POMERIUM

Context-Defined Access Control

Simplify and secure access to your infrastructure and internal applications

Zero Trust, Zero Compromises

Actual zero trust architecture principles for production environments based on NIST 800-207.

Centralized Authorization Policies

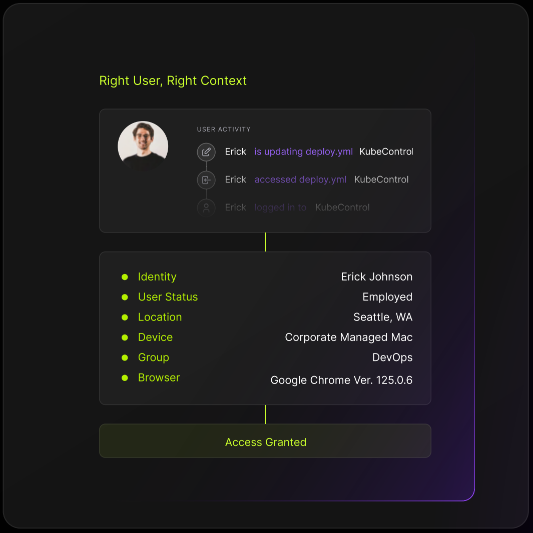
Real-time, fine-grained authorization control and audit logs on every single action, based on all available context.

Protect Anything, Everywhere

Plays nice with cloud-native tools like K8s on any infrastructure – cloud, bare metal, VMs, and more

At Pomerium, we believe that context defines access. Pomerium enables users to combine identity, device and any other available context to build centralized fine-grained authorization policies to secure access to internal applications, databases, Kubernetes API and workloads, and more without a client.

Pomerium adheres to the key principles of Zero Trust Architecture, meaning that all user requests are continuously verified, with no implicit trust granted to users or devices. All of this is enabled without the need for a client or agent on the device. Because of this clientless access, Pomerium is nearly invisible to the user, staying out of their way and letting them spend more time working on what matters most – instead of waiting for their VPN to update.



Right User, Right Context

USER ACTIVITY

Erick is updating deploy.yml KubeControl

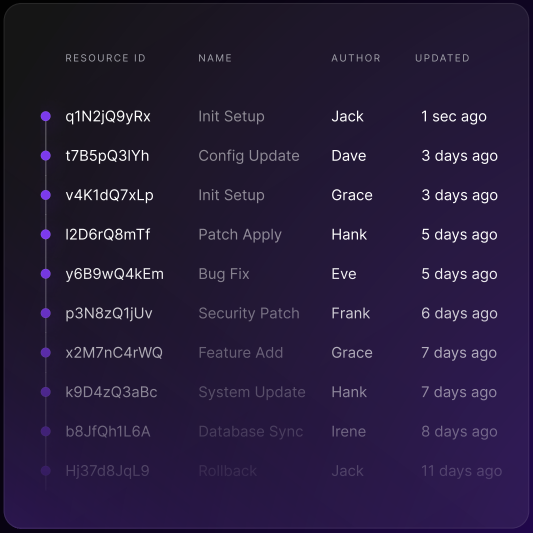
Erick accessed deploy.yml KubeControl

Erick logged in to KubeControl

● Identity	Erick Johnson
● User Status	Employed
● Location	Seattle, WA
● Device	Corporate Managed Mac
● Group	DevOps
● Browser	Google Chrome Ver. 125.0.6

Access Granted

Instant, frictionless, clientless access that users love



RESOURCE ID	NAME	AUTHOR	UPDATED
q1N2jQ9yRx	Init Setup	Jack	1 sec ago
t7B5pQ3IYh	Config Update	Dave	3 days ago
v4K1dQ7xLp	Init Setup	Grace	3 days ago
l2D6rQ8mTf	Patch Apply	Hank	5 days ago
y6B9wQ4kEm	Bug Fix	Eve	5 days ago
p3N8zQ1jUv	Security Patch	Frank	6 days ago
x2M7nC4rWQ	Feature Add	Grace	7 days ago
k9D4zQ3aBc	System Update	Hank	7 days ago
b8JfQh1L6A	Database Sync	Irene	8 days ago
Hj37d8JqL9	Rollback	Jack	11 days ago

Immutable session logs with full chain of custody that security teams love

Common Pomerium Use Cases

Whether you're a homelab user or at a Fortune 50 company looking to provide secure remote access has never been easier. Pomerium's architecture is flexible enough to accommodate nearly any infrastructure, database and application.

Securing Kubernetes

Secure Kubernetes API, workloads and upstream apps with a single, centralized policy enforcement point.

Securing Hybrid/ Multi Cloud Environments

Pomerium's proxy lives at edge, and its policies are centralized, enabling you with access control that can be deployed anywhere.

Securing Internal Databases

Limit lateral movement on your network by locking down access to sensitive databases and adding continuous verification for all requests.

Securing Legacy Applications

Upshift your security model across the hundreds if not thousands of internal applications that developers have created that lack proper AuthN and/or AuthZ.

Dashboard Access

Easily deploy dashboards with a URL to business users and executives and eliminate the monthly pings asking for VPN troubleshooting help.

