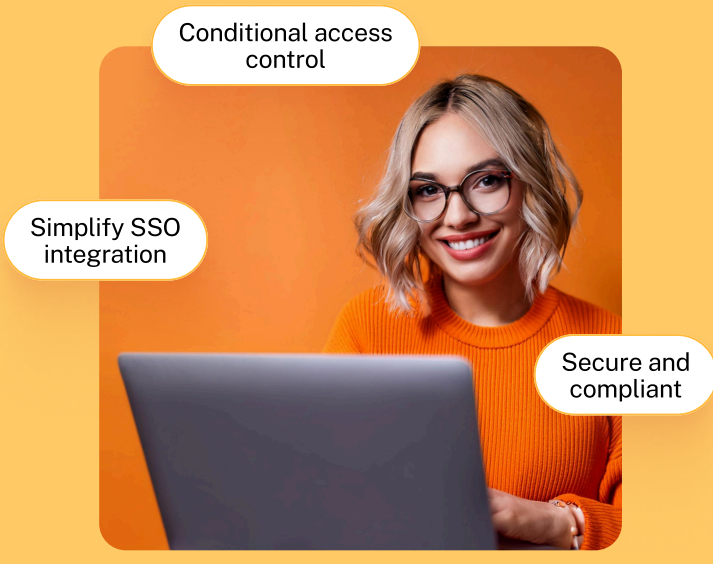


Implement conditional access with UEM-driven Zero Trust.



Traditional access controls fall short, unmanaged devices put your business at risk. Zero Trust Access verifies every user and device before granting access. Enforce digital security with UEM-driven policies and zero trust access. Verify every login through contextual signals and device authentication with Scalefusion OneIdP. Enable conditional access to ensure only compliant devices and authorized users connect. IT teams gain full control, blocking threats, reducing breaches, and securing corporate data.

Enable secure, conditional and context-driven access.




Secure device and user access, at every step.

Secure every access point with a one pane solution. Verify users, devices, and applications before granting access—eliminating security gaps to implement a zero trust model.


Verify every user & every device	Least privilege, maximum security	Smarter authentication for stronger security
Ensure only trusted users and secure devices gain access through federated authentication. No exceptions, no shortcuts.	Grant users access to only what they need. No excess permissions, no unnecessary risks.	Strengthen enterprise defenses with UEM-driven identity security. Enforce access controls, reduce digital risk, and ensure compliance.

Purpose-built features for frictionless Zero Trust Access.




Conditional SSO

One-click access with a single set of credentials. Control access based on device status, use OTP for unmanaged devices, and set app-specific conditions for users.




Device Authentication

Grant access based on context and compliance. Enforce location, IP, Wi-Fi, and time-based rules. Users log in with IdP credentials—no local passwords are needed.




User Portal for SSO

Enable employees to log in once and access all work apps through a single, secure interface. Maximize productivity and eliminate login fatigue for stronger security and control.



