Teleport

Defending against Identity Provider (IdP) Compromise

Implementing Infrastructure Defense in Depth - keeping critical systems and data secure in the event of identity provider compromise

White Paper

Contents

Teleport partnered with security researcher Doyensec to explore the current state of the third-party identity management security market and steps that companies can take, using Teleport, to implement an additional layer of security in order to reduce the impact of a compromised SSO provider. The paper summarizes Doyensec's findings, including a Hardening Checklist for defense against IdP compromise, as well as commentary from Jack Poller, Principal Analyst of Paradigm Technica. Customers may request Doyensec's full research report from their Teleport account manager.

Introduction

As organizations increasingly adopt Single Sign-On (SSO) as the central point of authentication, Identity Providers (IdPs) become a focused point of attack for threat actors to gain access to critical infrastructure and sensitive data. Recent incidents have highlighted a growing threat landscape targeting these identity ecosystems, posing significant risks to the security posture of both businesses and individuals.

> Organizations must take action now to harden their infrastructure against compromised identity provider scenarios.

This paper introduces Infrastructure Defense in Depth, an approach to infrastructure security that companies can adopt using Teleport to keep their critical systems and data protected even in the event that their identity provider is compromised, using the capabilities and configurations outlined in this paper.

The Threat Landscape

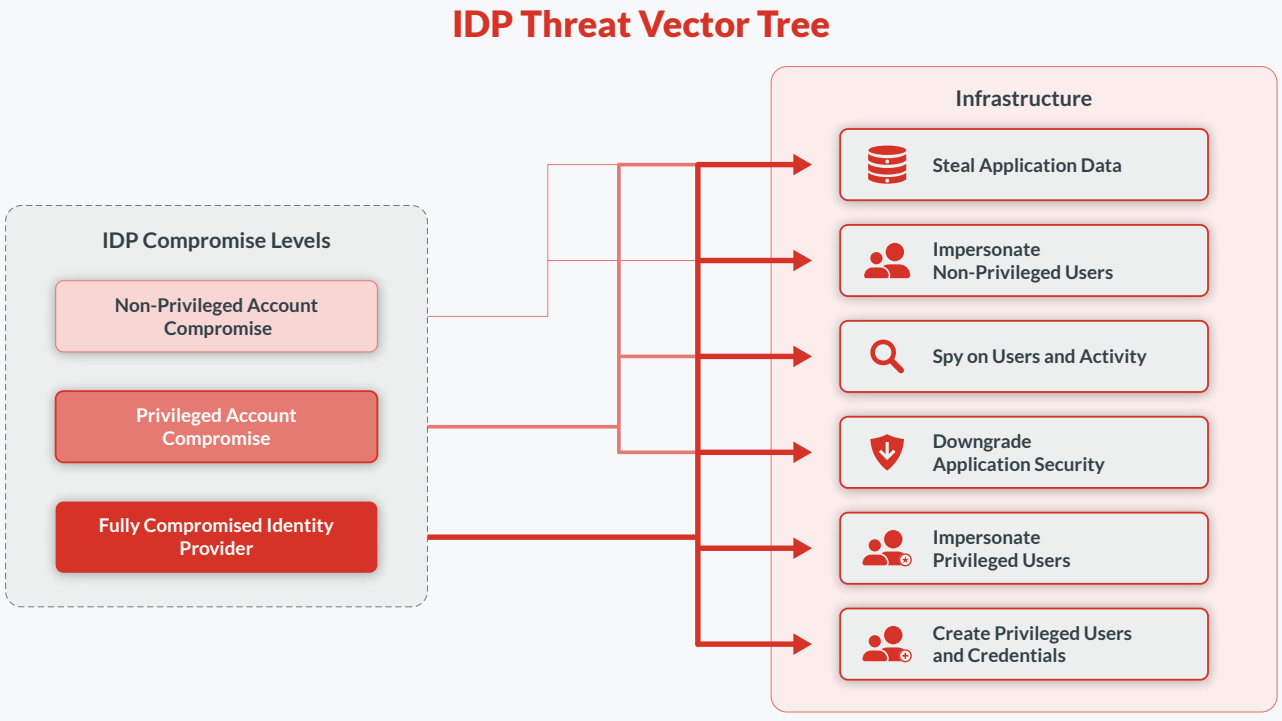
Recently, there has been an unprecedented rise in threat actors targeting Identity Providers (IdPs). As organizations increasingly rely on centralized identities for user authentication and access control on a wide range of business-critical services, the compromise of an identity provider poses increasingly severe risks to downstream infrastructure.

