Zscaler on Zscaler

How Zscaler IT Operates and Secures Its Own Enterprise Using Zscaler Products



©2026 Zscaler, Inc. All rights reserved.

WHITEPAPER

Executive Summary

Zscaler's IT organization runs the same security platform we deliver to customers; at Zscaler scale, pace, and scrutiny. This paper provides a practical view into how we operationalize Zero Trust across users, private applications, internet/SaaS access, branches, and cloud workloads using Zscaler services.

Our goal is not simply to "deploy products," but to operate a repeatable model that delivers:

- **Least-privilege access:** App-level access based on user identity, device posture, and context—default deny with time-bound exceptions and continuous verification
- **Secure access by default:** Eliminate inbound exposure and reduce attack surface while enabling users to work from anywhere
- **High availability and resilience:** Maintain reliable access to critical business applications through resilient service design and operational readiness
- **Measurable digital experience:** Monitor performance from endpoint to app/SaaS to reduce MTTR and improve user satisfaction
- **Operational agility:** Scale operations through clear ownership, automation, and structured escalation paths

Leadership insight: *Decoupling IT responsibilities and product ownership by domain (security, connectivity, endpoints, cloud, SOC, etc.) is essential to operate Zscaler effectively at scale. A shared responsibility model reduces silos, improves accountability, and accelerates troubleshooting.*

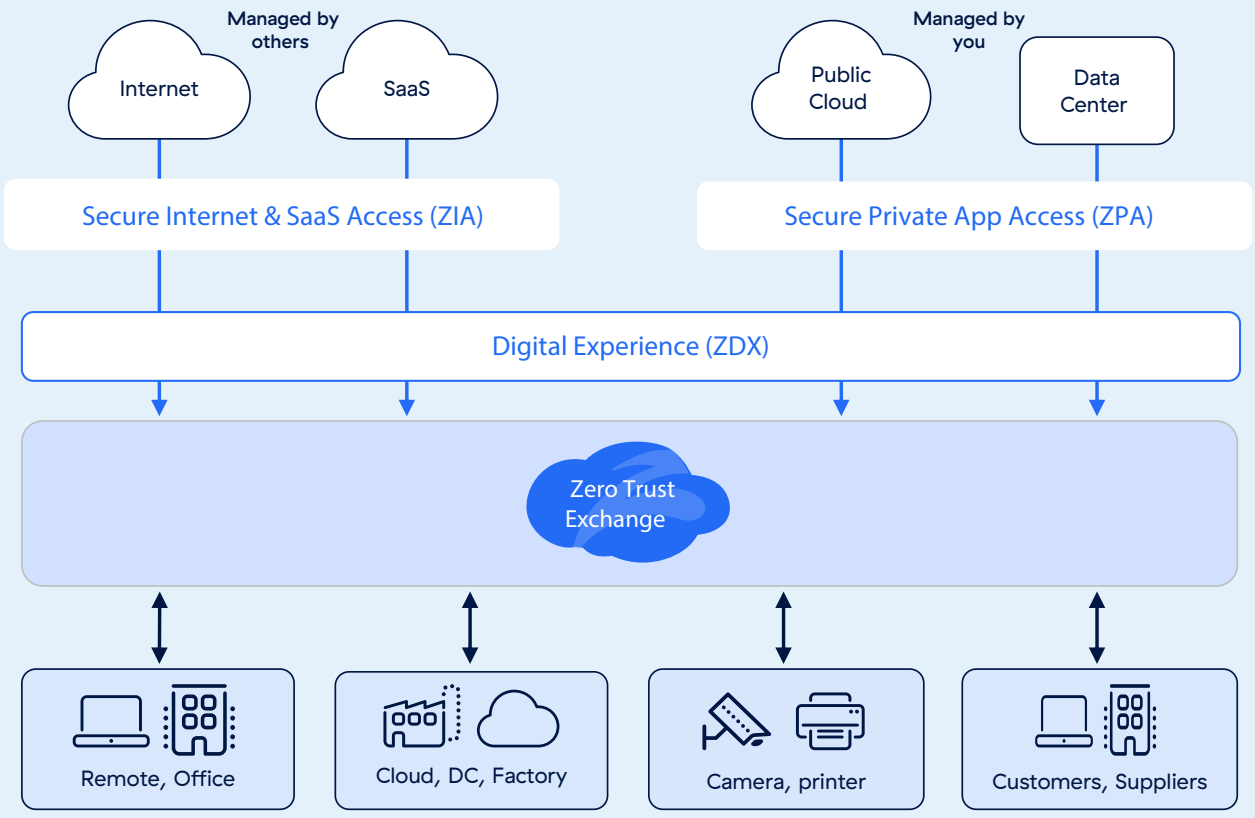
©2026 Zscaler, Inc. All rights reserved.

