Zero Trust Automation At-A-Glance

AT-A-GLANCE

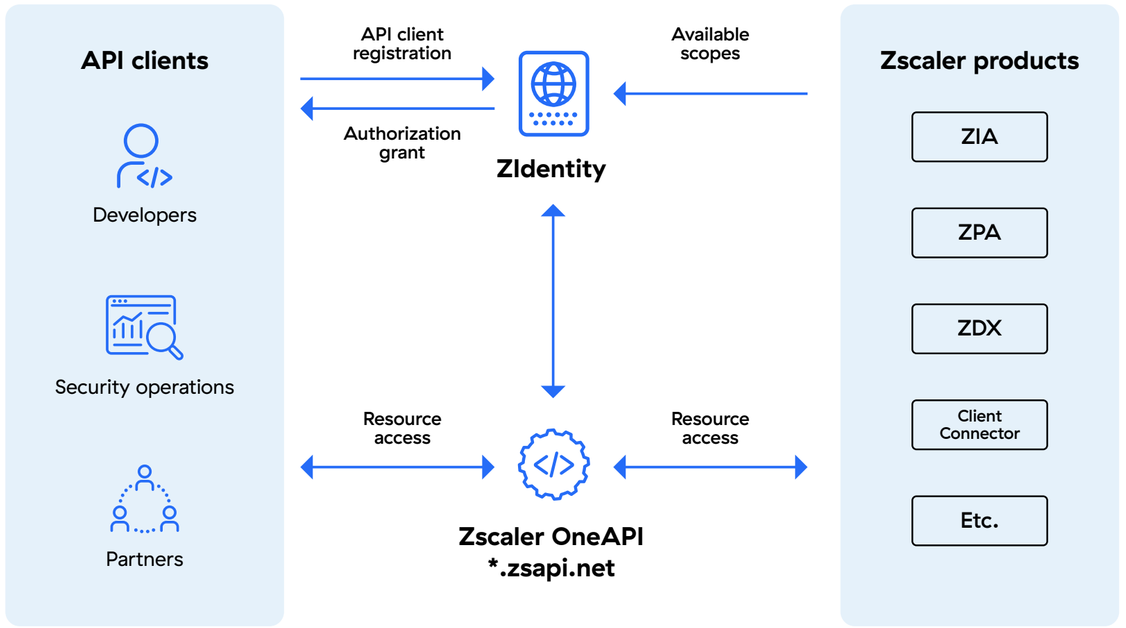
To help administrators manage the ever-increasing numbers of IT products and applications in recent years, organizations have been shifting away from human interactions with disjointed user consoles and embracing automation. This has enabled IT teams to cope with tool sprawl, simplify reporting and analytics, and reduce opportunities for human errors that could otherwise lead to costly security breaches.

Today, in an era when AI is used to write code and perform regular job duties, automation is now effectively a new administrator. Reflecting this reality, Zscaler introduced OneAPI, an automation service that's specifically designed for automation engineers.

Automation with Zscaler

The Zscaler Zero Trust Exchange was designed from the beginning to operate in an API-first fashion. Its web console, which human security engineers have been using for many years, actually interacts on the backend with Zscaler's infrastructure via APIs. As such, every new service and feature is built to be configured and accessed via API. This elegant approach is perfectly suited for enabling automation engineers to efficiently deploy, maintain, and access Zscaler solutions programmatically via code.

With OneAPI, Zscaler takes this approach to the next level, further improving security and operational efficiency for automation engineers.



Zscaler OneAPI

Zscaler offers OneAPI, a single programming interface for the entire Zero Trust Exchange platform, instead of using a legacy model with multiple, solution-specific APIs. This streamlined approach accelerates the deployment, maintenance, usage, and expanding adoption of Zscaler solutions. OneAPI enables automation to act as another administrator, with identity, auditing, visibility, and change control all available for any API clients, including ServiceNow, Postman, and homegrown applications.

Zscaler OneAPI has a global footprint, leveraging a distributed cloud native platform for low latency and high availability. API calls are routed to the closest region and respect geographic data sovereignty requirements.

One common API endpoint

OneAPI provides a common API endpoint (api.zsapi.net) that enables platform engineers to access ZIA, ZPA, ZDX, Zscaler Client Connector, and more. They no longer have to worry about the intricate inner workings of product provisioning, policy structure, tenant configurations, and so on. For use cases like automating policies that disable access to risky internet destinations, or automating the creation of private app segments, engineers can simply program against api.zsapi.net.

Programmatic access to analytics data

Beyond managing configurations, practitioners are also tasked with drawing information from various 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 also enables automation to pull analytics from products throughout Zscaler's platform. This empowers engineers to streamline the building of their own widgets and dashboards that need Zscaler data. As examples, it can gather findings like granular details of top incidents, as well as threats blocked over a customizable period of time.

OAuth 2.0

Authentication and authorization of API clients follow OAuth 2.0 standards for both coarse and fine-grained role-based access control (RBAC). This enables security teams to hold automation accountable at the same level as a human administrator. Every API call is logged against the identity of the API client and is tracked to completion. The activity trace is auditable, and behavioral restrictions can also be enforced—just as they could for human users.

API clients on ZIdentity

OneAPI relies on Zscaler ZIdentity, a unified identity platform, for the identity registration and ongoing management of API clients. No separate activation or provisioning is required—customers using ZIdentity can configure API clients as they would human clients. ZIdentity acts as the central decision point for the scopes an API client is granted (which can be adjusted at any time). Full visibility and control is maintained, with audit logs and request IDs propagated throughout the system.

Why adopt zero trust automation?

	PROBLEM	SOLUTION
Greater speed and scalability	• Security incidents and regulations call for rapid zero trust adoption • Time from purchase to deployment can be too long • Integrating organizations after M&A is often delayed • Rolling out branch locations can take too much time	• Reducing duplication of manual effort across products • Using templates to accelerate the resolution of use cases
Reduced complexity	• Having point solutions makes administration more difficult • Complexity fosters poor policy coordination and security gaps • Lacking shared security accountability overly burdens security teams	• Unifying policy creation in a single place via API • Using RBAC on APIs to coordinate policy and improve security • Empowering other functions to build their own security policies
Resource optimization	• Manual efforts can foster errors, harming security and productivity • Admins mired in mundane tasks have less job satisfaction • Expensive human talent is often significantly underutilized	• Simplifying code reviews ahead of deployment • Having restore points for code in case of a need to roll back • Using automation as an admin and first line of defense • Focusing engineers on more challenging, rewarding work

Zscaler OneAPI enables customers to make automation an administrator, accelerating time for deployment and integrations, and reducing opportunities for human error that could create risk. With OneAPI, customers can unlock new use cases, such as microsegmentation projects, simplifying reporting and analytics, auditing their environment, and optimizing their team's return on investment.

To learn more about zero trust automation with Zscaler OneAPI, visit zscaler.com/automation or speak to your Zscaler account team. Engineers can dive deeper at our help site, help.zscaler.com/oneapi

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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

zscaler™

Zero Trust Everywhere