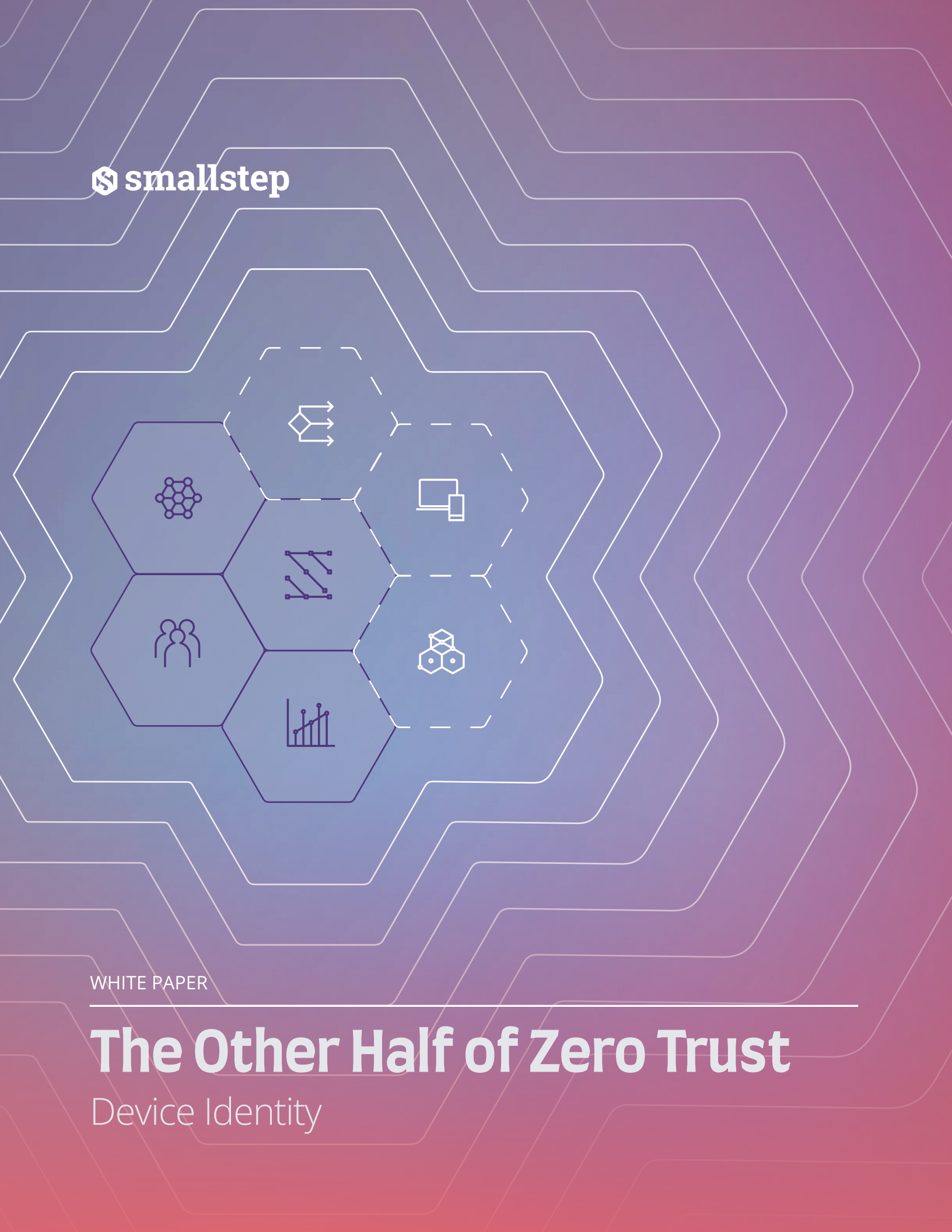
smallstep



WHITE PAPER

The Other Half of Zero Trust

Device Identity

Introduction and Background

The Rise of Zero Trust

Zero Trust is a security philosophy that states no entity (user, system, or device) is inherently trusted—every access request must be verified each time. Although the concept has been around for years, it has become a top priority for modern security architectures, especially as remote work, cloud computing, and digital transformation initiatives have expanded the potential attack surface.
Most organizations begin their Zero Trust journey by focusing on human identities—implementing Single Sign-On (SSO), Multi-Factor Authentication (MFA), and user access policies. This is critical, but it is only half the story. Each endpoint (laptop, server, container, IoT device) is also an actor in your environment that can be compromised.