Reference Architecture (At a Glance)

Zscaler's internal architecture aligns controls, visibility, and ownership across the user–to–app path:

- **Users & Devices:** Zscaler Client Connector (ZCC) enforces access and provides telemetry.
- **Internet & SaaS:** Zscaler Internet Access (ZIA) provides policy enforcement for web/security controls (e.g., SWG, firewall, DLP, cloud app controls, browser isolation).
- **Private Applications:** Zscaler Private Access (ZPA) enables app–level access via App Connectors deployed in cloud environments.
- **Experience Visibility:** Zscaler Digital Experience (ZDX) provides end–to–end experience monitoring (device, Wi–Fi, ISP, path, and application performance).
- **Cloud & Data Security:** Cloud Connector and data security capabilities support cloud posture and data risk management (e.g., DSPM and related controls where applicable).

This architecture supports a core principle: **users connect to applications, not networks, based on identity, device posture, and policy.**



©2026 Zscaler, Inc. All rights reserved.

Operating Model: Shared Service Responsibility

To operate Zero Trust at enterprise scale, Zscaler IT uses a multi-team shared responsibility model. This creates clear separation of duties while enabling fast escalation and deep troubleshooting across domains.

Responsibility Mapping

Team	Primary Responsibility	Key Tool/Focus
Zscaler on Zscaler IT Security	Policy, Segmentation Strategy, ZCC Rollout	ZPA, ZIA, ZCC admin
Application Owners	App Connector health, Internal DNS, Listener config	ZPA App Connectors
Service Desk	L1 Triage & Evidence Collection	ZDX Dashboard
Network Operations	Branch and edge resiliency patterns, OOB and resiliency during support	ZDX Dashboard and AI-driven insights
CISO/SOC	Policy Standards & Threat Monitoring	Analytics, Risk, Alerts
Endpoint Engineering	Device integrity & ZCC Deployment	ZCC Lifecycle, OS Patching

Zscaler on Zscaler (ZonZ) IT Security Team

- Owns ZPA access policy, application segmentation, and ZIA policy (firewall, URL filtering, DLP, browser isolation, cloud app controls, and related enforcement)
- Operates security analytics and risk-focused capabilities (e.g., risk, deception, posture-driven controls where deployed)
- Centrally manages Zscaler Client Connector configuration strategy and global rollout coordination

Application Owners

- Own and operate ZPA App Connectors in their cloud environments
- Integrate business applications and remediate app-side configuration issues (security groups, routes, DNS, app listener configuration, dependencies)

©2026 Zscaler, Inc. All rights reserved.

Service Desk/ITSM Integration

- Owns day-to-day end-user triage and first-line troubleshooting
- Uses ZDX as the first stop to identify whether issues originate from device health, local network/Wi-Fi, ISP, SaaS, or application reachability
- Standardizes incident workflows, triage templates, and knowledge articles for recurring issues

CISO Organization/Security Operations (SOC)

- Defines security policy frameworks and control objectives aligned to risk and compliance
- Monitors and triages alerts; refines detections to reduce false positives and improve signal quality
- Coordinates response for security incidents with IT/SecOps owners as needed

Endpoint Engineering

- Owns device lifecycle: Provisioning, compliance baselines, OS/app patching
- Ensures ZCC installation and endpoint integrity at scale (with defined deployment rings and rollback criteria)

Cloud Operations

- Drives cloud connectivity patterns (e.g., Cloud Connector where applicable)
- Partners with security on cloud posture controls and cloud platform standards

Network Operations

- Manages Zero Trust Branch and edge resiliency patterns (e.g., branch gateways/L3, segmentation strategy)
- Owns out-of-band and resiliency mechanisms to maintain access during constrained onsite support scenarios
- Uses ZDX to boost productivity with end-to-end visibility from user devices across any network to SaaS, cloud, and data center apps
- Leverages ZDX AI-driven insights to benchmark ISP performance across the internet and detect last-mile and intermediate ISP issues to improve end-user productivity

©2026 Zscaler, Inc. All rights reserved.

