The Top Zero Trust Automation Use Cases

How to Automate Your Use of Zscaler with OneAPI

EBOOK

Table of Contents

An Overview of Zero Trust Automation and OneAPI

IT professionals oversee complex, ever-expanding suites of tools. To save themselves time and reduce the need to pivot between interfaces, they are increasingly demanding the ability to manage solutions programmatically (via code). In addition to enabling consolidated ease of management, programmatic access facilitates the automation of IT solutions and enables them to be operated by AI agents (both of which save even more time for practitioners). In light of all this, Zscaler built its Zero Trust Automation solution so that admins can programmatically deploy and manage the Zero Trust Exchange platform via OneAPI.

OneAPI is a single API endpoint that provides programmatic access to the entire Zscaler Zero Trust Exchange. This unified programming interface eliminates the need for managing multiple API endpoints and enables seamless access to Zscaler solutions like ZIA, ZPA, ZDX, Zscaler's authentication service (formerly ZIdentity), Client Connector, Branch Connector, and Cloud Connector. And if a change is made that needs to be undone, practitioners can easily reverse it by reverting to a previous version in their code repository and re-applying the configuration.

To leverage OneAPI, practitioners just code against api.zsapi.net.

OneAPI is designed to provide compatibility with any API client that needs access to the Zero Trust Exchange. This includes home-grown apps, SaaS apps like ServiceNow, automation and infrastructure-as-code (IaC) tools like Postman, Terraform, and Ansible, and even AI agents.

The Zscaler Automation Hub (automate.zscaler.com) makes it as easy as possible to embrace Zero Trust Automation via the API client of any admin's choosing. The hub provides:

- An AI-powered copilot that answers questions and surfaces relevant content
- Collections of code snippets for automating simple tasks like pulling policy violations
- Playbook templates for automating more involved processes like deploying connectors
- Python and Go SDKs for building custom applications that need to access Zscaler
- Comprehensive help documentation for any automation use case

Leveraging Zero Trust Automation entails the use of Zscaler's authentication service, which provides unified authentication, authorization, and access management across Zscaler's solutions. It ensures secure interactions with OneAPI by leveraging OAuth 2.0 to authenticate API clients, and by supporting role-based access control (RBAC) to granularly determine which API clients can perform which operations. Additionally, the authentication service enables audit through compliance-ready logs that contain all API calls (and request IDs for each one).

Zero Trust Automation operates as part of the Zero Trust Exchange, the AI security platform built on zero trust, which is the world's largest security cloud, comprising over 160 full-compute data centers around the globe. This ensures maximum reliability and performance anywhere in the world—API clients authenticate once and are routed to the closest point of presence (PoP). As a result, API-based workflows are executed both seamlessly and securely.

With Zscaler, organizations can automate three different categories of tasks:

1. **Changing configurations:** API clients can make updates in Zscaler across policies, URL categories, app segments, and other settings, enabling rapid changes that require no manual intervention.
2. **Retrieving analytics data:** API clients can pull data from the Zero Trust Exchange, extracting granular insights from traffic analyses and streamlining the creation of widgets and dashboards.
3. **Generating notifications:** API clients can push custom alerts for App Connector health, trust portal events, infrastructure issues, and more, ensuring real-time awareness of any critical events.

Throughout the rest of this ebook, you can see the top use cases that Zscaler customers automate through OneAPI. By doing so, security, networking, and developer teams can reduce operational complexity, unlock greater speed and scalability, improve ROI, and leverage automated security with superior risk reduction.

Accelerating the Implementation of Zero Trust Architecture

Implementing zero trust is a large-scale, transformative process that can require significant time and effort when it is performed manually. Admins have to configure user groups, app segments, URL categories, PAC files, connectors, policies, and much more, and verify that everything throughout their environment is working properly. Otherwise, there can be problems with security posture and user experience—both of which will be discussed further below.

Zero Trust Automation empowers organizations to simplify this tedious deployment process. After setting up their API clients in the authentication service, admins can use the automation, API, and infrastructure-as-code (IaC) tools with which they are already familiar to deploy Zscaler via code. With this programmatic approach streamlining implementation, admins can roll out Zscaler without needing to manually navigate or familiarize themselves with the UI.

