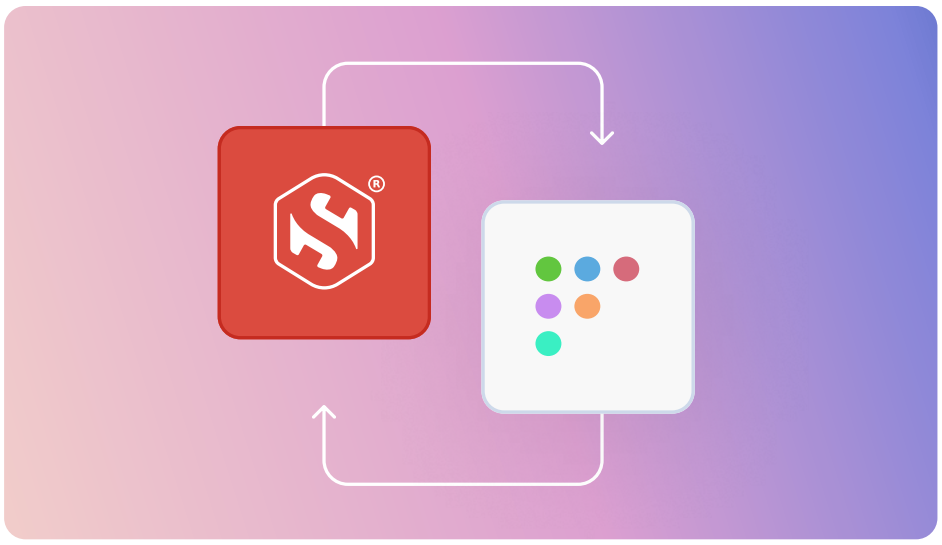
DATA SHEET

Fleet + Smallstep

Scalable Zero Trust Enforcement



Fleet offers modern, cross-platform device management: compliance, controls, software deployment, visibility and vulnerability detection all in an API-first design which can be controlled with GitOps-based configuration or the Fleet UI. Smallstep elevates that foundation with hardware-backed security. Our lightweight Fleet integration ensures that only trusted, Apple devices can successfully enroll into Fleet with ACME Device Attestation providing hardware-backed proof-of-identity.

Enrolled devices also receive non-exportable client certificates to access Wi-Fi, VPN, and other internal services securely based on this identity.

As the creator of the world's first Device Identity Platform, Smallstep brings deep expertise in PKI, certificate automation, and short-lived credentials to secure modern infrastructure. **Hardware-bound device identity is the new foundation for Zero Trust.**

When device trust is added as a security layer in your device management workflows, threats from bad actors with valid credentials can be mitigated.

Customer Benefits

Cross-OS Device Attestation

Devices enrolled and monitored by Fleet automatically receive trusted, short-lived certificates from Smallstep's agent via ACME DA workflows, ensuring authenticated, hardware-bound identity.

Enhanced Visibility & Compliance

Fleet continuously tracks device posture - OS version, patches, vulnerabilities - while Smallstep ties that data to device certificates, enabling dynamic access policies based on real-time identity and compliance status

Open & Extensible Architecture

Both platforms embrace open standards (osquery, REST, GitOps), reducing vendor lock-in and allowing customers to customize workflows, queries, and identity pipelines

