Teleport

2024 State of Secure Infrastructure Access

Survey Report

Since the password was first introduced into computing in the early 1960s, it has had the singular goal of holding back the hordes: hackers, criminals, hostile nation-states, insiders, and countless other malicious black hats.

It has been a lonely vigil, and the headlines show it has been a losing battle. Amazon, Apple, Microsoft, Marriott, and Uber have all experienced high-profile data breaches in recent years. Why is it that some of the world's most technically advanced, highly funded companies failed to secure their computing systems? And if they failed, what hope do the rest of us have?

It was precisely these questions that motivated Teleport to commission our **2024 State of Secure Infrastructure Access survey**. We wanted to learn how large enterprises sought to secure their valuable computing infrastructure, and how their efforts were going. And ultimately, we hoped to learn the best practices that would allow enterprises to gain the upper hand.

What we found was very interesting ...

Contents

Secure Infrastructure Access Matters

Securing access to computing infrastructure is extremely important to the enterprises we spoke to. But infrastructure access security isn't easy. Three of four say it is getting somewhat hard to extremely harder each year. Why?

- **Cloud computing** complicates securing access to computing infrastructure due to its distributed nature, which increases potential entry points and requires robust, scalable security measures across diverse environments.
- **An increase in identity attacks** complicates securing access to computing infrastructure by making it challenging to distinguish between legitimate users and malicious actors, thereby undermining access control and security measures.
- As **infrastructure becomes more complex**, securing access to computing systems becomes more challenging due to the increased number of potential vulnerabilities and entry points that need to be managed and protected.
- **Remote work** makes it harder to secure access to computing infrastructure, because it often involves diverse and unsecured home networks, increasing the risk of unauthorized access and data breaches.
- **Malicious actors are using AI** to craft attacks. This makes attacks cheaper to execute and more effective.

As to what, exactly, is more challenging, enterprises cite five big challenges:

- **Massive scope of what they're protecting** complicates securing access due to the increased scale, complexity, and diversity of components that need to be managed and protected.
- **The proliferation of credentials and secrets** from emerging silos such as cloud, edge, and IoT significantly complicates securing access to computing infrastructure by introducing a multitude of diverse and numerous access points that require meticulous management and constant vigilance.
- **An expanding attack surface** (cloud, microservice architectures, containers, etc.) increases complexity and potential vulnerabilities, making it more challenging to secure access to computing infrastructure.
- **Regulatory compliance** adds complexity to securing access to computing infrastructure by imposing stringent requirements and controls that must be meticulously followed to protect sensitive data and ensure legal adherence.
- **Support of DevOps methodologies** complicates securing access to computing infrastructure due to the dynamic and collaborative nature of continuous integration and delivery, which demands frequent changes and broad access permissions.

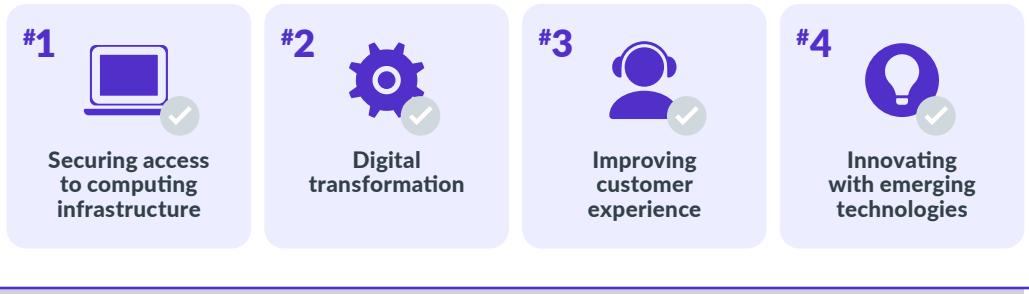
We asked enterprises to tell us what are the most difficult attacks to protect against. They responded with five attack vectors:

- **AI impersonation by threat actors** is difficult to defend against because it can mimic legitimate user behavior with high accuracy, making it challenging to distinguish between genuine and malicious access attempts.
- **Social engineering attacks**, like phishing, are difficult to defend against because they exploit human psychology and trust, often bypassing technical security measures by manipulating individuals into revealing sensitive information.
- **Compromised privileged credentials and secrets** are difficult to defend against because they provide attackers with elevated access, making it challenging to detect unauthorized activities and secure the computing infrastructure effectively.
- **Breach and pivot attacks** are challenging to defend against in securing access to computing infrastructure due to their complex nature and the stealth tactics employed, allowing attackers to move laterally within a network undetected.
- **MFA resets** are challenging to defend against because attackers can exploit social engineering tactics to manipulate support staff or users into bypassing security protocols, thereby compromising access to computing infrastructure.

In summary, we found that securing access to computing infrastructure was important, but getting more difficult by the day. How important? We asked respondents to rank their IT initiatives by importance. It turns out that **infrastructure access security is more important than any of the leading IT initiatives** enterprises are commonly working on, such as digital transformation, improving the customer experience, or driving innovation with emerging technologies.

With this level of importance, we were curious about what enterprises are doing to secure infrastructure access.

Secure Infrastructure Access: Top Technology Initiative



State of Secure Infrastructure Access Practices

Enterprises employ a wide range of security safeguards designed to secure infrastructure access. The most common cited tactics are listed here, in order of adoption:

- **Multi-factor authentication:** MFA enhances security by requiring multiple forms of verification, making unauthorized access to computing infrastructure significantly harder.
- **VPN:** Crucial for securing access to computing infrastructure by encrypting data and protecting it from unauthorized access.
- **Identity Provider (IdP):** Secures access to computing infrastructure by centralizing authentication and ensuring only authorized users can access sensitive resources.
- **SSO:** Enhances security by centralizing authentication, reducing password fatigue, and minimizing potential attack vectors.
- **Using AI to make safeguards more accurate and effective:** Analyzes patterns and detects anomalies.
- **Phishing-resistant password-less authentication:** Enhances security by effectively preventing unauthorized access to computing infrastructure.
- **Zero Trust Networking:** Minimizes security risks by continuously verifying every access request.
- **Use of cryptographically authenticated identities for systems or resources:** Prevents guessing of passwords (or obtaining them through phishing).
- **A unified store for all identities (people, machines, services):** Streamlines authentication and authorization, enhancing security by providing centralized control and monitoring of access to computing infrastructure.
- **Use of cryptographically authenticated identities for users:** Makes it more difficult to guess passwords (or obtain them through phishing).
- **PAM:** Privileged Access Management (PAM) enhances security by controlling and monitoring privileged access to critical computing infrastructure.
- **IGA/ITDR:** Identity Governance and Administration (IGA) and Identity Threat Detection and Response (ITDR) solutions provide enhanced security by controlling access and detecting threats to computing infrastructure.
- **CIEM:** Cloud Infrastructure Entitlement Management (CIEM) ensures only authorized users have access to specific cloud resources, reducing the risk of unauthorized access.

Clearly, enterprises implement safeguards on a wide range of fronts. How effective are these efforts?

Teleport

Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.