To further accelerate things, Zscaler offers the Automation Hub, a free resource that provides helpful tooling across Postman, Ansible, Terraform, and other solutions. It equips practitioners with collections of proven templates and code snippets so that they can get up and running without having to start from scratch. And as their organizations grow to include more employees, applications, office locations, and so on, previously established workflows can be repurposed and repeated seamlessly. As examples, admins can automate the setup of new Branch Connectors or the configuration of security policies for new apps.

Automating Your Threat Response

When a compromised employee account is detected, the security team must take action as quickly as possible to mitigate the damage of any ongoing attacks. First, they need to invalidate all of the user's active authorized sessions. Then, they must implement a new policy that prevents the user account from reaching any private applications. After that, they should also create a policy that blocks the account from accessing any internet destinations that could represent a further risk. Once these crucial steps are taken, admins can investigate how the user-account was compromised, and take further action to prevent it from occurring again in the future. However performing this entire process takes time that disrupts productivity for practitioners and gives opportunity for threats to do more damage.

With Zero Trust Automation, manual effort can be removed from remediation via end-to-end playbooks that streamline the process. First, the compromise is detected and Zscaler generates an alert through ServiceNow, PagerDuty, or whatever other tool may be preferred. Then, that API client triggers an automated workflow using OneAPI that automatically writes and posts changes within Zscaler to cut off access for the compromised account—without requiring any human intervention. Once quarantine is completed, automation can also reverse the policy changes in order to restore user and device access. All of this happens in the blink of an eye, saving time for administrators and preventing threats from launching full-scale attacks.

Optimizing User Experience and Productivity

Maintaining exceptional digital experiences requires real-time visibility across the full user connection as well as intelligent, granular troubleshooting. Fortunately, Zscaler Digital Experience (ZDX) provides both of these for network and help desk personnel. It offers deep visibility from the user device, across any network path, to any SaaS, cloud, internet, or data center destination. This, along with AI-Powered Root Cause Analysis, enables rapid resolution for any user experience issues. Overall, the result is superior productivity for both end users and admins. However, manually navigating the Zscaler UI to leverage ZDX can pull admins out of their normal workflows, leaving an opportunity to streamline their efficiency even more.

Zero Trust Automation uses OneAPI to automate the retrieval of analytics from ZDX. Admins can programmatically pull this data into their preferred dashboards, whether homegrown or third-party, so that they can proactively monitor key metrics on user activity, device health, app performance, network performance, and the overall health of the sites from which users are working.

Additionally, when performance issues do arise, automation through OneAPI can trigger real-time ZDX notifications that are sent to administrators via ServiceNow, Pagerduty, or any other tool. These alerts deliver in-depth insights, such as when the issue started, where the issue is taking place, how many users are affected, which apps are affected, and how many service requests have been generated. This allows network and help desk teams to act more quickly and more effectively, preventing productivity losses both for themselves and for end users.

Monitoring and Ensuring Deployment Health

Historically, when practitioners wanted to inspect their Zscaler deployments to ensure that everything was working correctly, they needed to sign in and manually inspect health dashboards that showed the conditions of their tunnels, App Connectors, app segments, user devices, and so on. This was a standard part of “keeping the lights on” not only when using Zscaler, but when using any other solution, as well.

Rather than requiring this hands-on effort, OneAPI enables the automatic retrieval of Zscaler analytics data for any API client. It can pull the information admins need into the dashboards and widgets where they like to monitor their different solutions, empowering them to check on Zscaler deployment health within their normal workflows.

In addition to the above, automation can deliver real-time notifications the instant that something goes wrong. As a result, admins don’t have to spend as much time actively monitoring for deployment health issues, and they don’t have to risk finding out about problems secondhand—after complaints arise, productivity slows, and pressure to fix things swells.

Practitioners can receive alerts via Slack, email, pager applications, and more, giving them information about what went wrong and why. And when they need to make changes to Zscaler configurations in order to fix something, they can do so via code in the API clients of their choosing, giving them the flexibility and control to move as quickly as possible. Additionally, with support for code restore points, admins can roll back to previous, proven configurations by reverting to a prior version in their code repo.

