



Zscaler Professional Services

Rapid Response Services

Zscaler will partner with your organization to provide Rapid Response Services in the event of a cybersecurity breach. Our team of expert consultants will respond within 24 hours to immediately deploy Zscaler products and revert your valuable traffic to a safe environment. We then proceed to rollout the Zscaler platform products in your production environment. We care as much about your business as you do. Rely on our expertise and experience to help where you need it most.

Rapid Response Services	
Duration	4 Contiguous Weeks 8 Hours per day Monday - Friday
Customer Focus	~ (Any Size)
User Count	~ (Any Number of Users)
Resources	Professional Services Consultant Project Manager (Onsite optional; Part-Time) Architect (Part-Time, Remote only)

Implementation Phases	
Week 1 (Onsite)	Kick-Off, Design, Build and Pilot
Week 2 (Onsite)	Build, Complete Pilot and start Production
Week 3	Rollout
Week 4	Complete Production. Project Closure and Handoff

Benefits of Professional Services:

- **Valuable Zscaler Experience:** Our PS Consultants bring deep architectural and operational experience, bolstered by thousands of implementations, that help you reduce risk and increase project success
- **Bridge Resources and Knowledge Gaps:** Access Zscaler's expertise to efficiently fill potential skill or resource gaps, without having to hire additional resources
- **Leading Practice Guidance:** Achieve your business objectives quickly by leveraging our years of experience and knowledge of leading practices
- **Accelerate ROI:** Feel confident knowing your deployment has been set up for success, by relying on Zscaler's proven project methodology

Once engaged, our Professional Services Team will focus on deployment of one or both of the following Zscaler platform products to mitigate risks associated with your specific cybersecurity breach situation.

Rapid Response – ZIA

- Policy Posture Configuration* to include:
 - SSL Inspection rules
 - Cloud App Control rules
 - URL Filtering rules
 - Sandbox rules
 - File Type Control rules
 - Cloud Firewall rules
 - DNS Control rules
 - IPS Rules
 - SIPA Apps (If both ZIA & ZPA are in scope)
- Preconfigured policies provided by leading practice blueprint
- Data Protection
- Leading practices for mobile users (Android/iOS)
- Alerting and Reporting
- Production Rollout Support

Rapid Response – ZPA

- Environment Configuration* to include:
 - App Segments, Wildcard Segment, Bypass Segment
 - Segment Groups
 - Servers
 - Server Groups
 - App Connectors
 - App Connector Groups
 - ZPA App Bypasses
 - Browser Access
 - PRA
 - Client to Client Connectivity for remote administration
- Leading practices for mobile users (Android/iOS)
- Alerting and Reporting
- Production Rollout Support

* Expectations around configuration constraints will be addressed as part of the engagement.

Disclaimer: [Zscaler Deployment and Professional Services Disclaimer](#)



Experience your world, secured.™

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](#).

© 2022 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](#) 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.