Guidance for IT Leadership

To replicate this operating model:

- Adopt a clear Responsible, Accountable, Consulted, Informed (RACI) matrix: Define who owns policy, deployment, troubleshooting, escalation, and ongoing management per Zscaler product.
- Engineer the handoffs: Ensure responsibilities connect cleanly across teams to prevent “ticket ping-pong.”
- Publish runbooks and escalation criteria: Make it easy for L1 to gather the right evidence and route incidents correctly.

Operational Processes

Operating Cadence and Control

A scalable model requires more than tooling. It requires consistent process:

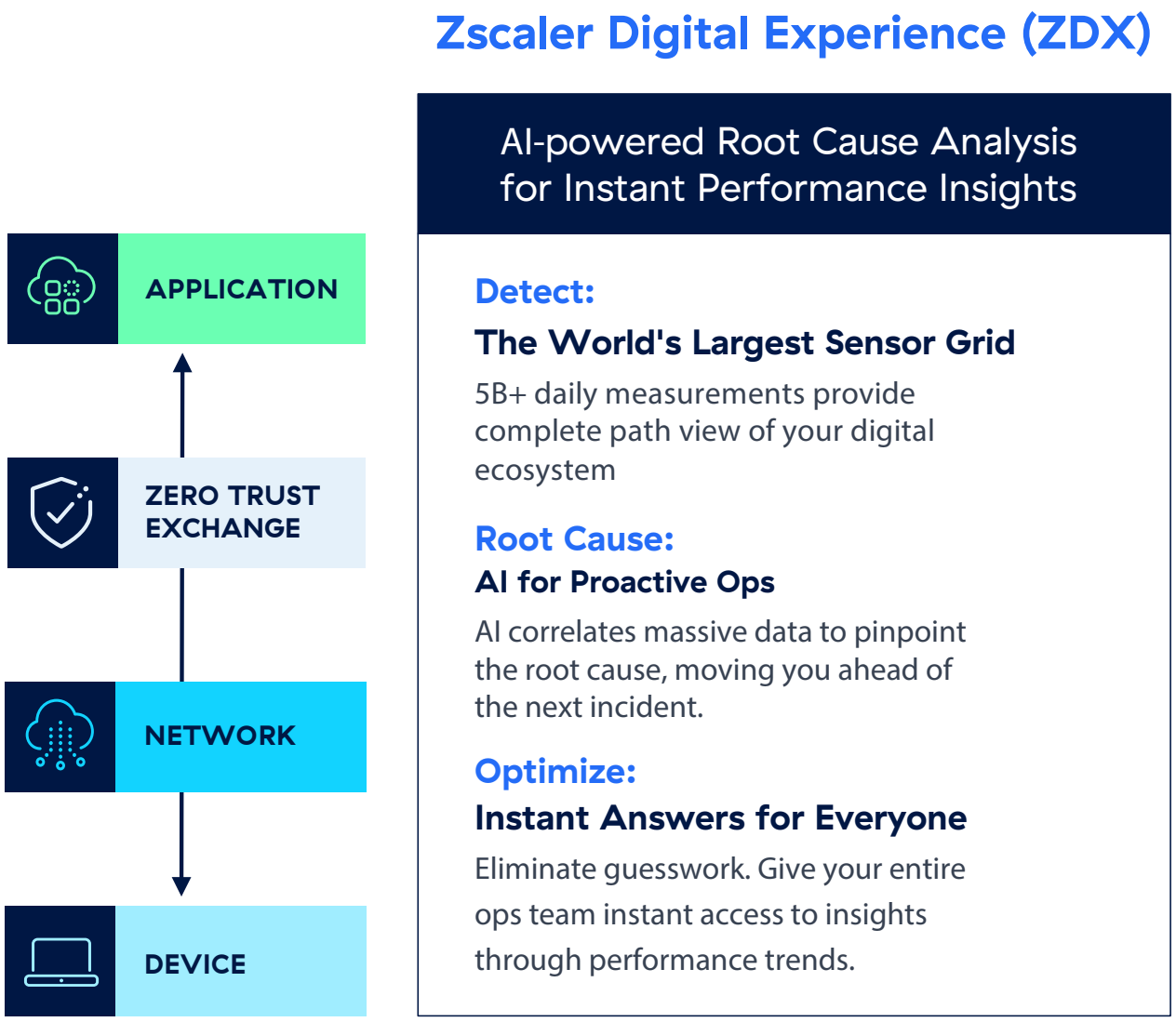
- Standardized incident triage: Consistent evidence collection and escalation thresholds
- Structured change management: Defined approvals and rollback expectations for high-impact policy or client changes
- Continuous improvement loop: Recurring issues become dashboards, automations, and knowledge articles

©2026 Zscaler, Inc. All rights reserved.

