



3 ways to fail your zero trust journey and how to prevent them

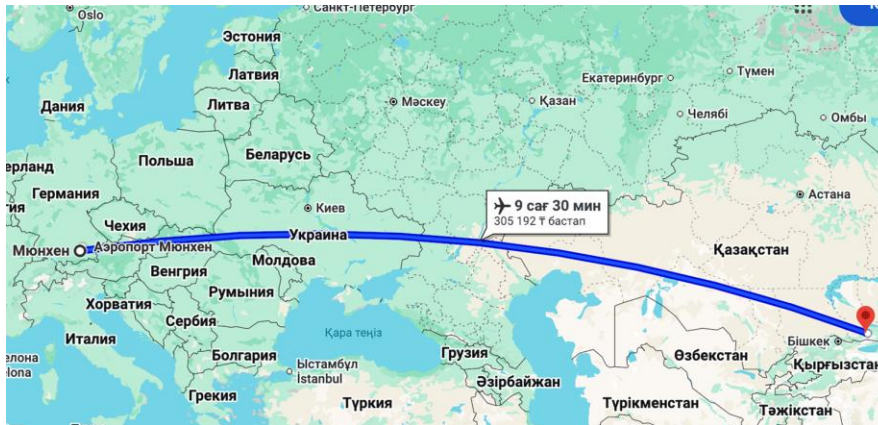


Alexey Sazhin
Senior Solutions Engineer
Cloudflare

Alexey Sazhin



- SE at Cloudflare
- > 10 years in PS, Customer Success, Pre-Sales for Zero Trust and WAN migrations
- ex Cisco
- CCIE and Juniper JNCIE-SP
- Surfing, Snowboarding
- <https://www.linkedin.com/in/asazhin/>



Agenda

- 1 Introduction
- 2 3 Fails
- 3 Conclusion

Poll

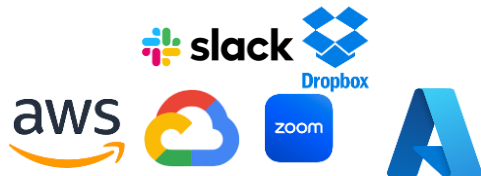


Raise your hand if you had
Zero Trust experience

1-Minute Zero Trust History Recap



Birth of the first commercial firewalls establishes the "castle and moat" security model



Google's implemented "BeyondCorp" ZT for GCloud marks beginning of modern Zero Trust thinking



Cloudflare One introduced



1994

2010

2011

2020

2025




The rise of cloud, mobile, and SaaS blurs the traditional network perimeter

Zero Trust becomes a mainstream enterprise strategy, shifting the focus from network location to the user and device identity

Fail 1

“We'll Figure It Out Later”



Ok, what
do we do
now?

We'll figure
it out as we
go.