Letting AI Agents Manage Your Zscaler Deployment

As organizations strive for faster threat response, greater operational simplicity, and reduced management overhead, they are harnessing the power of AI to automate cybersecurity operations. Specifically, IT admins are now using AI agents to manage their security solutions and perform complex workflows on their behalf. However, that requires that those solutions have model context protocol (MCP) servers, which enable AI agents to access tools via their APIs. At Zscaler, we are acutely aware of this demand for AI-driven security automation and its technical requirements.

With the powerful combination of OneAPI and the Zscaler Integrations MCP Server, admins can grant comprehensive Zscaler management to AI agents, including Claude Desktop, Cursor, Visual Studio Code, and other MCP-compatible clients. These agents receive identities like any other API client in the authentication service. They are authenticated via OAuth 2.0 and receive role-based access control (RBAC) to ensure that every action they perform is secure and controlled. Each API call they make is logged and assigned a request ID to enable visibility, audit, and regulatory compliance. And with the ability to undo AI agents' changes and revert to prior Zscaler configurations, admins never have to lose control.

In other words, with Zero Trust Automation, AI agents can manage the full Zscaler deployment lifecycle, streamlining operational efficiency and enhancing cybersecurity posture.

Simplifying IT Integration During M&A

Traditionally, when two organizations come together through M&A, IT integration means integrating their networks so that their employees can access each other's network-connected resources. But this complex approach leads to scope creep, extended integration timelines, and ballooning costs. Zscaler circumvents these challenges because its zero trust architecture provides access directly to apps without requiring network access; as a result, organizations don't need to integrate their networks during M&A. Nevertheless, admins must ensure that this direct-to-app access is provided as quickly and securely as possible. But that process involves manually configuring user groups, applications, and access policies—all while trying to minimize business disruption.

Zscaler's Zero Trust Automation solution further simplifies IT integration by enabling admins to create and use standardized templates. So, with purpose-built security and access policies prepared ahead of time, IT teams can onboard a new organization merely by enabling its users in the identity provider (IdP). From there, Zero Trust Automation automatically pulls the new users into Zscaler, where the preconfigured policies are instantly applied—without additional manual intervention.

This automation reduces administrators' time and labor requirements while ensuring that every user is secured by the same zero trust architecture on day one. By templatizing and standardizing IT integrations, organizations gain consistent security enforcement, streamlined IT processes, and faster time-to-value for their mergers and acquisitions.

Automating Zero Trust Across Customers for MSSPs

Managed security service providers (MSSPs) face inefficiency challenges as they oversee the security of their customers. That's because they typically have to log in and out of tenants, over and over, so that they can manually configure settings, monitor deployments, and identify incidents across different organizations.