Zscaler Digital Experience (ZDX): Operational Best Practices

Natively built into the Zero Trust Exchange platform, Zscaler Digital Experience (ZDX) provides end-to-end visibility across the device, network, and application that enables IT teams to instantly detect and pinpoint root causes via AI-powered root cause analysis (RCA) to execute device, network and app remediation—such as clearing caches, restarting services, or rerouting around ISP outages—to ensure peak employee productivity.

ZDX is most effective when it is treated as an operational system of record for **user experience and app reachability**, not just a dashboard. At Zscaler, we use ZDX to shorten time-to-triage, improve escalation quality, and proactively detect issues before they become widespread incidents.



©2026 Zscaler, Inc. All rights reserved.

Start With What Matters

Begin by defining what "good" looks like and aligning monitoring to business outcomes.

- **Define success metrics** for each critical application:
  - **Availability:** Can users consistently reach and authenticate to the app?
  - **Latency:** Time to establish connections and complete transactions
  - **Responsiveness:** Page load time, interactive performance, and user-perceived delay
  - **User impact:** Number of users affected, where they are located, and how long the issue persists
- **Prioritize crown-jewel applications** first:
  - Key **SaaS applications** (e.g., identity, collaboration, CRM, ERP)
  - Key **ZPA/private applications** (crown jewel apps and admin portals)

Scope Tests Intelligently

ZDX becomes significantly more actionable when tests reflect real access patterns.

- **Don't run every test for every user:** Over-testing creates noise and makes alerting less trustworthy.
- **Apply tests only to the users who should access the application** (by role/group).
  Exclude users who should not access the app to reduce false positives and irrelevant alerts.
- Scope by **groups and representative locations:**
  - Role-based user groups (e.g., Sales, Engineering, IT)
  - Geographic locations/major ISP regions
  - Remote vs office users (when applicable)

©2026 Zscaler, Inc. All rights reserved.

Standardize Test Cadence

Consistency is key for trending and for distinguishing transient blips from real issues.

- Use a **consistent test interval** so results trend cleanly over time.
- **5-minute testing** works well for most critical tests (ZonZ standard), balancing speed of detection with signal quality.
- For less critical apps, consider **longer intervals** to reduce operational overhead and alert fatigue.

Integrate With ITSM and Tune Alerting

To move from reactive troubleshooting to proactive operations, ZDX should drive workflow without generating unnecessary tickets.

- **Integrate ZDX alerts with your ITSM platform** so issues are routed with context and evidence.
- **Tune alert thresholds** to reduce false-positive tickets:
  - Trigger based on **number of impacted users**
  - Use **severity-based thresholds** (critical vs. informational)
- Ensure tickets include actionable metadata (app name, location/ISP, impacted user, time window, key metrics, and any correlated signals).

©2026 Zscaler, Inc. All rights reserved.

Train Every Support Tier

ZDX delivers the best outcomes when every tier uses it consistently and knows what "good triage" looks like.

- Tier 1 (Service Desk): Quick triage and guided workflows
  - Confirm if the issue is device, local network/Wi-Fi, ISP, SaaS, or private app path
  - Capture a consistent evidence set before escalation
  - Turn every team member into an expert with ZDX Copilot by asking data, knowledge, and troubleshooting questions to resolve issues faster and handle more complex tasks
- Tier 2/3: Deeper analysis and higher-quality escalation
  - Identify whether the fault domain is endpoint health, network path, Zscaler policy/traffic steering, or application environment
  - Provide precise escalation details (impacted users, regions/ISPs, performance deltas, and time correlation)

Customer takeaway: *Start small with crown-jewel apps and well-scoped user groups, standardize cadence, integrate alerts into ITSM with tuned thresholds, and train each support tier to use ZDX as the common troubleshooting language.*

Operational Impact of ZDX

When Tier 1 and Tier 2 teams were enabled and trained on ZDX, Zscaler IT saw measurable gains in support efficiency and escalation quality:

- **MTTR reduced from 27 hours to 6.7 hours:** Faster triage and clearer fault-domain isolation accelerated resolution
- **First Touch Resolution improved from 70% to 80%:** More issues were resolved at first contact, reducing unnecessary escalations to higher support tiers

©2026 Zscaler, Inc. All rights reserved.

