

Introduction to Zero Trust Exchange (EDU-200)

Application Programming Interface (API) – A set of definitions and protocols for building and integrating application software.

Attack Surface – The total number of all possible entry points for unauthorized access into any system.

Cybersecurity Threat – A malicious act that can harm systems or data through destruction, theft, alteration, disclosure, or denial of access/service.

Data Loss Prevention (DLP) – A security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.

Internet Protocol (IP) – A set of standards for addressing and routing data on the Internet.

Phishing – A type of cyberattack where an attacker poses as a legitimate entity, such as a bank, government agency, or a well-known company, to trick users into revealing sensitive information.

Software-as-a-service (SaaS) – A cloud-based software model that delivers applications to end-users through an internet browser.

Secure Sockets Layer (SSL) – A security protocol that creates an encrypted link between a web server and a web browser.

Transport Layer Security (TLS) – Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.

Virtual Private Network (VPN) – An encrypted connection over the Internet from a device to a network.

Zscaler Digital Experience (ZDX) – A service built as a multi-tenant, cloud-based monitoring platform to probe, benchmark, and measure the digital experiences for every single user within your organization.

Zscaler Internet Access (ZIA) – A cloud native security service edge (SSE) solution that builds on a decade of secure web gateway leadership.



Zscaler Private Access (ZPA) – A Zscaler's service that enables organizations to provide access to internal applications and services while ensuring the security of their networks.

Zero Trust Architecture (ZTA) – A data-centric methodology that focuses on protecting resources over the network perimeter.

Zero Trust Exchange (ZTE) – A cloud-native platform that allows direct and secure connections based on the principle of least-privileged access, which means that no user or application is inherently trusted. Trust is built based on the user's identity and on context, such as the user's location, the security posture of the device, the content being exchanged, and the application being requested.



Experience your world, secured.™

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. Zscaler, Inc. (HQ)

120 Holger Way
San Jose, CA 95134
+1 408.533.0288
[zscaler.com](https://www.zscaler.com)