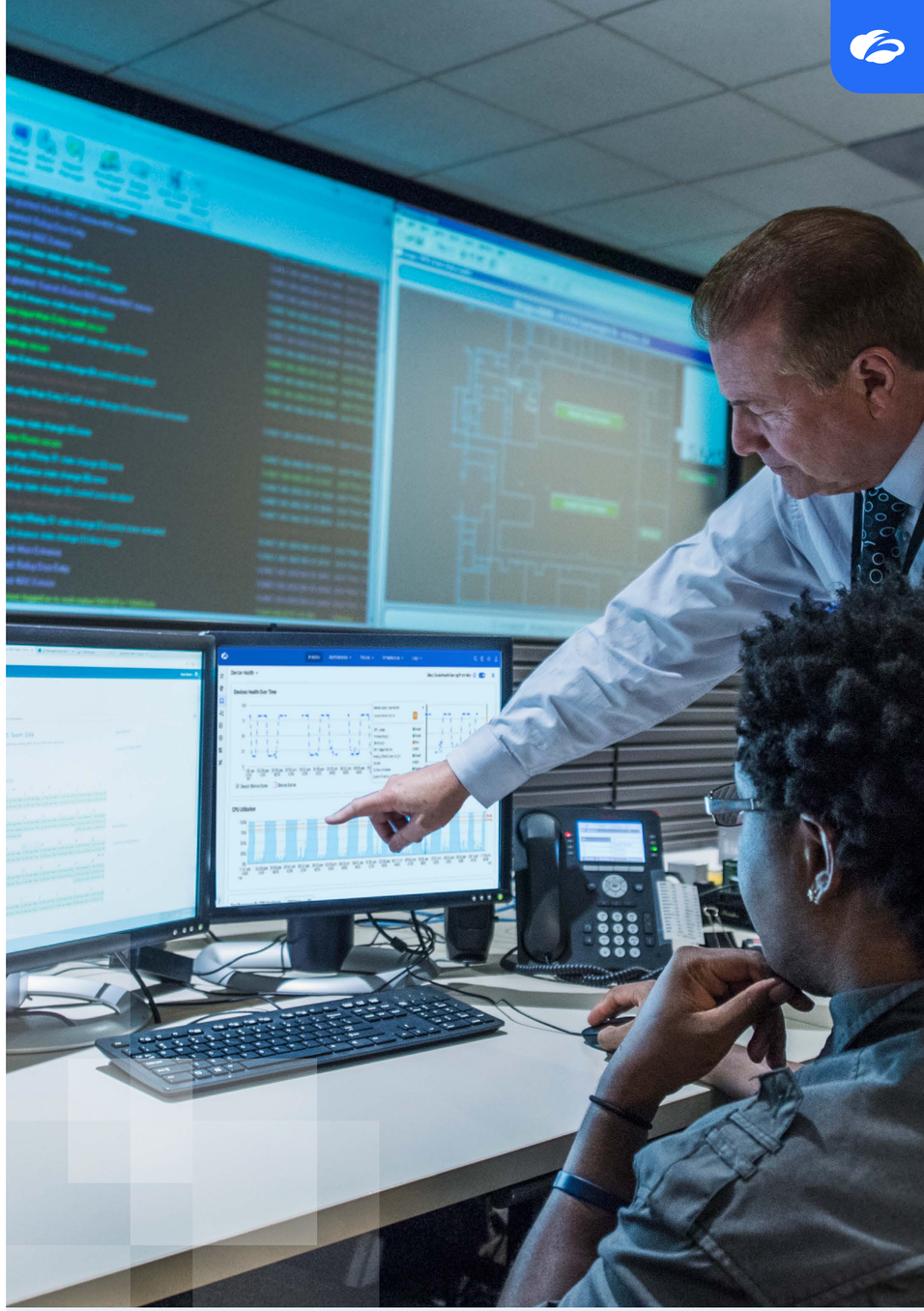
Zero Trust Automation eliminates these challenges through programmatic Zscaler access at scale. That means MSSPs can leverage their preferred automation, API, and infrastructure-as-code (IaC) tools to manage their customers' Zscaler deployments via code—without signing in and out of different tenants. And with helpful out-of-the-box tooling collections for automating different processes, MSSPs can streamline workflows and eliminate the manual effort associated with configurations, analytics, and alerts.

First, they can automate Zscaler deployments and configuration changes by coding in their preferred tools and using templates that set up standardized security policies across their customers. For example, Zero Trust Automation can quickly write and post changes that block malicious or unproductive websites for all of their different tenants.

Next, MSSPs can automate the retrieval of Zscaler analytics data for the dashboards where they monitor each of their customer's various security solutions. In other words, they can unlock granular visibility into customers' Zscaler environments without having to manually log in and out of their different tenants.

Finally, MSSPs can streamline alerts and subsequent remediation workflows. Automated notifications for security incidents and performance issues ensure that admins are immediately made aware of any problems, while remediation steps (like isolating threats or updating permissions) can be executed in an automated fashion based on playbooks.

With Zero Trust Automation, MSSPs reduce complexity, ensure that best practices are enforced across their customers, and enhance their own operational efficiency.



Streamlining Security for CI/CD Pipelines

When a new application is built via continuous integration and continuous delivery (CI/CD) pipelines, security policies and protections must be put in place as the app goes into production. This includes setting up access controls that restrict access to the right users, as well as securing apps against vulnerabilities like SQL injection, cross-site scripting (XSS), and other risks in the OWASP Top 10. Traditionally, app developers must wait for security engineers to configure these defenses, but that means that the app has some period of time when it lacks protection and is vulnerable to threat actors.