Level 2/3 Troubleshooting: ZonZ IT Security

The ZonZ team uses ZPA telemetry and analytics to confirm:

- **Who is accessing which private applications**
- **Which App Connector and location handled the session**
- **Whether device posture checks passed** for the targeted application
- **Connector health and reachability tests** (DNS/ICMP/TCP checks from the connector perspective)

ZonZ also correlates ZPA signals with ZDX to understand whether performance issues are user–path related versus application–side.

If indicators point away from policy/connector health, ZonZ escalates to the application owner with specific evidence (connector tests, timestamps, failing ports, affected users, and error patterns). This ends "war rooms" by providing definitive proof that issues originate in the home Wi–Fi, ISP, or the application itself, rather than the Zero Trust architecture.

Application Owner: App/Cloud Environment Validation

Application owners validate the environment and app dependencies:

- Security groups/firewall rules/NACLs and route tables
- Application listener health and expected open ports
- Name resolution and internal dependency connectivity from connector subnets
- Changes in the app stack that correlate to the incident window

Recommended Troubleshooting Sequence

1. Validate **identity and entitlement**
2. Validate **device posture and client state**
3. Validate **policy and app segmentation**
4. Validate **connector health and reachability**
5. Validate **application environment and dependencies**

©2026 Zscaler, Inc. All rights reserved.

Incident Management: Zscaler Private Access (ZPA)

Level 1 Triage: Service Desk

Service Desk starts with ZDX to determine whether symptoms come from:

- Device health constraints
- Home/Wi-Fi/ISP issues
- SaaS service degradation
- General path performance problems

They also perform basic validation:

- Simple connectivity checks and comparative tests (e.g., behavior differences from a non-corporate endpoint where appropriate and permitted)
- Clear ticket documentation including impacted URLs/apps, timestamps, user groups, and repro steps

When widespread ISP outages or regional brownouts are identified through ZDX, IT teams can use ZIA policies to instantly reroute traffic around failing ISP nodes to a different, healthy Zscaler data center. This active control maintains user connectivity and productivity while competitors can only "report" the failure.

Level 2/3 Troubleshooting: ZonZ IT Security (Policy & Controls)

ZonZ investigates ZIA incidents by category using the appropriate insights and logs (e.g., web, firewall, and endpoint/mobile-related reporting as applicable). Common scenarios include:

- **Website or category blocks** (false positives, newly registered domains, miscategorization)
- **Policy mismatches** for specific user groups or geographies
- **Time-sensitive business access** needs requiring controlled exceptions

When a business exception is required, we implement **time-bound access** for a limited audience and automatically revert after the approved duration. This prevents "temporary" exceptions from becoming permanent policy drift.

©2026 Zscaler, Inc. All rights reserved.

Zscaler Client Connector (ZCC): Agile Endpoint Operations

Zscaler uses the ZCC Admin capabilities to centrally manage client configuration, enablement, and phased upgrades. This approach reduces operational fragmentation and allows rapid, controlled deployment of new features.