The Single Sign-On (SSO) provider is chosen as an entry point by attackers specifically because of its trusted highly privileged position managing authentication within the target business. Common patterns employed by attackers include: social engineering, broad-based or spear phishing campaigns, bribing employees for 2FA codes, prompt-bombing, credential stuffing, session hijacking, password spraying, access tokens leakage and counting.

The blast radius of potential attacks heavily depends on the number of Service Providers (SPs) that trust the identity provider to authenticate and authorize internal actions, as well as the level of compromise itself:

- **IdP Vendor Compromise:** This scenario delineates all cases in which a vulnerability or misconfiguration allows an attacker to obtain access to the IdP. This affects all organizations using the identity solution and consequently, they are considered as the worst case scenarios, because of the breadth of the affected audience.
- **IdP Instance and Account Compromise:** The compromise of a single identity provider instance involves a threat model with factors related to misconfigurations, credential leakage, and social engineering attacks against employees. These are threats that target a specific company rather than the IdP solution itself.

The following threat model lays out the various compromises that a company needs to consider depending on the point and severity of attack:



Reducing Impacts from an IdP Compromise

The recent breaches experienced throughout the industry highlight the importance of in-depth security measures to prevent an attacker from compromising an IdP and abusing it to move laterally in the organization. No SSO provider should be assumed to be and remain secure.

> "No SSO provider should be assumed to be and remain secure."
>
> - Luca Carettoni, CEO, Doyensec

The Infrastructure Defense-in-Depth (IDiD) approach consists of implementing an additional layer of security over the identity provider, with protection mechanisms and configurations that defend against the aforementioned threats. The security layer needs to be present on the service providers trusting the IdP as the source of authentication for users.

This approach helps the identity provider and the defense-in-depth provider to work together to strengthen end-user
security. Additionally, the role of the defense-in-depth provider eliminates the need for each Service Provider to independently layer in equivalent levels of defense, which is difficult to achieve with consistency across vendors and is expensive.

Secure Infrastructure Access with Teleport

Teleport, a provider of secure infrastructure access, hardens infrastructure security with on-demand, least privileged access based on cryptographic identity and zero trust, coupled with identity security and policy governance. This architecture eliminates secrets and standing privileges, eliminating broad attack surface leveraged by threat actors:

Modern Access Control	
Governance	Built-in identity and policy governance. Identity locking. Access graph.
Secretless Authentication & Ephemeral Privileges	Least privileged, on-demand access; request workflows. Tamper-proof audit w/ identity-aware session data.
Zero Trust	For applications and workloads. Identity and protocol-aware, reverse tunnels.
Cryptographic Identity	Provisioned and enforced for all users, devices, machines, resources.

Defense-in-Depth Protection Mechanisms

In addition to the architecture described above, companies can employ the following features as protection mechanisms that can be deployed to stop threat actors in compromised IdP scenarios. This chart lays out the role that each key feature can play in blocking threat actors from pivoting from an initial breach to more sensitive data or systems in infrastructure.

Feature	Role in Infrastructure Defense in Depth
Per-session Phishing-Resistant MFA	Protects users against compromises of their infrastructure access, if the threat actor bypasses / controls the MFA on the IdP.
Access Requests	Implements the principle of least privilege, leaving an attacker with no permanent admins to target.
Dual Authorization	Prevents a single successful phishing attack from compromising infrastructure.
Mandatory Phishing-Resistant MFA Enrollment	Prevents weak access patterns.
Web Authentication (WebAuthn)	Secures user identities and prevents attacks like vishing by adding another layer of physical authentication to verify user identities.
MFA for Administrative Actions	Secures against the exploitation of compromised admins, by re-verifying the user's identity promptly before performing any administrative action.
Device Trust	First MFA device enrollment is useful to protect against compromised IdP forcing the auto-provisioning of new users.

Hardening Steps and Best Practices in Configuration

Doyensec further identified in its testing configuration guidelines that can harden security further. These protect against:

- attackers hijacking access reviewer privileges
- roles mapping matching attacks
- exploitation of auto-provisioning of new users, and
- hijacking of both privileged and unprivileged accounts.

Doyensec testing demonstrated that these configurations protected against all tested scenarios of IdP compromise. These recommended configurations are laid out in Appendix B, with a security checklist included in Appendix C.

Teleport

Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.