The Device Blind Spot

Even the most robust user authentication (SSO, MFA, background checks) can't detect which endpoint is being used. If employees—or attackers with stolen user credentials—can log in from unverified laptops, personal gaming rigs, or ephemeral virtual machines, your Zero Trust efforts lose much of their value.
That's where Device Identity comes in: it ensures only legitimate, recognized corporate devices can initiate connections to your most sensitive resources. While it's designed to work alongside other endpoint security measures, such as device posture checks, its real strength is preventing any unknown or unauthorized device from gaining access—even if someone possesses valid user credentials.

> We thought we had a solution for device identity until we talked with Smallstep and learned about the gaps we hadn't seen.
>
> Senior Security Engineer • Enterprise SaaS Company

What is Device Identity

Device Identity helps prove that a particular endpoint is genuine and authorized to access your environment. It often involves:

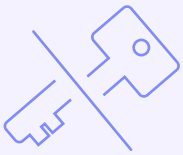
- **Hardware Identifiers:** A cryptographic certificate, secure key pair, or hardware-based token that uniquely identifies the device.
- **Trusted Inventory:** A r eal-time repository that tracks each recognized device and its current trust status (active, quarantined, retired).
- **Lifecycle Management:** Automated issuance, renewal, and revocation of device credentials so no machine retains stale or overprivileged access.
- When properly implemented, Device Identity ensures that even if an attacker steals valid user credentials, they can't log in from an untrusted or unknown machine.

Why Traditional Approaches Fall Short

Many enterprises rely on endpoint security tools like antivirus, EDR, and MDM. While these can be valuable, they frequently fail to establish a root of trust at the device level.

Common pitfalls include:

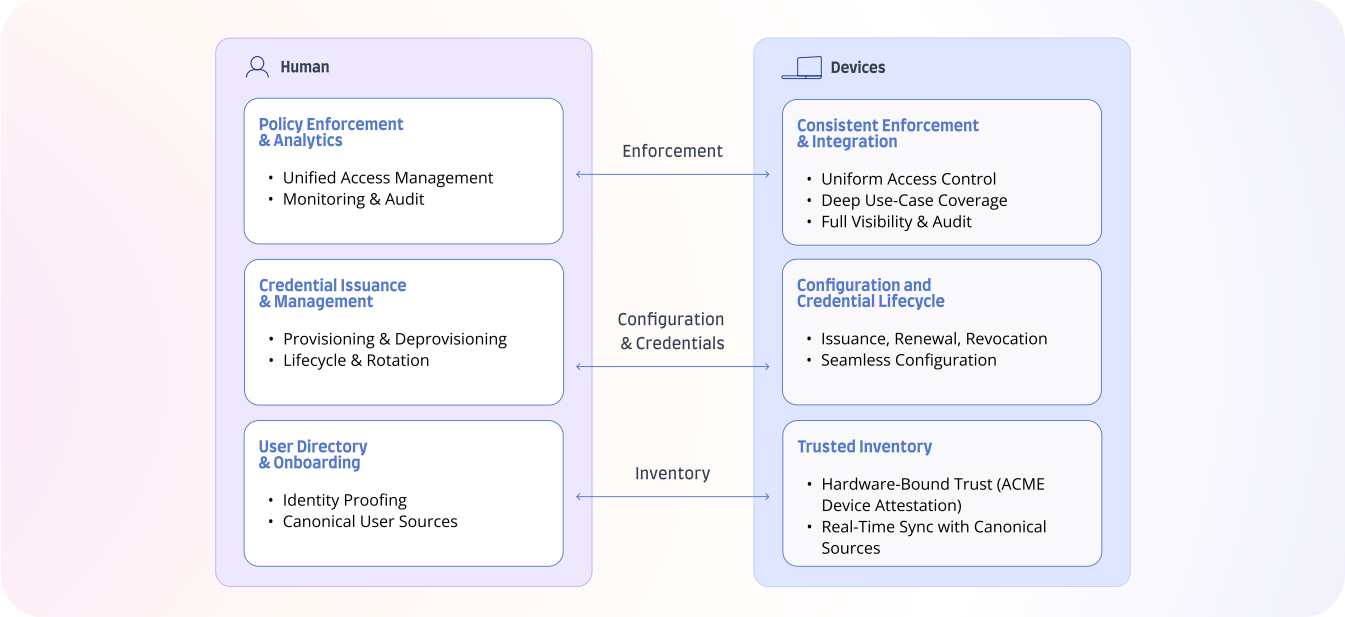
- **Disjointed Tools:** PAM (Privileged Access Management) protects privileged accounts but not everyday endpoints. MDM (Mobile Device Management) often covers only certain platforms (e.g., Windows, macOS, iOS) and may ignore Linux workstations commonly used by developers. EDR (Endpoint Detection and Response) can spot malicious activity but can't verify the authenticity of the device itself.
- **Incomplete Inventories:** IT teams frequently lack a single, real-time view of all active devices across Windows, macOS, Linux, and BYO (bring-your-own). Shadow IT or newly provisioned VMs can slip under the radar, leaving unknown or unmanaged endpoints in the environment.
- **Weak or Exfiltratable Credentials**: Password-based device logins are easily stolen or shared. SCEP (Simple Certificate Enrollment Protocol) can issue certificates but doesn't enforce a hardware-level bond, leaving them susceptible to cloning. Attackers may also exfiltrate credentials—passwords, tokens, or non-hardware-bound certificates—and reuse them for unauthorized access.
- **Limited Enforcement**: Even if some devices are tracked, identity checks might only be enforced at certain points (e.g., Wi-Fi or VPN) while ignoring other critical workflows like SSH, Git commits, or internal web apps.



Key Takeaway

If your devices cannot prove they're genuinely part of your trusted fleet, your Zero Trust model has a critical gap.

The Two Halves of Identity



Key Principles of a Zero Trust Device Strategy

- **Continuous Verification:** Trust must be established and revalidated at every step. If a device is compromised or decommissioned, its access rights should immediately reflect that change.
- **Hardware-Based Attestation:** By binding device credentials to a hardware root of trust—such as TPM chips or Apple's Secure Enclave—you drastically reduce the potential for cloned credentials or spoofed certificates.
- **Short-Lived Certificates:** Renewing certificates on a frequent schedule ensures that if an attacker does manage to obtain a credential, it becomes useless within a short window.
- **Integrations with Enforcement Points:** Consistent device checks must be enforced across all access channels—from VPN and Wi-Fi to SSH and web apps—to avoid blind spots in your security posture.
- **Real-Time Inventory:** A single source of truth for all corporate-owned machines—automatically updated by MDM, ITAM, or supply-chain integrations like Intel TSC, Apple Business Manager (formerly DEP), or Windows Autopilot—gives security teams immediate visibility into which devices can be trusted.

Smallstep's Approach to Device Identity

Trusted Inventory with ACME Device Attestation

Smallstep uses ACME Device Attestation to issue cryptographic certificates tied to hardware roots of trust. This process ensures each laptop, server, or VM is uniquely and verifiably yours, not just a random machine using a stolen credential.

- **Canonical Sources:** We automatically sync data from your MDM, ITAM, or Intel TSC to keep track of the real-time device landscape.
- **Hardware Binding:** When a device requests a certificate, Smallstep ensures the certificate is anchored in hardware-level identity.