Just-In-Time Admin

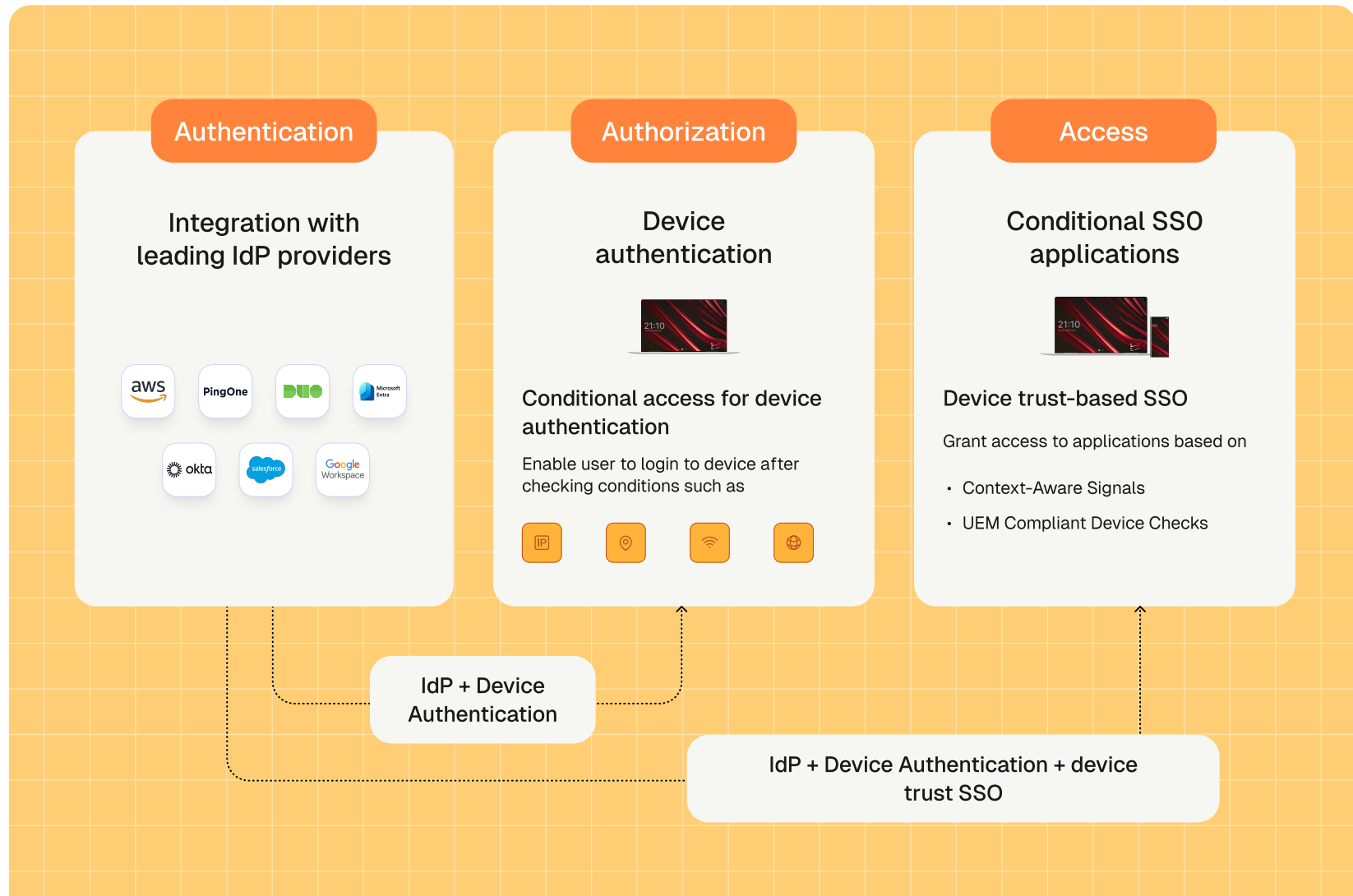
Temporarily grant admin access when needed. Automatically revoke privileges, prevent shadow IT risks, and keep track of all admin actions with detailed logs.



Federate User Identities


Centralize user management with federated identities—sync directories, enforce policies, and streamline access across your organization.

Zero Trust architecture for secure access.




With Scalefusion OneIdP	Without Scalefusion OneIdP
Secure access – Only trusted devices can open corporate emails.	Unmanaged devices can access corporate data.
Stronger login security – Every login is checked, no matter the location, network, or device.	Emails and apps are exposed to risky networks.
Smart access control – Access adjusts in real time based on security risks.	Untrusted devices create security risks.
Easy & safe logins – Single set of credentials for all apps with custom security rules.	Weak authentication with outdated security rules.
Device-aware security – Only approved devices get in.	Too many password resets and access requests.

The Scalefusion X-factor.




One pane solution built for everyone.

A powerful, intuitive hub for Admins, CISOs, CTOs, and others to manage devices with ease. Stay organized, boost efficiency, and focus on what matters—access controls.



24/6 support. Always within reach.

No downtime, no delays. Get expert assistance anytime, anywhere, with an average response time of under 5 minutes.



Seamless integration. Scalable & simple.

Transform your enterprise digital ecosystem with hassle-free migration and smooth integration, powered by Scalefusion.

Secure every access—get OneIdP today!

Contact Sales

Book a Demo