Teleport

Modern Infrastructure Demands a Modern Approach to Privileged Access

Contents

Privileged Access Management (PAM) solutions emerged decades ago with a noble mission: closely guard credentials with elevated privileges. But in years since, a lot has changed — especially within infrastructure environments.

Modern infrastructure is dynamic, cloud-native, ephemeral — and complex. Your engineering and security teams need to balance development, operations, and security needs, and with increasing agility as infrastructure scales across more technologies, more geographies, and more environments.

Increases in complexity also introduce daunting access control challenges. Enabling and enforcing secure access across vast multi cloud and containerized environments requires capabilities that many legacy PAM solutions were not designed to deliver in a developer-friendly way. And as metrics like time-to-market become synonymous with business success, your organization's critical development processes cannot afford to be sidelined by manual and inefficient workflows that were designed for static environments and IT-centric use cases.

Instead, you must design privileged access to be as agile and ephemeral as modern infrastructure — and we're here to show you how.

In this white paper, we define the key challenges in securing access to modern computing infrastructure. We will then examine an anonymized case study based on real world discussions with hundreds of organizations. This example will illustrate the challenges organizations face when attempting to adapt their legacy access controls to modern infrastructure environments.

Finally, we will describe how platforms for secure infrastructure access, such as Teleport, are purpose built for modern infrastructure environments — and can unlock engineering productivity, harden organizational security, and enable companies to meet compliance burdens with ease.

The challenges of modern infrastructure

There are many attributes that distinguish modern computing infrastructure from its predecessors. Chiefly, modern infrastructure is:

- Ephemeral
- Automation-dependent
- Complex, globally distributed, and highly diverse

Traditional PAM models may be ill-equipped to support environments with these attributes, resulting in difficulties scaling secure access, ensuring productivity, and consistently enforcing policies across diverse infrastructure.

However, modernized privileged access models — built to support cloud-native, dynamic, and complex infrastructure — can resolve many of the same challenges.

In this section, we will explore these modern infrastructure attributes and the access challenges that accompany them in greater depth.

Traditional PAM

- Static credentials and vaulting
- Manual request/approval processes
- Focus on network segmentation
- Siloed management and limited visibility
- Not well suited for automated workflows and cloud environments

Modernized privileged access

- Cryptographic identity; no credentials
- Least privileged access governed by RBAC and workflows integrated with developer tools
- Zero-trust architecture
- Unified dashboards and controls
- Purpose-built for ephemeral and cloud-native environments

Modern infrastructure is ephemeral (not static)

Credentials are all too commonly exploited by attackers. In fact, attacks using stolen or compromised credentials have increased by more than 71% (IBM X-Force, 2024).

Traditional access management strategies rely on credential-based access, including passwords, tokens, and API keys. As infrastructure grows, so does its complexity, including users, resources, machines, and technologies — and with them, an explosive volume of credentials that need to be dynamically managed.

The probability of human error increases with this complexity. Hard-coded secrets and passwords scattered across source code or configuration files can lead to secrets sprawl or implemented and forgotten SSH keys, making it difficult to protect access paths from compromise due to human error. Threat actors can also target long-standing privileges, employing breach and pivot tactics that enable them to rapidly move laterally within compromised infrastructure.

The best defense to secure credentials from threat actors? Turn to identity-based authentication methods that eliminate them altogether.

The best defense to secure credentials from threat actors? Turn to identity-based authentication methods that eliminate them altogether.

Modern infrastructure is automated (not manual)

Infrastructure has come a long way since the basic LAMP stack (Linux, Apache, MySQL, PhP). In fact, most modern environments are increasingly built around ephemeral resources and software, with layers upon layers of complexity.

The dynamic, highly scalable nature of today's infrastructure does not fit with access controls based on static resource assumptions. Legacy PAM systems designed for static policy configuration and manual elevation of privileged access are a poor fit with environments where resources are being rapidly scaled up and down. To efficiently and consistently control access to modern infrastructure at scale, automation is critical — not only for maintaining development agility, but also for minimizing overhead or error caused by human intervention.

In many cases, privileged access is also required by machines. Modern solutions for privileged access need to unify human and machine access control and accommodate ephemeral resources, rather than remain oriented around persistent applications and systems.

Modern infrastructure is complex (and increasingly so)

As organizations expand their infrastructure across multiple platforms, resource types, and geographical locations — including on-premises and multi cloud — legacy PAM solutions may struggle to keep pace. This diversity in resource types adds significant complexity when creating and enforcing access policies, as each technology may have its own unique approach to policy definition.

These policies may often start within security engineering teams as the complexity of the technology and its use cases fall outside of traditional IT concerns. This creates a proliferation of "access silos," caused by the fragmentation of identity and policy. This makes it difficult to establish which users have access to what resources, which can complicate compliance audits and make centralized oversight challenging.

Modern infrastructure environments are shapeshifters, rapidly adapting as the needs of the business change and new technologies emerge. Access policies need to be able to keep pace with these evolutions, while also reducing the risks of misconfiguration which can create vulnerabilities.

Top infrastructure access challenges according to security leaders

86-90%

Productivity & development

Supporting DevOps and CI/CD is a major hurdle, with 86% ranking it as a top infrastructure access challenge. 90% also prioritize developer adoption of access solutions for smoother workflows. (Teleport, 2024)

88%

Attack surface & credential risks

The expanded attack surface from cloud, microservices, and containers is a primary concern for 87% of organizations, with 88% also grappling with the growing number of credentials and secrets adding to security silos. (Teleport, 2024)

94%

Infrastructure access

Compliance is critical, with 94% of respondents emphasizing the importance of passing audits. An equal 94% highlight team efficiency as a key factor for selecting infrastructure access solutions. (Teleport, 2024)

Teleport

Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.