CLOUDFLARE

SOLUTION BRIEF

Privileged access to cloud and on-prem infrastructure

Simplify access (authN/authZ/audit) for infrastructure targets — without disrupting developer workflows.

The over-privilege problem

While organizations have embraced Zero Trust initiatives that modernize secure access to apps and networks, infrastructure security or Privileged Access Management (PAM) strategies are largely siloed, overcomplicated, or ineffective.

- **Too risky:** Long-lived and shared keys too easily stick around and inflate risks related to excessive permissions and lateral movement
- **Too clunky:** Manual credential rotations and poor visibility plague admin productivity

Extending Zero Trust controls to infrastructure

Rather that adopt a legacy PAM tool or build a homegrown server access or key management solution, you can repurpose the same mindset your team is already using for Zero Trust Network Access (ZTNA) and related VPN replacement initiatives.

Verify infrastructure access the same way as apps — leverage existing identity provider groups and use SSO, MFA, and device context to build policies. Ensure only the right users access the right infrastructure resources, while logging everything along the way.

Cloudflare's consolidated approach

Converging privileged access with ZTNA

Cloudflare acts as an aggregation layer that extends modern IAM tools and granular, contextual verification further than other Secure Access Service Edge (SASE) vendors. This means:

- Expanding the scope of VPN replacement beyond an organization's apps and networks to its most sensitive infrastructure resources
- Reducing total cost of ownership by consolidating privileged developer access and general employee/contractor access

Cloudflare modernizes privileged access to infrastructure

Reduce risks

Prevent secure shell (SSH) key leaks and eliminate over-privilege risks that can leave infrastructure exposed.

Streamline operations

Avoid the complexity of legacy PAM or DIY solutions, with a simple, granular policy editor and audit logging built in.

Support developer workflows

Implement Zero Trust controls that don't disrupt developer, DevOps, or site reliability engineering (SRE) teams' native workflows.

Architecture overview

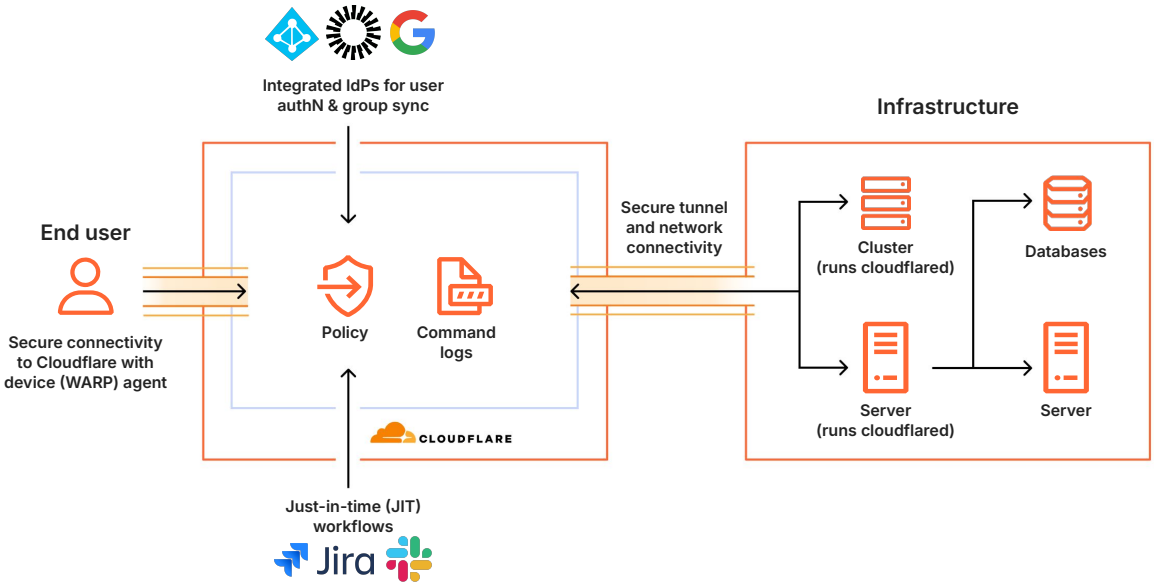

Figure 1: Diagram reflects acquired technology from BastionZero getting natively rebuilt into Cloudflare's ZTNA service. For a list of currently supported capabilities already delivered, see the Access for Infrastructure technical documentation.

How it works

Authenticate, authorize, and audit privileged access to targets, not networks

- Create Zero Trust access policies for target machines and specify ports, protocols, and user connection context (e.g., *root* or *ec2-user*).
- Stay out of developers' way by fitting into their existing workflows — no special CLIs or commands.
- Authenticate using single sign-on (SSO), multi-factor authentication (MFA), device posture, and other context.
- Support compliance auditing requirements by providing clear visibility and logging every end-user command.

Why Cloudflare for infrastructure access?

The most comprehensive ZTNA solution on the market

No other SSE / SASE vendor provides DevOps-friendly Zero Trust controls for infrastructure access alongside typical user-to-app workflows. And various infrastructure access startups merely tout yet another point solution.

Cloudflare's ZTNA service helps organizations consolidate legacy PAM or home-built server access capabilities into a broader VPN replacement plan or SASE architecture journey. All through Cloudflare's connectivity cloud — one of the largest, fastest, and most reliable networks in the world.

Want to learn more? See our step-by-step technical documentation, or request a conversation.

