Zero Trust Automation At-A-Glance

AT-A-GLANCE

Due to the ever-increasing number of IT products in recent years, security, network, and IT teams have been shifting away from disjointed administrator interfaces and seeking to manage solutions programmatically (via code). That's because manual administration fosters operational complexity that hinders agility, wastes time and resources, and is vulnerable to sophisticated threats. Programmatic administration, on the other hand, provides consolidated ease of use and, more importantly, enables the automation of solutions. As a result, automation now effectively serves as an administrator for countless organizations' IT ecosystems.

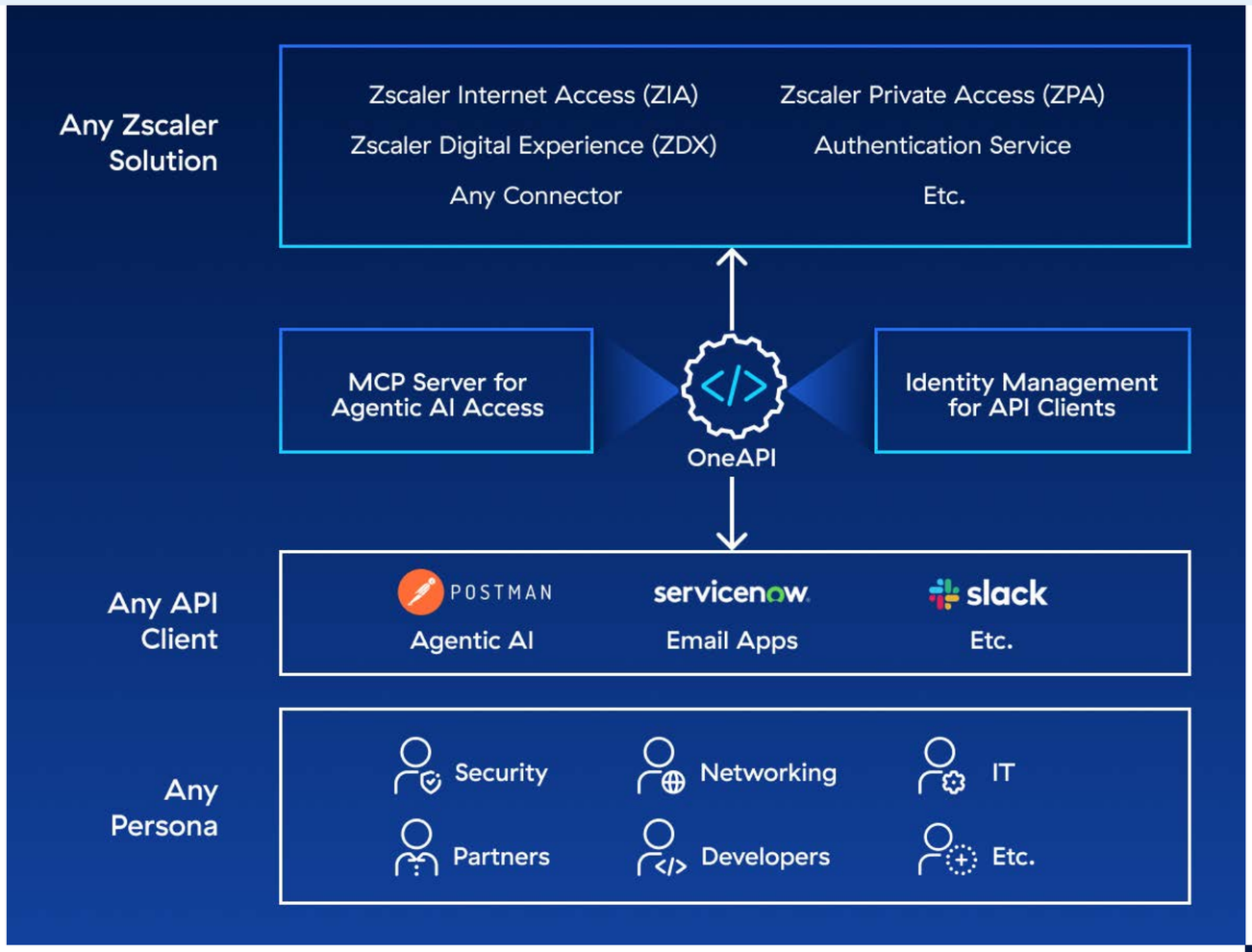
The Zscaler Zero Trust Exchange, the AI security platform built on zero trust, is the ideal fit for this automation-centric reality.

Zscaler's API-centric design

The Zero Trust Exchange was designed from the beginning to operate in an API-first fashion. Its administrative interface, which humans have been using for years, actually interacts on the backend with Zscaler infrastructure via API. As such, every new service and feature is built to be accessible through API. This elegant approach is perfectly suited for deploying, managing, and accessing Zscaler solutions via code—and this is accomplished through OneAPI, specifically.

OneAPI and Zero Trust Automation

OneAPI is the singular application programming interface for the entire Zero Trust Exchange platform. It provides a common API endpoint (api.zsapi.net) for programmatic access to ZIA, ZPA, ZDX, Client Connector, and any other Zscaler solution. That means practitioners don't have to worry about the intricate inner workings of product provisioning, policy structures, tenant configurations, and so on.



