevant to your SSO use case. Utilize JumpCloud-hosted endpoints for cloud LDAP and cloud RADIUS to ensure your hybrid workforce can access necessary files, applications, Wi-Fi networks, and VPNs.

- SAML 2.0, SCIM, OIDC
- LDAP
- RADIUS

Disparate: SAML 2.0, SCIM, OIDC — Okta, Azure, OneLogin, Auth0

LDAP — Zscaler, Barracuda

RADIUS — Zscaler, Barracuda, NinjaOne

Authorize

Ensure that mission-critical data is safe and that users only access information relevant to their role and level with role-based and group-based access. Lock down confidential resources while ensuring that users have day-one access to the files and applications they need to get work done.

- Role-based access
- Group-based access
- Conditional access

Disparate: Role-based access, Group-based access, Conditional access — Active Directory, Azure AD, Okta, OneLogin