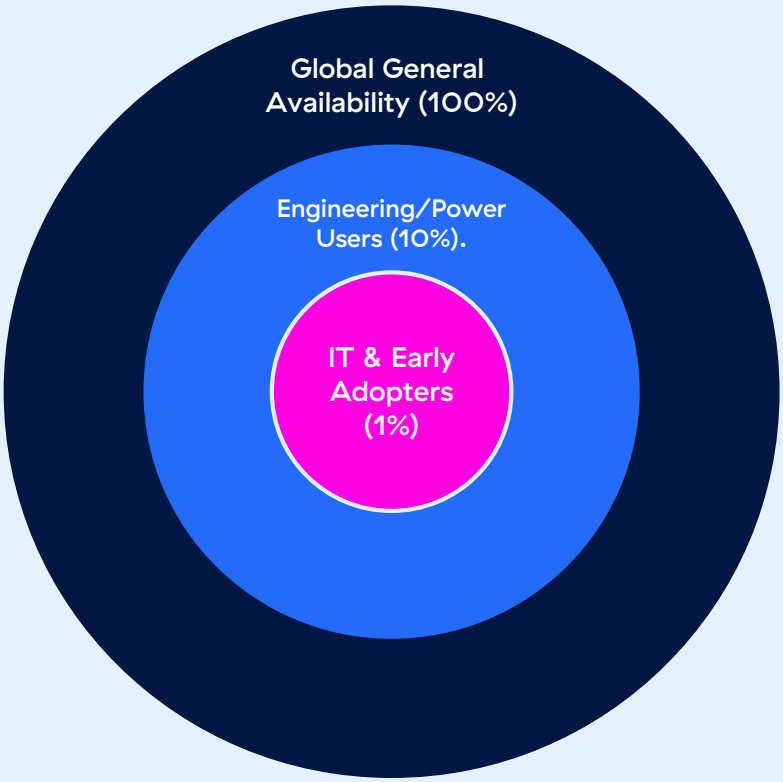
Deployment Structure

- Deployment groups aligned to organizational needs (e.g., IT, Engineering, early adopters, G&A)
- Role-based rollouts to balance velocity and safety

Phased Rollouts

- Incremental rollout (e.g., 1% → 100% over a defined period such as 7 days, adjusted based on risk)
- Version strategy: IT/early adopters validate pre-release or limited availability builds; broad population remains on stable GA releases
- Operational safety: Defined rollback triggers (e.g., login failures, crash rate increase, ticket spikes, performance regressions)

Phased Rollouts" for Zscaler Client Connector



Guidance for customers: *Create deployment roles and treat client and connector updates like a production change—small initial blast radius, measurable health checks, and controlled expansion.*

©2026 Zscaler, Inc. All rights reserved.

Collaborative Security: From Policy to Detection to Operations

Zscaler's internal Zero Trust posture is reinforced through a layered organizational model:

- **CISO/GRC** defines policy standards and ensures alignment to risk and compliance objectives.
- **SOC** provides continuous monitoring, threat intelligence, and alert triage. The SOC continuously tunes detections to improve signal quality and reduce false positives.
- **Operational teams** (ZonZ IT Security, Cloud Ops, Network Ops, and Service Desk) execute day-to-day platform operations, troubleshooting, and response actions.

This tiered model; **policy definition, intelligent monitoring, and rapid operational response**, enables Zscaler to scale securely while adapting quickly to evolving threats and business needs.

Conclusion: Lessons and Takeaways for Leadership

Operating Zero Trust at scale requires an operating model, not just technology. Key lessons from Zscaler on Zscaler include:

- **Operationalize structure, not just product:** Map responsibilities to your IT org and formalize cross-team workflows for triage, escalation, RCA, and change control.
- **Empower decentralization with guardrails:** Enable app/cloud owners to manage their connectors and environments while central security maintains standards and escalation paths.
- **Embrace automation and self-service:** Integrate dashboards and workflows into ITSM; automate recurring tasks and standardize evidence collection.
- **Test, tune, and evolve:** Use deployment rings, proactive monitoring, and feedback loops, especially for new features and releases.
- **Microsegment by default:** Enforce least privilege and isolate access across endpoints, cloud, and branch networks.
- **Invest in enablement:** Build targeted runbooks, knowledge bases, and training for each operational role.
- **Measure what matters:** Track experience health, access reliability, policy exception trends, upgrade success rates, and MTTA/MTTR.
- **Design for scale and resilience:** Review your service model on a regular cadence and adapt as your workforce and application landscape changes.

By applying these principles and the operating blueprint illustrated here, customers can accelerate adoption, improve operational outcomes, and maximize the security and business value of the Zscaler platform.

©2026 Zscaler, Inc. All rights reserved.

Glossary

Term	Full Name	Description
ZIA	Zscaler Internet Access	A cloud native security service edge (SSE) platform that provides secure, policy-based access to the internet and SaaS applications through comprehensive web, threat, and data protection controls.
ZPA	Zscaler Private Access	A Zero Trust Network Access (ZTNA) service that enables secure, identity-based access to private applications in data centers or public clouds, eliminating the need for legacy VPNs and reducing the attack surface.
ZDX	Zscaler Digital Experience	A digital experience monitoring (DEM) solution that provides end-to-end visibility into performance across the user device, local network, ISP, and application path to proactively identify and resolve experience issues.
ZCC	Zscaler Client Connector	A unified endpoint application that secures user devices, verifies identity and posture, and intelligently steers traffic to the Zscaler Zero Trust Exchange regardless of the user's location

zscaler™ | Act Fast. Stay Secure.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, and ZDX™, and other trademarks listed at **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.

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