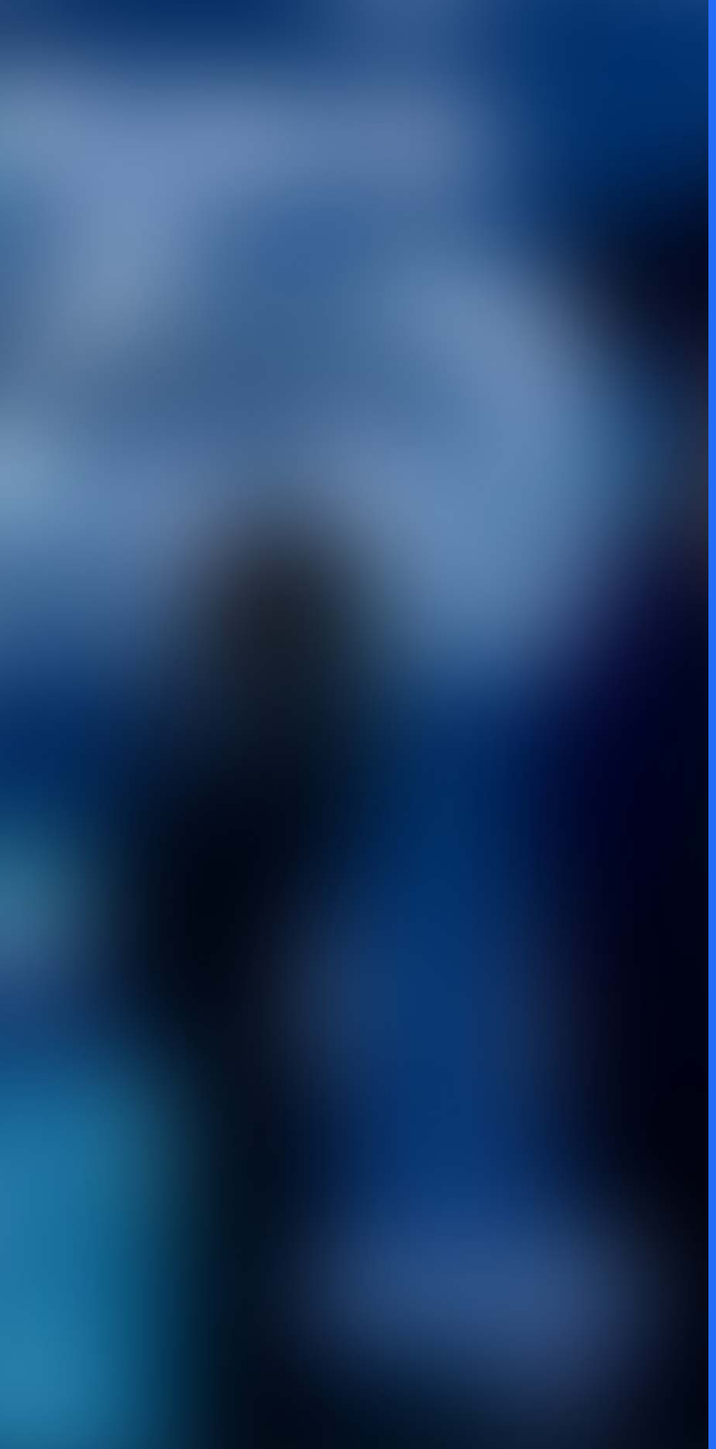
To overcome this challenge, developers need security to be a seamless, built-in part of their CI/CD pipelines. They need to ensure that the appropriate policies are in place and that all required settings are properly configured in a timely fashion. Only then can applications be deployed both quickly and securely.