Seamless Integration

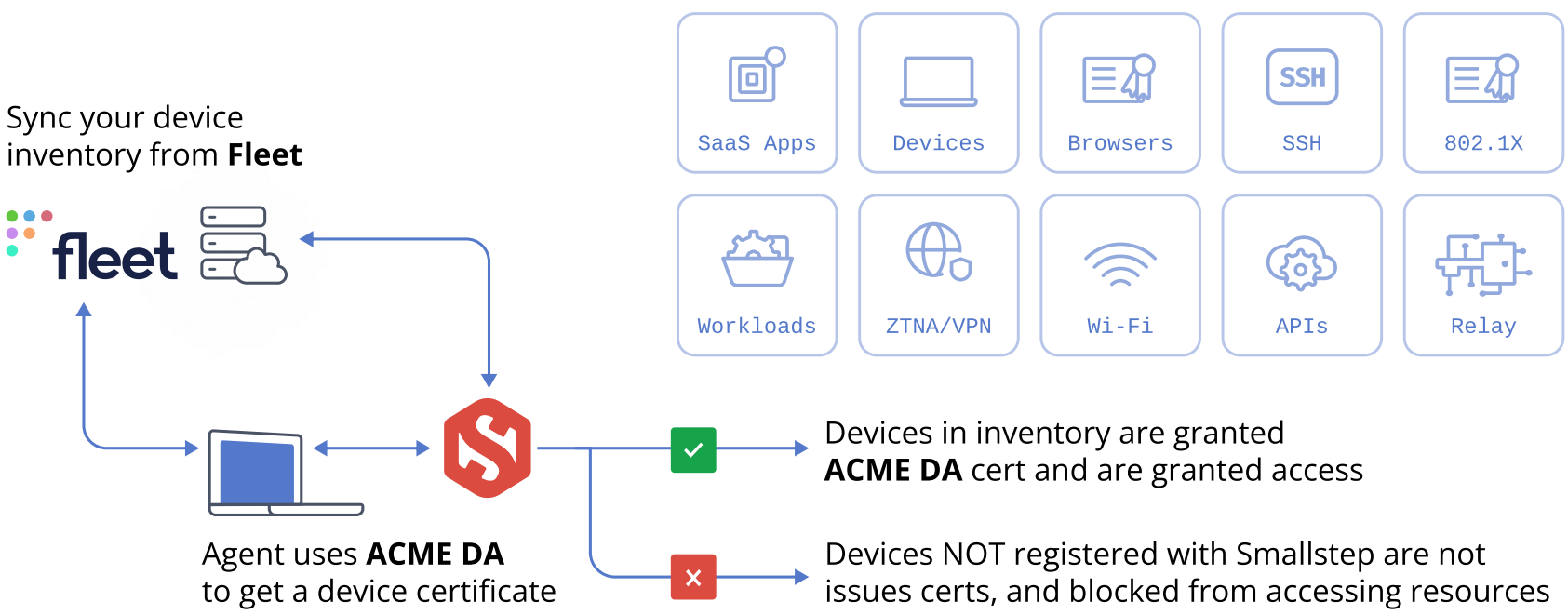
Fleet REST APIs, GitOps support, scripting, and webhook events align naturally with Smallstep's automation-first certificate issuance, enabling smooth CI/CD and fleet-wide rollouts

fleet

When **Smallstep** is added to **Fleet**, a device's hardware identity becomes an authentication factor. Instead of relying solely on shared secrets and user credentials, Smallstep silently verifies device trust, blocking unauthorized machines without adding friction for users.

Fleet provides transparent, cross-platform device management, osquery-based device visibility, vulnerability detection, compliance monitoring and GitOps orchestration empowering your teams to manage and secure devices at any scale.

Frictionless for Users
Smallstep is an invisible second factor, where the silicon is the key. Users log in from authorized devices without any additional steps - no YubiKeys to plug in, no codes to enter. Stronger security, seamless experience.



> “Smallstep and Fleet are working together to solve problems that the market simply can’t or won’t address. **The combined solution allows us to deploy Linux devices at scale as a first class (OS) citizen.**”
>
> – VP Enterprise Systems & Security

Smallstep is the world’s first Device Identity Platform™, enabling Zero Trust, certificate-based access to infrastructure, applications, and networks. Built in partnership with Apple and Google, Smallstep uses cryptographic attestation and short-lived, hardware-backed credentials to replace passwords, SSH keys, and VPN clients. By integrating with tools like Jamf, Intune, and Okta, Smallstep ensures that only trusted users on compliant devices can access sensitive systems—delivering true Zero Trust security without user friction.

smallstep