BYOS

Make your network invisible

Byos Edge Trust



Outline

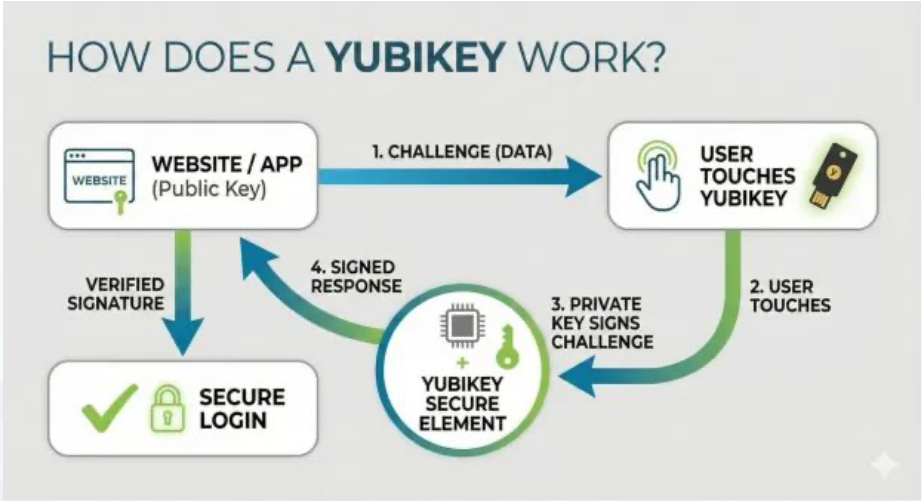
- **The Problem** - Why point-in-time hardware authentication is no longer enough
- **The Solution** - Continuous, autonomous, conditional machine posture verification
- **Enrollment** - One-time setup that cryptographically binds machine, hardware, and user
- **Platform Integration** - One trust signal across every platform you already operate
- **How It Works Demo** - A real-world login flow with hardware-verified access

© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

YubiKeys Were Built for a Different Era of Threat

YubiKeys solve one problem well: proving a user is present at the moment of login. But the moment authentication completes, their job is done - and so is your visibility.

- **Reactive, not continuous.** A YubiKey requires a user to initiate authentication. Unattended machines, industrial controllers, and unmanaged endpoints are invisible to it entirely.
- **Event-based, not ongoing.** Once authenticated, a compromised device stays authenticated. A YubiKey has no mechanism to detect or respond to anything that happens after the tap.
- **Binary, not conditional.** In or out. No posture check. No context. No admin override. A stolen credential with a cloned key gets the same access as a fully compliant, trusted device.



© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

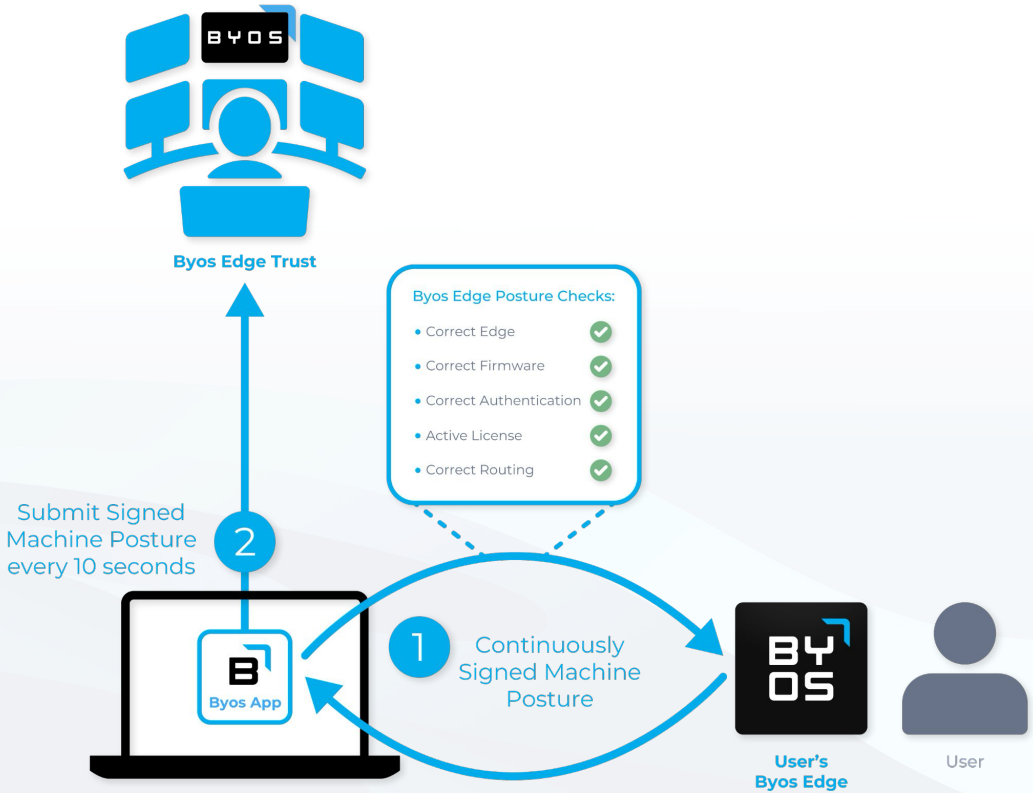
Byos Edge Trust: Machine Posture > Auth Tap