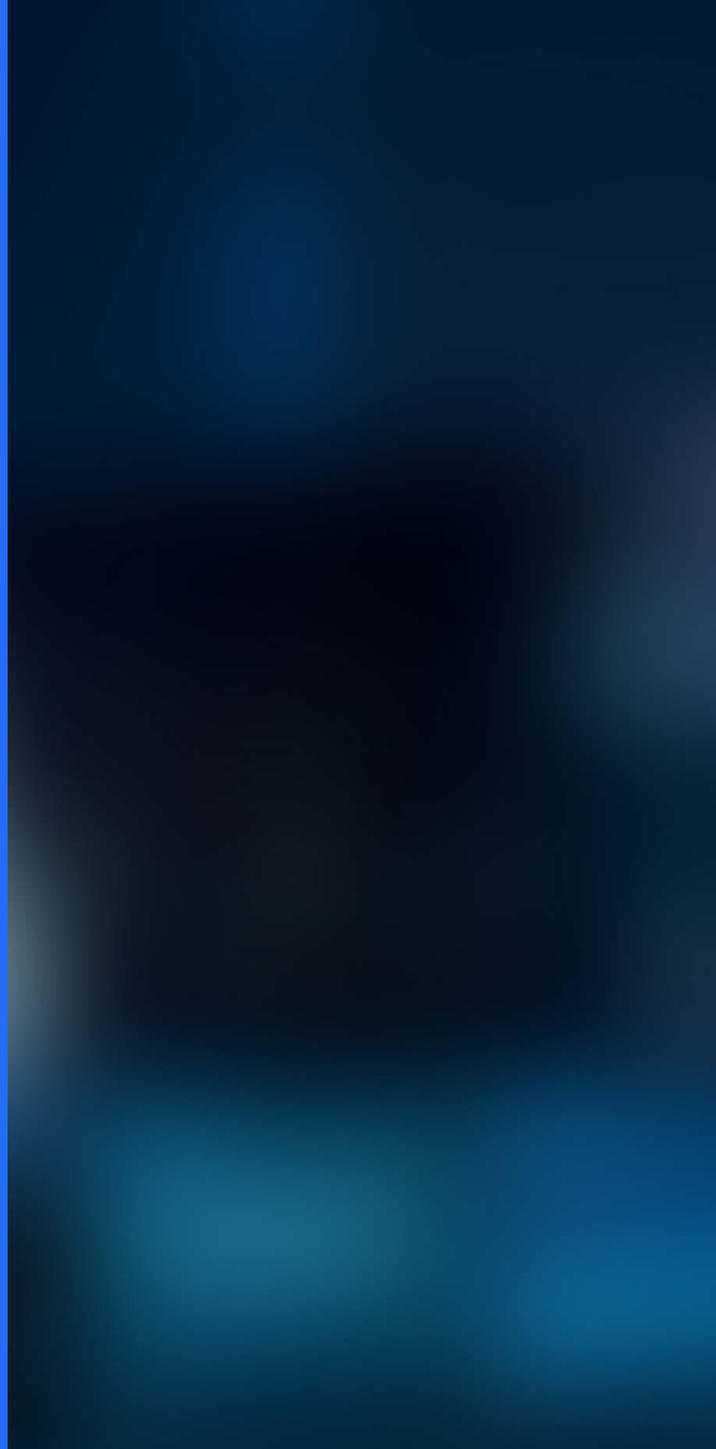
Zero Trust Automation makes the above possible through policy as code (PaC). As they build their apps, developers themselves can programmatically create and apply Zscaler security policies via Jenkins, GitLab, and other tools. With collections of code snippets and playbook templates, they can ensure that their policies are properly configured and aligned with security best practices. They can even automate all of this so that their new apps are secured without human intervention. And if developers make mistakes, they can restore previous, working versions of code in their repos and reapply them to Zscaler—minimizing disruption while maximizing productivity and security.

Wrap-Up

Organizations around the globe leverage OneAPI for programmatic access to any Zscaler solution. This empowers them to automate the full Zscaler deployment lifecycle, from initial implementation to ongoing management, across configurations, analytics, and notifications. Additionally, to the delight of overworked practitioners everywhere, this also enables agentic AI to serve as an administrator.

With greater speed and scalability, reduced operational complexity, and superior security, the benefits of OneAPI are clear. If you want to learn more, you can visit our webpage at zscaler.com/automation or, for a deep dive, go to automate.zscaler.com and explore the Automation Hub.





zscaler™ | Act Fast. Stay Secure.

About Zscaler

Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world's largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across more than 160 data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

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