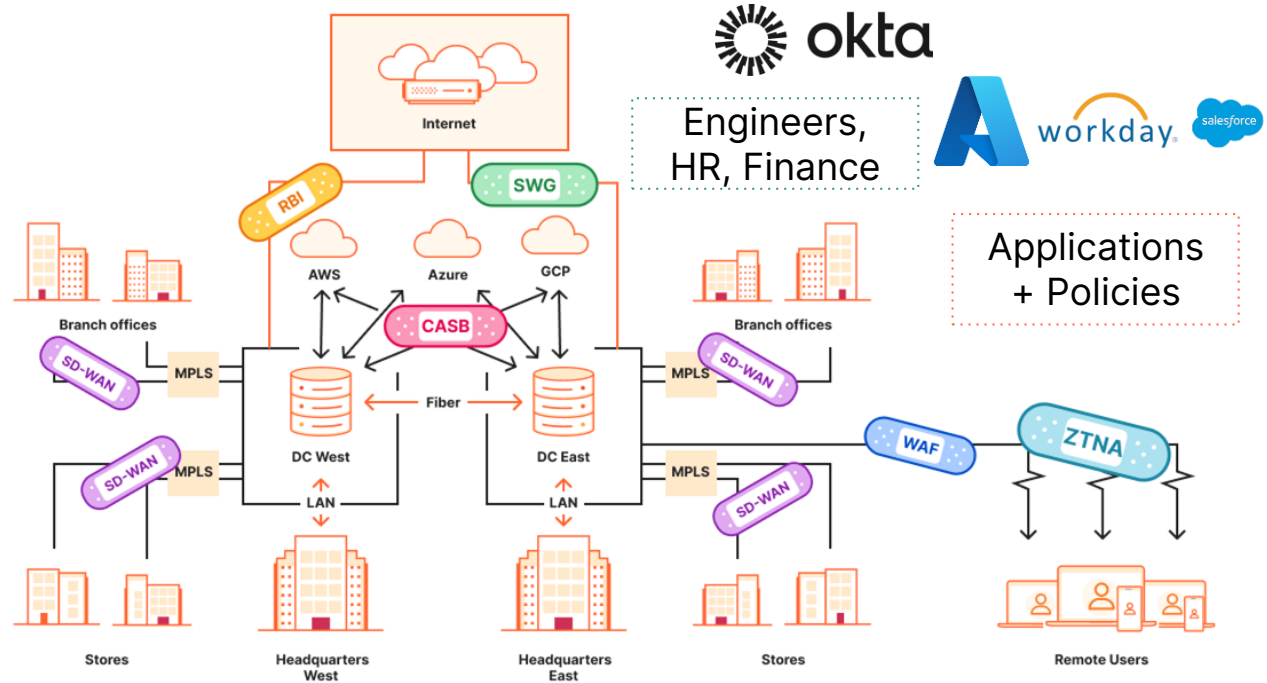
Many Projects fail before Start

Legacy:

- Evolutionary development of infrastructure -> tech debt

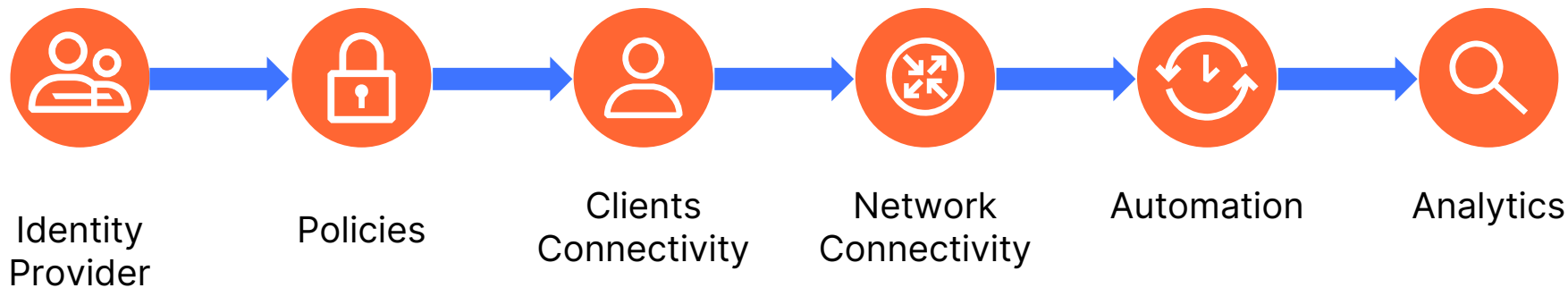
Future:

- Which Applications to protect?
- How users will authenticate?
- How can I connect my on-prem resources?

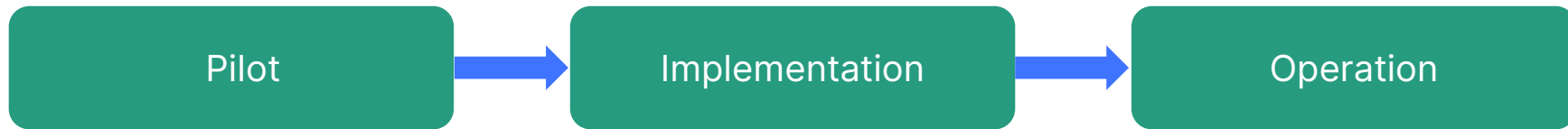


Good Practice

Use framework to properly scope project:



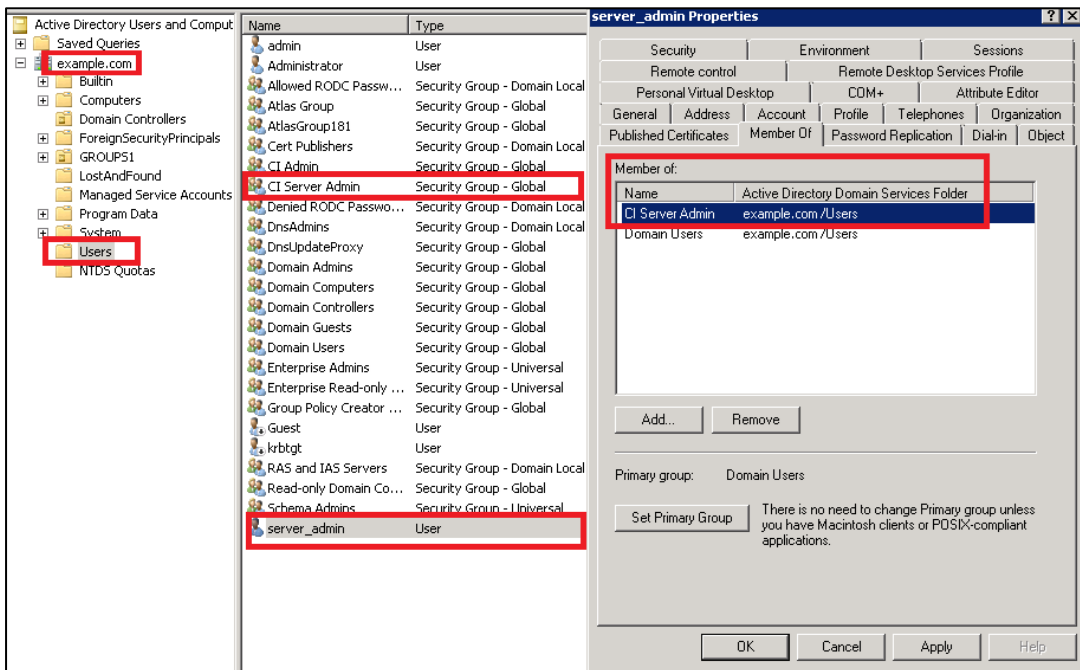
Don't forget about right sequence:



And What about Tech Debt?

Garbage In - Garbage Out:

- remove unused groups
- remove obsolete users



The screenshot shows the Active Directory Users and Computers console. The left pane shows the tree structure with 'example.com' and 'Users' highlighted. The right pane shows a list of users and groups, with 'CI Server Admin' and 'server_admin' highlighted. The 'server_admin Properties' dialog box is open, showing the 'Member of' tab with 'CI Server Admin' and 'example.com/Users' listed.

Name	Type
admin	User
Administrator	User
Allowed RODC Passw...	Security Group - Domain Local
Atlas Group	Security Group - Global
AtlasGroup181	Security Group - Global
Cert Publishers	Security Group - Domain Local
CI Admin	Security Group - Global
CI Server Admin	Security Group - Global
Denied RODC Passwo...	Security Group - Domain Local
DnsAdmins	Security Group - Domain Local
DnsUpdateProxy	Security Group - Global
Domain Admins	Security Group - Global
Domain Computers	Security Group - Global
Domain Controllers	Security Group - Global
Domain Guests	Security Group - Global
Domain Users	Security Group - Global
Enterprise Admins	Security Group - Universal
Enterprise Read-only ...	Security Group - Universal
Group Policy Creator ...	Security Group - Global
Guest	User
krbtgt	User
RAS and IAS Servers	Security Group - Domain Local
Read-only Domain Co...	Security Group - Global
Schema Admins	Security Group - Universal
server_admin	User

server_admin Properties

Member of:

Name	Active Directory Domain Services Folder
CI Server Admin	example.com/Users
Domain Users	example.com/Users