Automated Credential Lifecycle

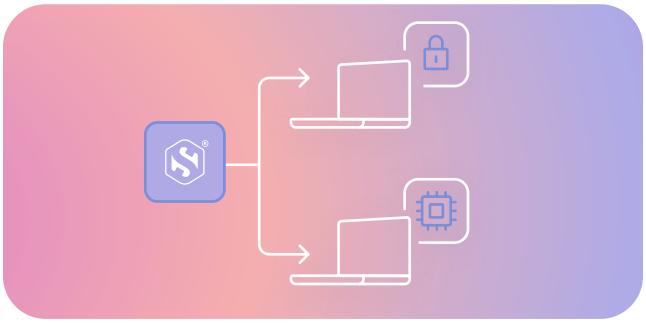
- **Issuance:** Each device receives a short-lived certificate upon successful attestation.
- **Renewal & Revocation:** Certificates regularly rotate behind the scenes, and revocation can happen immediately if the device is lost or compromised.

Configuration & Enforcement

- **Seamless Deployment:** Smallstep integrates with your environment—SSH, Wi-Fi, RADIUS, VPN, Git—so devices automatically present valid certificates when requesting access.
- **Consistent Policy:** Every resource that requires a device identity check uses the same underlying set of credentials. If a device is no longer trusted, it's locked out of all sensitive systems simultaneously.

Visibility and Audit

- **Centralized Audit Logs:** Security teams can see immediately which device accesses what and can easily pinpoint anomalous usage.
- **Extensible Framework:** As new device types appear (IoT sensors, containerized workloads), you can integrate them into this same platform.



Use Cases and Examples

Secure Developer Environments

Challenge: Engineers often have local development machines. How do you ensure code commits come only from approved corporate devices?

Solution: Each developer laptop receives a hardware-bound certificate. Git servers reject any commit attempt without a valid device certificate.

Unified Access for Remote Workforce

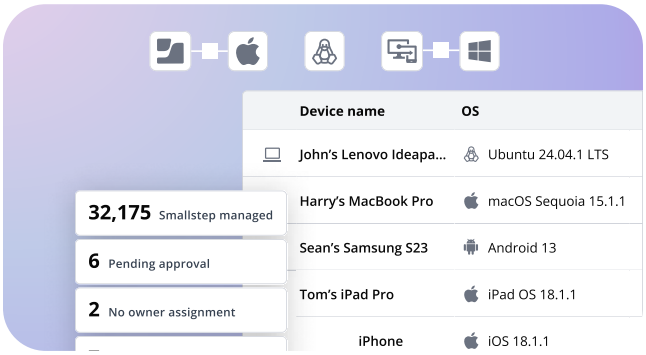
Challenge: Your teams use VPN, Wi-Fi, and web apps from many locations. BYO devices add complexity. How do you ensure that connections are limited to approved corporate devices?

Solution: Only devices with short-lived attested certificates gain access, guaranteeing remote sessions originate from genuine corporate endpoints.

Multi-Platform Fleet Management

Challenge: You have Windows, macOS, and Linux systems, plus ephemeral cloud instances. How do you get certificates and configuration to devices not in MDM?

Solution: Smallstep's platform issues certificates to every OS, plus containerized apps, ensuring each machine can authenticate seamlessly.



Conclusion and Next Steps

Completing Your Zero Trust Journey

Zero Trust is more than user authentication. It's about verifying everything: people, devices, and even the applications or services they run. Without a robust Device Identity strategy, your environment remains vulnerable, especially with remote work and cloud adoption on the rise.

Key Takeaway

- Device Identity prevents unauthorized hardware from accessing your network, even if a malicious user has valid credentials.
- Short-lived certificates anchored at the hardware level mean attackers can't simply clone or steal a device identity.
- Integrating device checks with your existing security stack (SSO, ZTNA, PAM, IAM) extends Zero Trust to every corner of your organization.

How Smallstep Can Help

Smallstep's solution automates hardware-based certificate enrollment for every device, ensuring consistent device trust and enforcement across all resources. Our goal is to simplify your transition to a complete Zero Trust architecture—covering both human and device identities—so you can focus on growing and innovating with confidence.

Ready to See It in Action?

Contact us at smallstep.com to schedule a personalized demo or proof of concept and learn how you can secure **the other half of Zero Trust** once and for all.

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.