This streamlined approach makes it easier to deploy, manage, and use Zscaler's portfolio of solutions via code. As a result, OneAPI can enable automation to act as any other administrator—with identity, auditing, visibility, and change control available for any API clients, including homegrown apps, AI agents, Postman, ServiceNow, Slack, and PagerDuty.

The Zscaler Automation Hub

The Automation Hub has all the resources organizations need to simplify and accelerate their automation journeys with Zscaler. An AI-powered copilot answers questions and surfaces needed content. Code snippets (in Go, Python, cURL, etc.) help admins automate API operations in Zscaler (like GET, PUT, POST, etc.) merely by copying and pasting. Playbooks serve as templates for automating more involved, multi-step processes. SDKs have prebuilt components and libraries to help developers automate workflows with Zscaler far more easily.

Visit **automate.zscaler.com** to experience the Automation Hub first-hand.

Automated configuration change

Manually setting and updating configurations can be time-consuming and error-prone when managing IT solutions in dynamic environments. Naturally, this creates challenges for maintaining proper security and connectivity. Fortunately, with OneAPI, engineers can automate the creation and modification of Zscaler configurations; for example, adding risky internet destinations to block lists, modifying user entitlements, deploying App Connectors, and more. By automating change implementation across the Zscaler platform, organizations can reduce administrative burden, accelerate responses to evolving requirements, and ensure robust security and connectivity across the IT ecosystem.

Automated analytics data retrieval

Practitioners are tasked with drawing information from their various IT solutions in order to build comprehensive dashboards and provide visibility to internal stakeholders. However, manually collecting data from disjointed tools wastes significant amounts of time for admins.

In light of this need, OneAPI enables automation to pull analytics from products throughout Zscaler's platform. This empowers engineers to streamline the building of widgets and dashboards that need Zscaler data. As examples, OneAPI can retrieve granular details about user experience issues or threats blocked over a customizable period of time.

Automated notification generation

Manually tracking and alerting on security and performance issues takes time, delays awareness for key stakeholders, and sometimes misses incidents entirely—particularly in large or dynamic environments. With OneAPI, organizations can automate the real-time creation and delivery of Zscaler notifications for any events they choose. As examples, they can generate alerts for account compromise, DLP policy violations, App Connector health issues, and network slowdowns in specific regions. This ensures prompt notifications and rapid responses—but it can also trigger closed-loop automation workflows in Zscaler that implement changes and remediate issues without human intervention.

API client identity and access management

API client authentication and authorization are handled centrally by Zscaler's authentication service, which governs the registration, management, and access scopes for API clients—just as it does for human users. This unified approach enables security teams to configure, monitor, and adjust API client permissions without the need for separate activation or provisioning.

API clients authenticate using OAuth 2.0, which provides both coarse- and fine-grained role-based access control (RBAC). This strengthens security by ensuring automation is subject to the same accountability, auditing, and behavioral restrictions as any other admin.

Every API call is logged and tracked to the originating API client, with full activity traceability, audit logs, and request IDs propagated across the system—ensuring complete visibility and control.

Global performance and compliance

As part of the Zero Trust Exchange, the world's largest AI security platform built on zero trust, OneAPI boasts a massive global footprint. OneAPI leverages this distributed, cloud native platform to minimize latency and maximize availability everywhere in the world. When an API client makes an API call, it is automatically routed to the nearest Zscaler data center for streamlined performance. Additionally, OneAPI supports 100% in-region routing and processing to support geo-restrictions and help meet regional compliance requirements (this capability is available upon request).

Wrap-up

OneAPI enables organizations to make automation an administrator of their Zscaler implementation. As a result, they can automate the full Zscaler deployment lifecycle, across configurations, analytics, and notifications, to improve their speed and scalability, ROI, and security.

To learn more about Zero Trust Automation with OneAPI, visit zscaler.com/automation and explore our webpage.

To dive deeper, go to automate.zscaler.com and explore the Zscaler Automation Hub.

Why adopt Zero Trust Automation?

ENHANCE SPEED AND SCALABILITY

Problem

- Organizations regularly add new users and applications
- IT integration after M&A activity often delays time-to-value
- Rolling out new branch locations can take too much time

Solution

- Templates reduce manual efforts for secure onboarding
- Standardized workflows accelerate IT integration for M&A
- Automation enables fast and repeatable site deployments

BOOST RETURN ON INVESTMENT (ROI)

Problem

- Practitioners struggle to manage all their various solutions
- Manual administration means costly management overhead
- Admins mired in mundane tasks have less job satisfaction

Solution

- Programmatic access enables unified solution management
- Automation saves both time and money for organizations
- Automating tasks frees admins to perform higher-value work

IMPROVE CYBERSECURITY POSTURE

Problem

- Cyber risk and regulations call for rapid zero trust adoption
- Manual administration can foster errors that harm security
- Sophisticated threats can strike unexpectedly at any time

Solution

- Automation speeds up the implementation of zero trust
- Predefined code and playbooks prevent human errors
- Automated threat response ensures instant remediation

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

Act Fast. Stay Secure.