Primary group: Domain Users

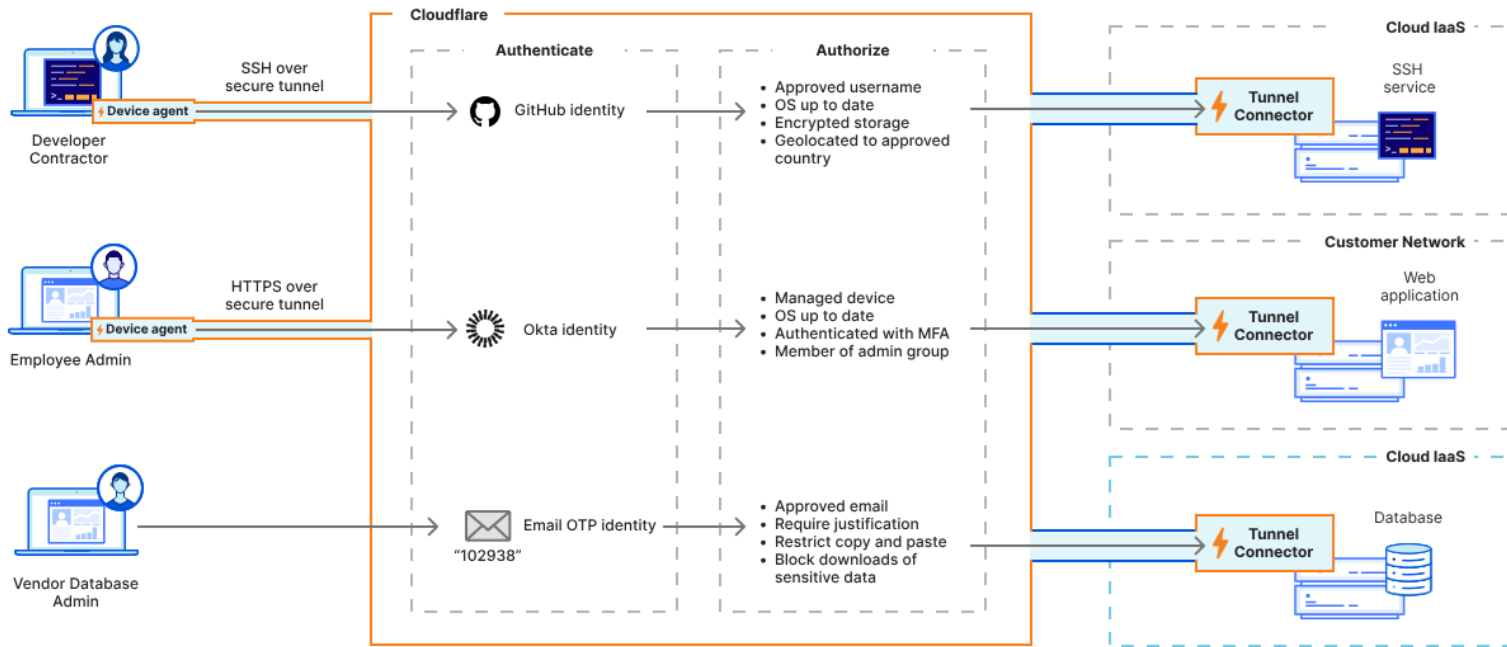
Set Primary Group: There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Fail 2

Put all your identity eggs in one basket



What is Identity Provider



Potential Problems with IdP

- Change ZT Team Domain -> Change Redirect URL in IdP
- Expired Token
- Rate-limiting

Home > Enterprise applications | All applications > App registrations > Cloudflare Access



Cloudflare Access | Authentication

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses. The redirect URI you send in the request to the login server should match one of the URIs listed here. [Redirect URIs and their restrictions](#)

<https://demoflare.cloudflareaccess.com/cdn-cgi/access/callback>

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Certificates (0)

Client secrets (1)

Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can

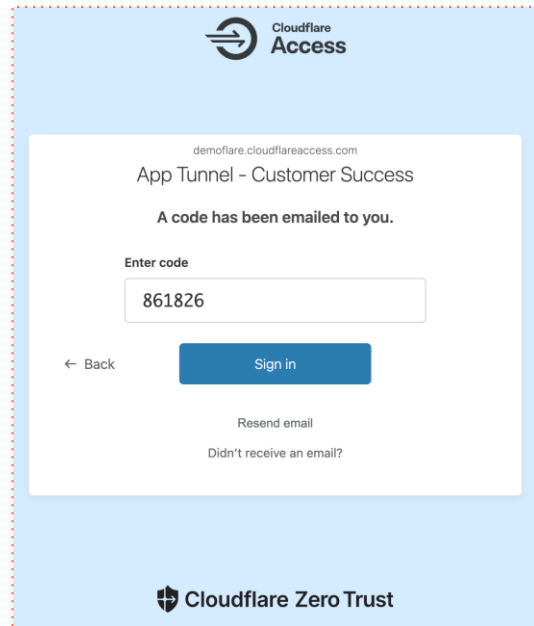
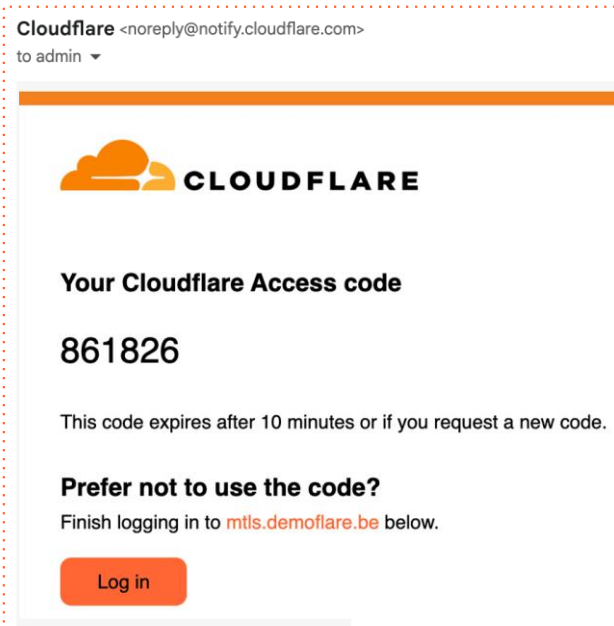
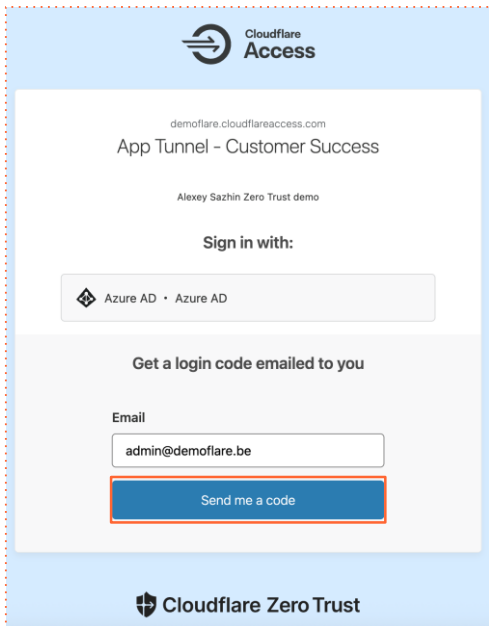
+ New client secret

