90-Minute Zero Trust Assessment

Implementing a Zero Trust security model can be a complex transformational journey. Our solution specialists will help evaluate your current security posture to get started.

Zero Trust is a Set of Principles

	Trust, but verify →	Never trust, always verify
Protection	Secure perimeter, safe inside network	Assume breach, encrypt end-to-end
Visibility	Log only login at the perimeter	Log every request everywhere
Control	Default allow, statically deny access based on network location	Default deny, dynamically grant access based on identity and context

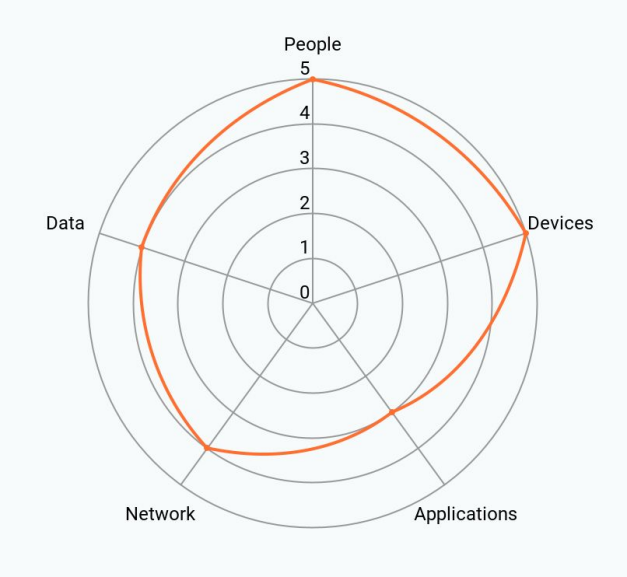
Business Drivers to Start Zero Trust

Enable Agility for Work-from-Anywhere	Immediate visibility and protection that scales as your remote workforce grows and your applications shift to the cloud
Third-Party Access	Segregated authorization for contractors or partners for safer collaboration
Identity Federation	Integrated authentication across identity providers for migrations or M&A activity
Strengthen Security	Modernize your VPN solution to contain breaches by stopping lateral movement
Simplify Administration	Consolidate sprawling security solutions to address cybersecurity skills gap

Assessment Outcomes

Maturity Score	Pain points and strengths of current security posture
Cost Optimization	Identification of cost savings for migrating to Cloudflare
Risk Identification	Risks and pitfalls before migrating to a Zero Trust model
Operating Model	Align people, process and technology on the new ways of working in a ZT mindset
Future State Architecture	High level design of Cloudflare integrated into your existing architecture
Proof of Concept Plan	High level plan to implement Cloudflare's Zero Trust platform today

Example Maturity Scoring



Assessment Framework

We will examine these key Zero Trust components:

People	Identify and categorize who is accessing data and applications (employees, contractors, partners)
Devices	What is used to access resources? (managed, unmanaged, mobile, IoT)
Applications	Where is access control required? (public cloud, on-prem, hybrid)
Networks	Can people move laterally across multiple applications and resources?
Data	What is your approach for protecting your most sensitive data resources?

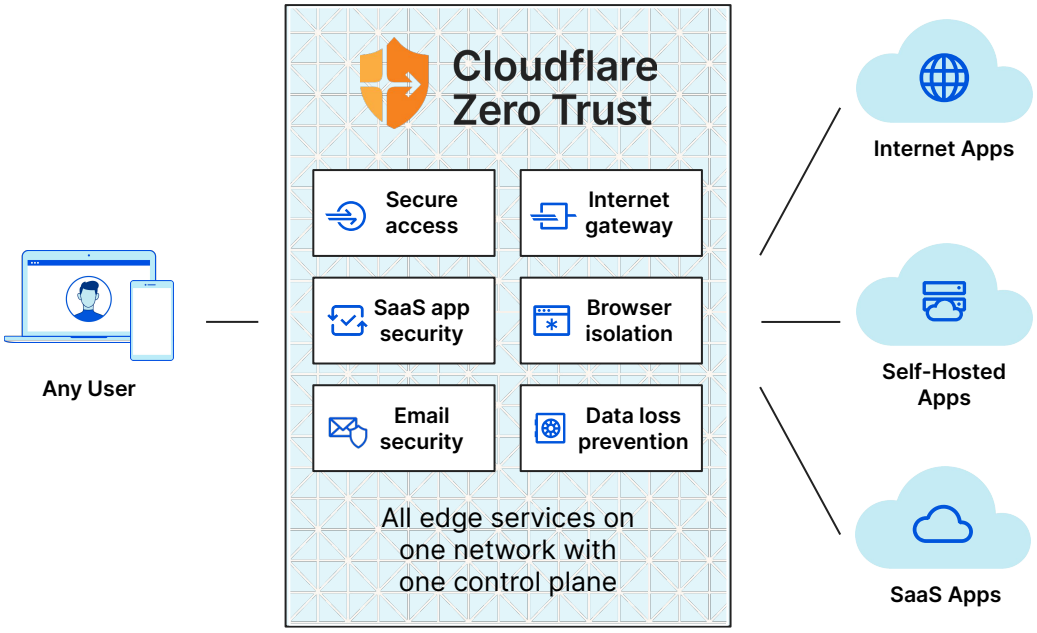
And apply the following assessment criteria to each:

Authentication	• Multi-factor authentication • Micro segmentation
Authorization	• Role-based access control • Access control granularity • Least privileged access
Automation Orchestration	• Automated remediation • DevSecOp principles
Analytics Visibility	• User behavior • Advanced threat detection
Operations Processes	• Skills to mitigate breaches • Who changes access control

Implementation Roadmap

During our engagement we will provide a high-level design for how Cloudflare can integrate with your existing architecture, including the identity access and management providers you use for your people, endpoint protection and management providers you use for your devices, and cloud providers you use for your applications and data.

Then, we'll plan out how to get started immediately with a proof of concept.



Contact us today to request your one-on-one engagement with a Cloudflare solution specialist.