Every ten seconds, six hardware-attested checks verify the device is physically present, unmodified, and compliant - no user interaction required.

- **Continuous, not reactive.** No tap. No prompt. No human required.
- **Ongoing, not event-based.** Post-authentication compromise triggers instant revocation across every integrated platform.
- **Conditional, not binary.** Six checks. Context-aware policy. Real-time admin control.

Each report is signed by the Edge's onboard hardware Root of Trust and verified server-side through Byos' PKI - attestation that no software agent can replicate.

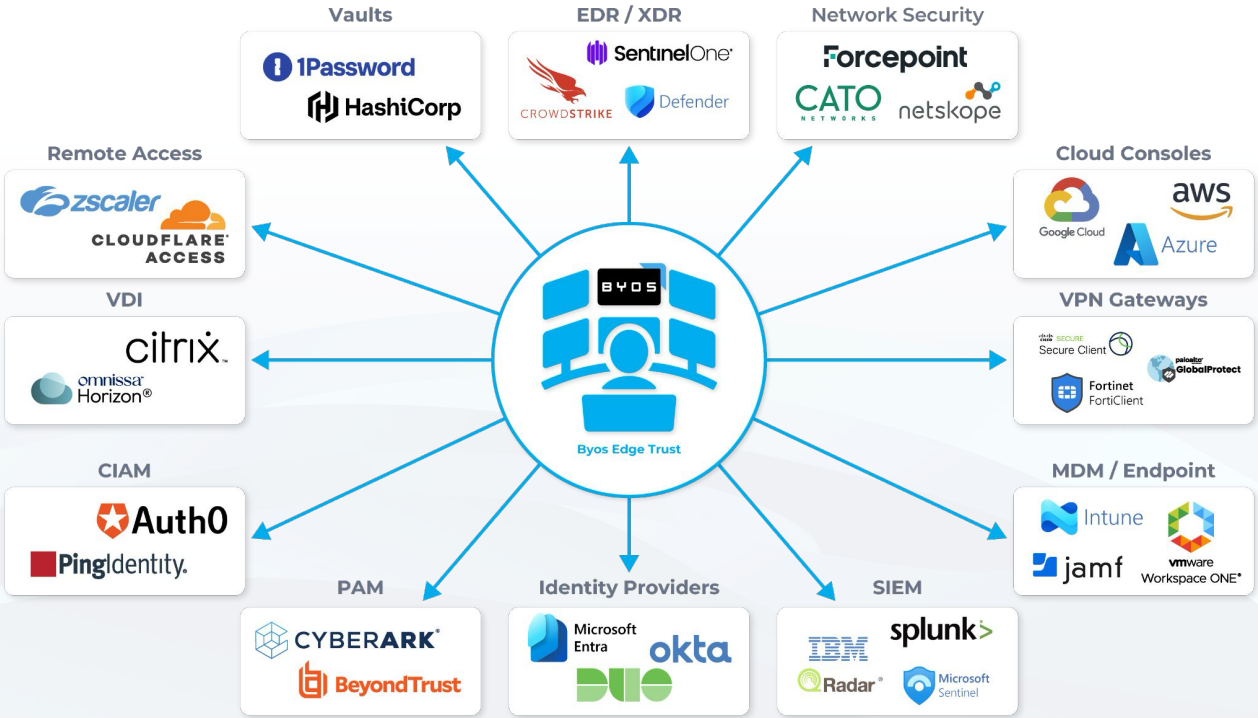
A YubiKey tells you someone was present at login. Edge Trust tells you whether that device should still have access right now.



© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

One Trust Signal. Every Platform You Already Operate.

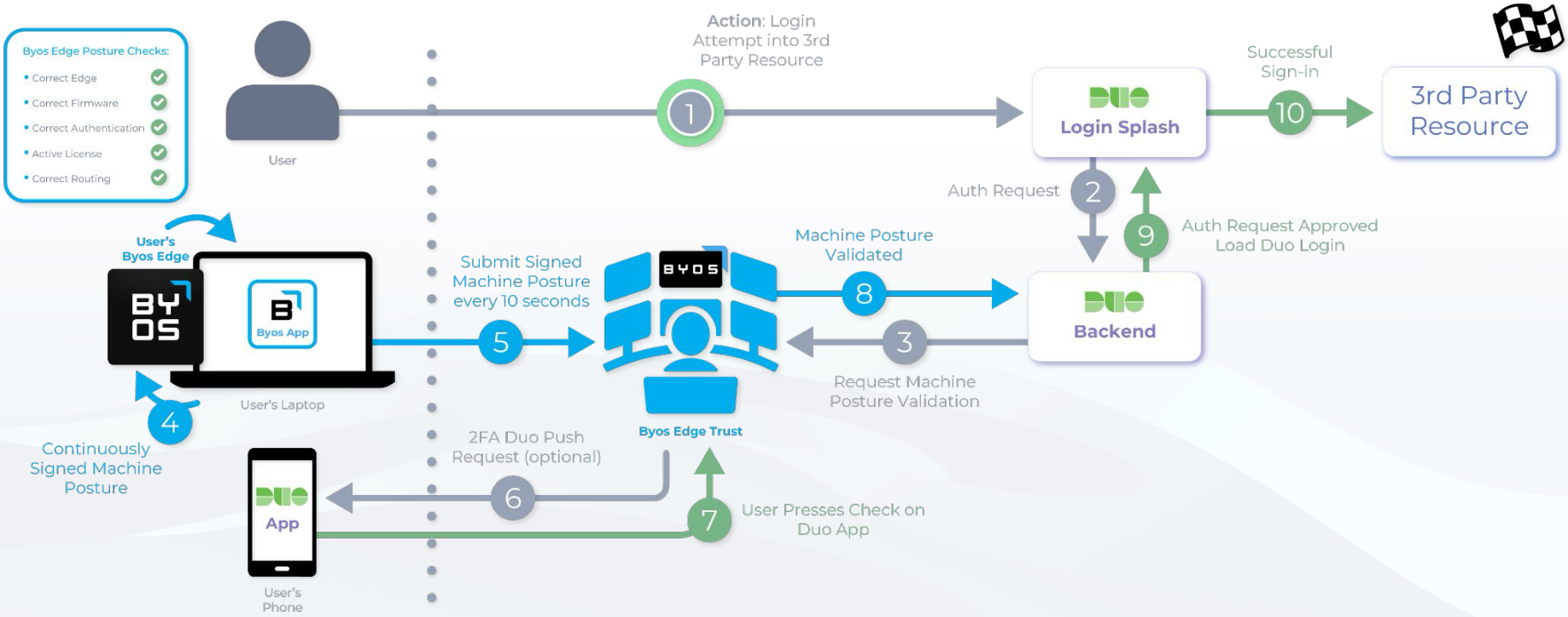
Edge Trust adds a hardware root of trust underneath your existing security stack — no rip-and-replace required. Real-time trust state changes flow automatically to ZTNA, SASE, EDR/XDR, MDM, SIEM, SSO, VPN gateways, vaults, and identity platforms. A single clean signal: trust granted or trust revoked.



© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

Example Login Attempt with Hardware-Verified Access.

Every step logged with full forensic detail. No session state carried by the server. Complete audit trail, no attack surface.

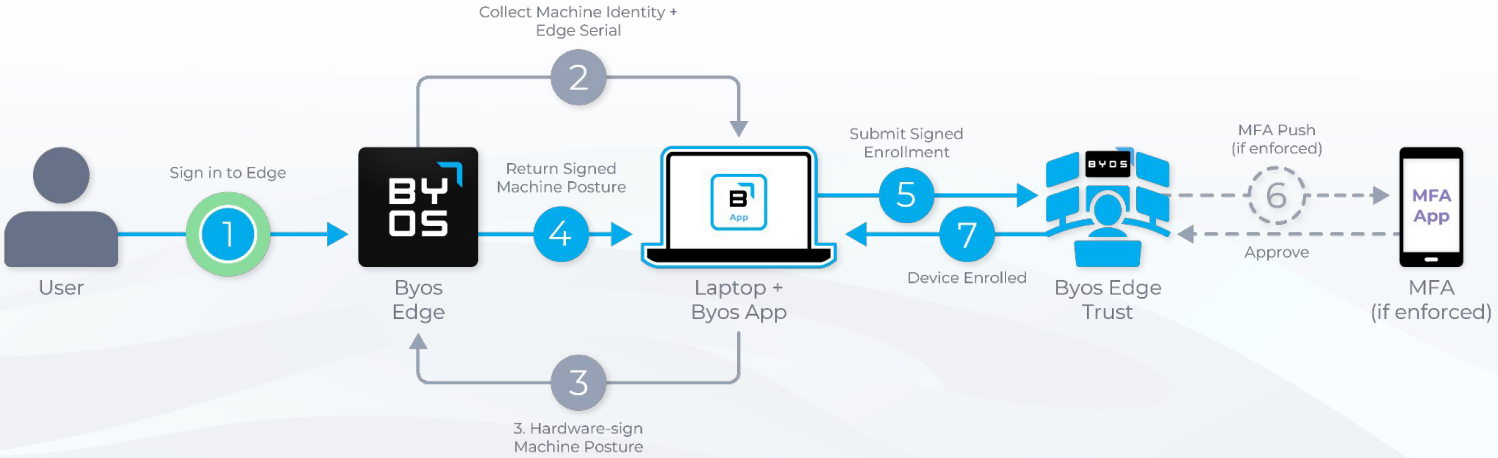


© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

Enrolled in Minutes. Bound in Hardware. Permanent.

The user signs into their Byos Edge device. The hardware signs an identity posture built from the machine chassis, motherboard, OS fingerprint, Byos Edge serial, and a unique per-user Salt kept in the OS Keyring.

The Byos Trust Server verifies and registers the enrollment. Optionally, you could add an MFA authorization push to the process. The device is cryptographically bound (machine, Edge, and user) in seconds.



© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

All Three Required. Compromise One, You Have Nothing.

