

The Trustless Access Platform

OVERVIEW

Remote access technologies are one of the most sensitive and valuable assets in your business. Whether your resources are located in the cloud or on-prem, IT and security must balance risk with employees' need to access them—anywhere and anytime. Organizations commonly use a patchwork of VPNs, jump hosts, and proxies to secure access. However, these so-called solutions typically require privileged access to your architecture.

Modern organizations have more risks and privileges to juggle than their people, processes, and technology can manage. Current access strategies involve a growing set of tools, secrets, and entitlements that overextended engineers must manage. The complexity of securing these across servers, containers, databases, and clusters only creates more risk that needs to be mitigated. As organizations continue to evolve for a hybrid world, many teams find themselves hamstrung by tools that are hard to manage, hard to secure, and hard to use.

BastionZero helps you break free from complexity with a cloud-native access experience that is simple to deploy, easy to use, and a breeze to maintain. The BastionZero Trustless Access Platform™ connects teams to resources without risking the keys to your kingdom. With our multi-root trustless access protocol, you can reclaim your architecture from over-privileged third parties and ensure that the right people have access to the right resources at the right time.

BENEFITS

- ✓ **Reduce Risk**
Simplify IT and network architecture without giving a third party the power to control or grant access to resources.
- ✓ **Boost Productivity**
Accelerate the pace of development and deployment with no additional infrastructure to deploy or manage.
- ✓ **Automate Compliance**
Scale least-privilege access and control which user or service can assume which role/account on which target.
- ✓ **Enhance Visibility**
Meet compliance needs with searchable command logs and session recordings that are identity-aware.

PLATFORM



BZ Access

Connect your team to sensitive resources securely, wherever they are.



BZ Authorization

Enforce powerful policies based on roles and user accounts via a single pane of glass.



BZ Authentication

Authenticate users and services using your SSO or IdP and our independent MFA.

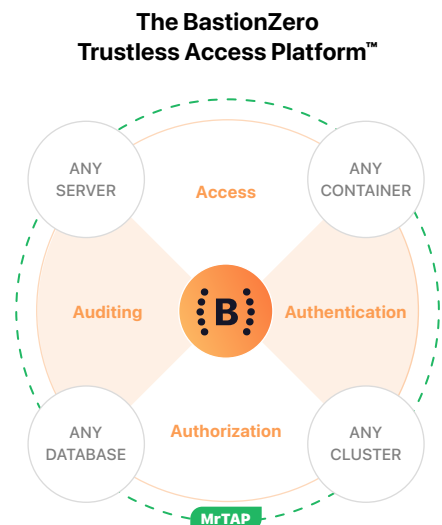


BZ Auditing

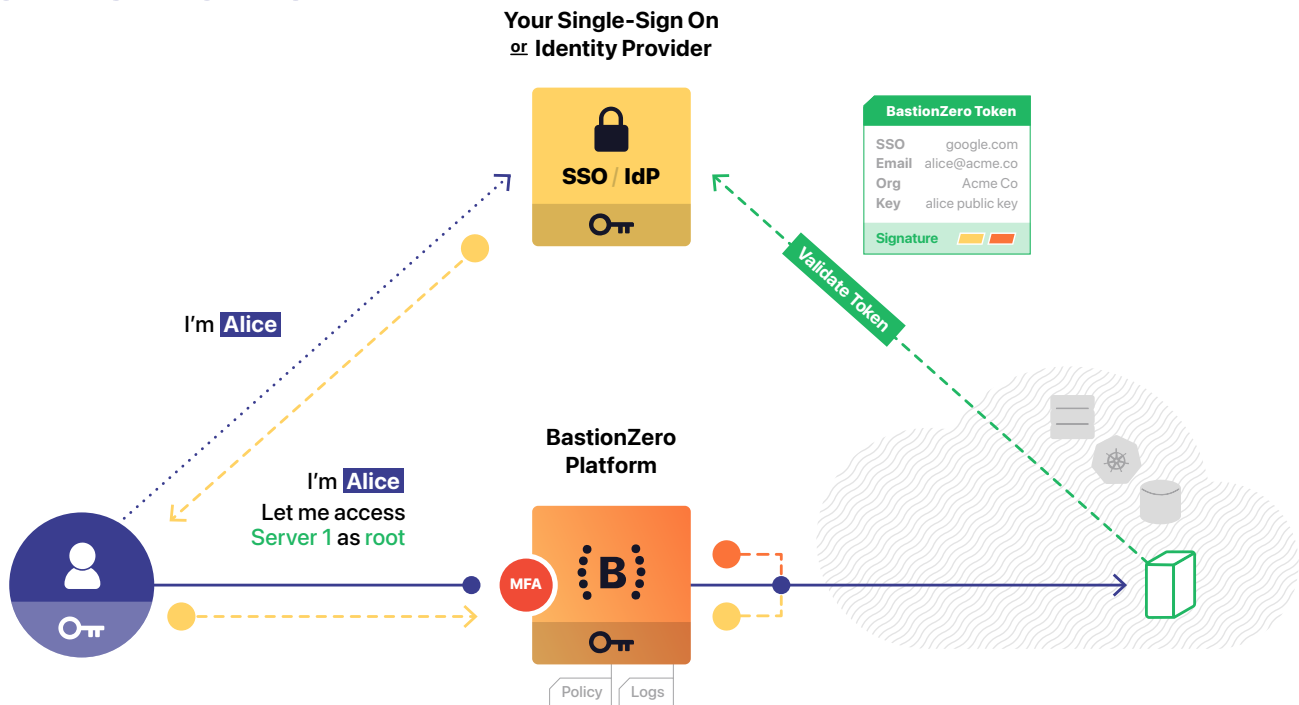
Memorialize all activity in your systems with command logs and session recordings.

Multi-Root Trustless Access Protocol (MrTAP)

BastionZero prevents single points of compromise with MrTAP, a cryptographic protocol that certifies every request using two signatures from independent roots of trust: our cloud service (MFA) and your single-sign on (SSO) or identity provider (IdP).



How It Works



FOR ENGINEERING

- + **Just-In-Time Access**
Remove development bottlenecks and empower engineers with real-time, approval-based access to the resources they need.
- + **Passwordless Authentication**
Ditch long-lived credentials and give engineers access without passwords, keys, and secrets that may be shared, lost, or stolen.
- + **Developer-First Workflows**
Meet engineers where they are with integrations for SSH and database clients, the command line, APIs and open-source tools.

FOR IT AND SECURITY

- + **Centralized Policy Controls**
Curb privilege creep through a single pane of glass with scalable guardrails that enforce who may access your systems, via what roles, when, and for how long.
- + **Identity-Aware Logging**
Know who did what to each resource, regardless of account, with comprehensive audit trails for every action taken on your infrastructure.
- + **No Open SSH or VPN Ports**
Close at-risk ports and automatically discover public, private, or hybrid cloud resources with a secure phone-home approach.

WORKS WITH



AWS



GCP



Azure



Linux



Chef



Okta



OneLogin



Puppet



Kubernetes



Ansible



Snowflake



Jupyter



Docker

...and more