Description	Expires	Value ⓘ
new client secret	9/9/2027	llg*****

Good Practice

Plan for IdP fallback:

- Use multiple IdPs
- fallback mechanism - email OTP



Fail 7

Unmonitored Genie



Challenges of AI

Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History

A publicly accessible database belonging to DeepSeek allowed full control over database operations, including the ability to access internal data. The exposure includes over a million lines of log streams with highly sensitive information.



Gal Nagli

January 29, 2025

3 minute read



ChatGPT Leaks Sensitive User Data, OpenAI Suspects Hack

The leaks exposed conversations, personal data, and login credentials.



Anuj Mudaliar Assistant Editor - Tech, SWZD

February 1, 2024



BBC

Hundreds of thousands of Grok chats exposed in Google results

21 August 2025

Share  Save 

Liv McMahon Technology reporter

07-30-2025 | PREMIUM

Exclusive: Google is indexing ChatGPT conversations, potentially exposing sensitive user data

Thousands of shared ChatGPT chats are now appearing in Google search results.

SHARE 

Alexey Playground ▶

Zero Trust Home

Analytics ▼

Risk score ▼

Gateway ▼

Access ▼

Networks ▼

My team ▼

Logs ▼

CASB ▼

Data loss prevention ▼

DEX ▼

Email Security New ▼Browser Isolation New ▼

Settings

Zero Trust Home

Welcome to Cloudflare Zero Trust

Connect and secure your users, networks, and data with Zero Trust security.

[Zero Trust documentation](#)[Overview](#)[Get started](#)[Recent searches](#)

7 of 50 available seats are in use.



NEW! The latest version of the WARP client brings you improved stability and performance. Visit [Downloads](#) to download it.

[Last hour](#)[Last 24 hours](#)[Last 7 days](#)[Last 30 days](#)

Top logins by application

[View all](#)

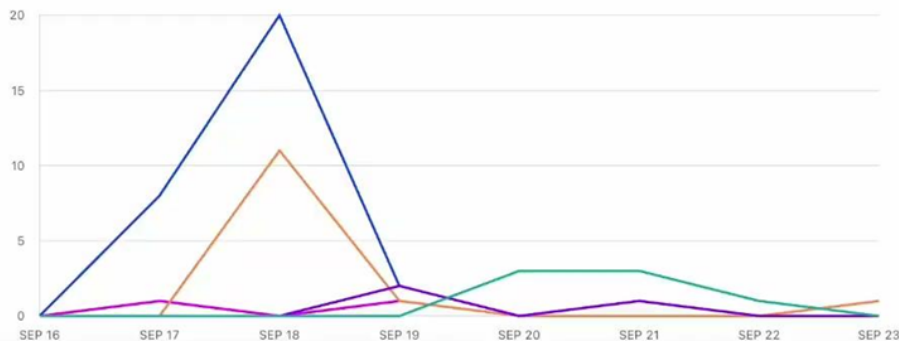
• Warp ...n App

• API_M..._HTTP

• Uploa..._HTTP

• App L...ncher

•



Application trends

No increase in logins over this time period.

94% ↓

Logins to demoflare.cloudflarea...

Collapse sidebar

Conclusion

Conclusion

- Zero Trust is not a project: it is a journey of continuous improvement
- Strong foundation is critical. Don't skip the planning and discovery phase
- Zero Trust is as much about people and processes as it is about technology.

Thank you

→ 1 888 99 FLARE

✉ enterprise@cloudflare.com

🌐 cloudflare.com