Developer Productivity

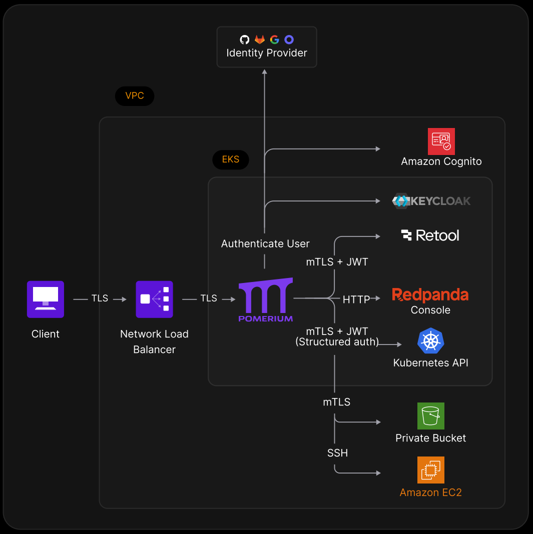
Make security part of the developer's toolkit by natively integrating Pomerium into your CI/CD pipeline.

Centralizing AuthZ Policies

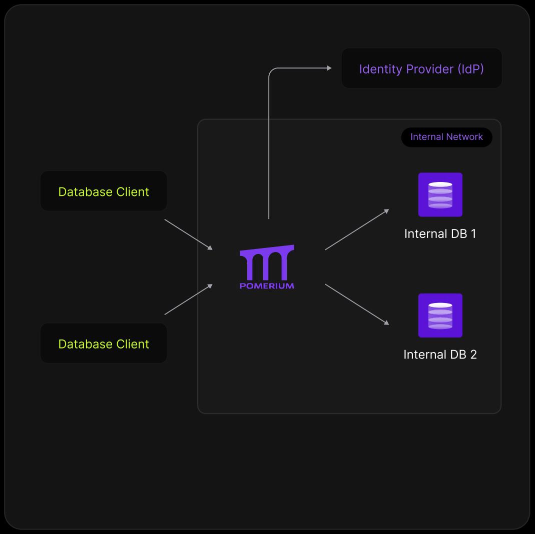
Pomerium's control plan allows you to centralize fine-grained authorization policies across all of your resources with support for HTTP, SSH, RDP, TCP, UDP, gRPC and more.

Eliminating IT tickets

Pomerium is clientless and native to the browser, and if a user does not have access to a resource, they can be prompted with self-remediation instructions.



Securing Kubernetes on Amazon EKS



Securing Access to Internally Hosted DBs

Why teams love Pomerium

DevOps

“What really drove our adoption of Pomerium was our migration to Kubernetes...what we were trying to do is divorce the idea of needing to have a VPN for privileged access.”

Zach Dunn
CISO

Security

“Pomerium is the lynchpin in our ZeroTrust platform strategy.... we will be relying on Pomerium to gate access to all internal resources for all employees.”

CTO of Security Architecture,
Financial Services firm (20k+ employees)

End Users

“My favorite part where users are like: “Oh, it just works?” And it’s crazy. It didn’t work like that before. So that’s awesome.”

Cory Rankin
Director of Technology

Developers

“Every company right now that is not using Pomerium would pay 100x over for Pomerium based what we’ve seen in dev time saved.”

Alex Lash
Principal Member of Technical Staff

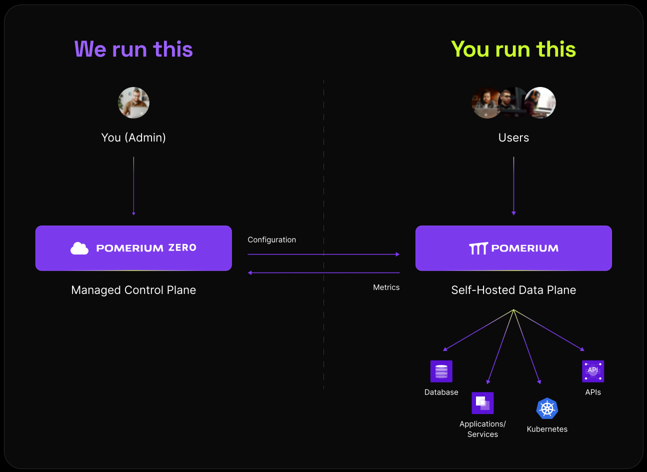
Products

Pomerium's reverse proxy (referred below as the Data Plane) is always self-hosted. The Control Plane can either be managed (hosted by Pomerium) or self-hosted depending on which edition better fits your organization's needs. Visit pomerium.com/pricing for a detailed overview.

01

Pomerium Zero

Ideal for businesses with up to 1000 users looking to get started quickly with zero trust, remote access.

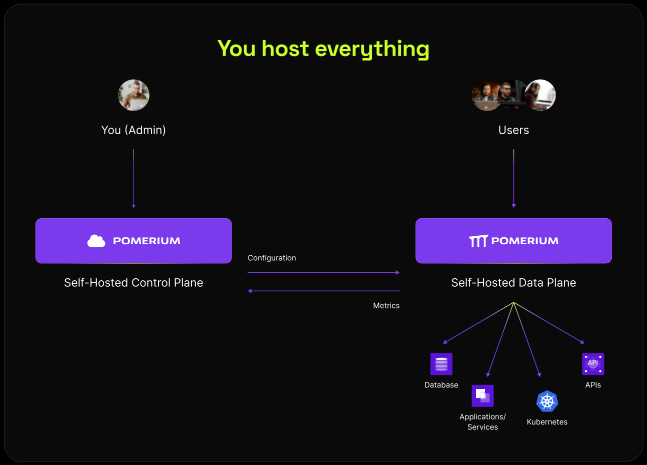


Managed Control Plane + Self-Hosted Data Plane

02

Pomerium Enterprise

Ideal for larger companies with complex environments who want total control over their entire deployment.



Managed Control Plane + Self-Hosted Data Plane

POMERIUM