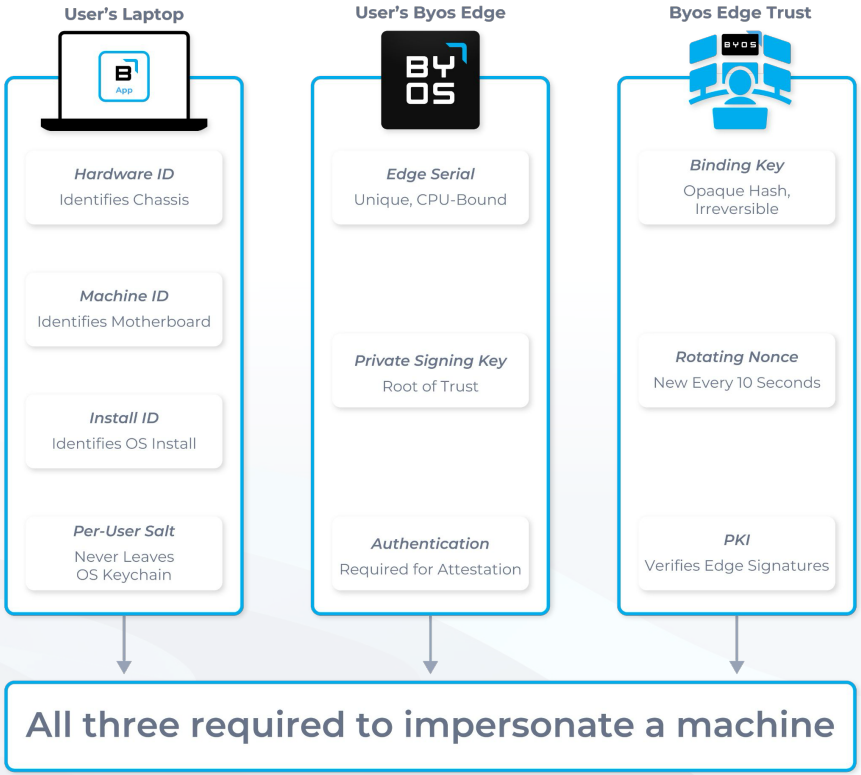
Six inputs from three independent sources are hashed into a single binding key using SHA3-512.

The **Trust Server** holds the hash, never the salt.

The **Byos App** holds the salt, never the full secret.

The **Byos Edge** signs challenges and never stores keys.

Change any input and the binding breaks. Capture any one component and you still can't forge attestation.



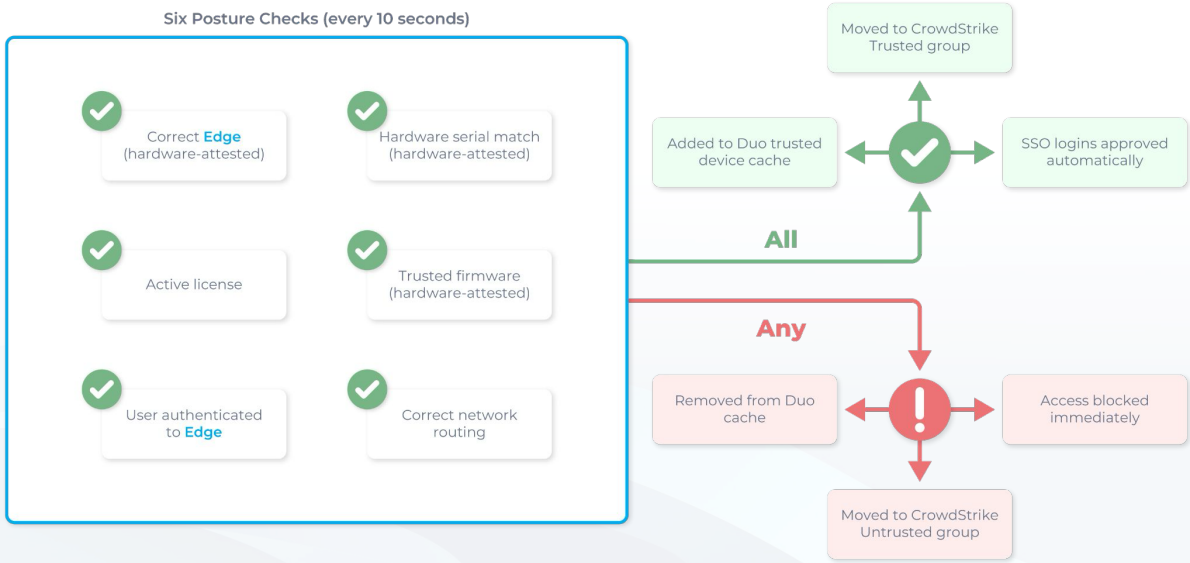
© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io

Six Checks. Two Outcomes. Zero Manual Steps.

Every ten seconds: correct Edge device, hardware serial match, active license, trusted firmware, authenticated user, correct network routing.

All six pass — device trusted, Duo cache updated, SSO approved automatically.

Any single failure — access blocked immediately, removed from Duo cache, moved to CrowdStrike Untrusted. No tickets. No delays.



© 2026 Byos Inc. - Ashburn, VA - All Rights Reserved. byos.io