CLOUDFLARE

SOLUTION BRIEF

Privileged access to cloud and on-prem infrastructure

Authenticate, authorize, and audit privileged access to infrastructure targets (SSH, RDP) — 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:** Persistent and shared keys linger too long, inflating risks related to excessive permissions and lateral movement
- **Too clunky:** Manual credential rotations and poor visibility plague security admin productivity, especially at scale

Extending Zero Trust controls to infrastructure

Rather that adopt a legacy PAM tool or build an in-house 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, as well as 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:

- Mitigating widespread security risks and performance challenges associated with traditional SSH and RDP access solutions.
- Reducing total cost of ownership by consolidating privileged developer access and general employee/contractor access.

Cloudflare modernizes privileged access to infrastructure

Reduce risks

Prevent SSH key leaks and mitigate RDP vulnerabilities that can leave sensitive infrastructure exposed.

Streamline operations

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

Support DevOps workflows

Implement Zero Trust controls without disrupting developer, DevOps, or site reliability engineering (SRE) teams' native workflows.

‘Access for Infrastructure’ architecture overview

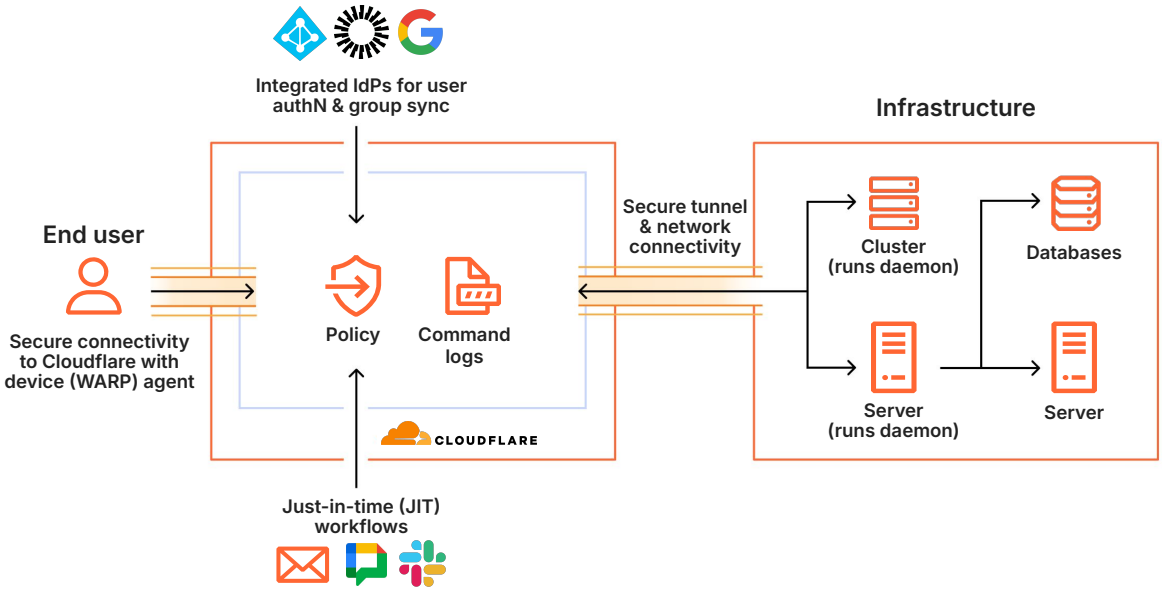

Figure 1: Diagram reflects the architecture of Cloudflare’s ZTNA service following native integration of acquired BastionZero technology. For the latest list of delivered capabilities, see the Access for Infrastructure technical documentation.

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*).
- Maintain developer agility by fitting into their existing SSH workflows — no special CLIs or commands.
- Provide browser-based RDP access for contractors and unmanaged devices through a high-performance proxy. No more Guacamole.
- Support compliance auditing requirements by providing clear visibility and logging of every end-user SSH command.

Why Cloudflare for infrastructure access?

Fast-track Zero Trust adoption with more comprehensive ZTNA

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 complimentary workshop.

