DATA SHEET

Zscaler Professional Services

ZPA AppProtection

ZPA AppProtection controls enable you to protect your internal application traffic from many types of attacks. AppProtection allows you to do in-line inspection of application flows in real time, and to inspect them for malicious content.

AppProtection is part of the Zscaler Private Access™ (ZPA™) platform, offering a simplified private access management solution. As a single platform, ZPA provides an easy way to inspect traffic and secure access, reducing the risk of misconfigurations and incompatibilities from multiple point solutions. It also lowers total cost of ownership (TCO) by reducing reliance on expensive hardware and associated software, and cuts infrastructure and SOC operational costs by simplifying architecture and eliminating maintenance overhead.

Based on leading practices, this offering is for organizations that want to adopt a more mature and proactive approach to prevent cybercriminals from accessing their sensitive data, credentials, and other digital assets by exploiting vulnerabilities in applications. Our Professional Services (PS) Consultant will review and configure security profiles and security and custom control policies to meet your organizational needs.

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

ZPA AppProtection		
Professional Services Scope	SCOPE:* • Assess and Review Use Cases • Configure up to 10 AppProtection Security Policies • Configure up to 5 AppProtection Security Profiles • Configure up to 5 Browser Protection Security Poliices • Configure up to 3 Browser Protection Security Profiles • Deploy up to 3 Custom Controls • Test and analyze Logs for Security Violations and User Access *** Any effort not explicitly stated is deemed out of scope** DELIVERABLES: • Design deliverable	
Credits	44	Redemption of sufficient credits for fulfillment of service offering per unit required
Maximum # of Units recommended	2	The maximum number of units recommended for this offering to be implemented in parallel. For organizations requiring more than stated recommended units, there are alternative SKUs that may better align to your needs
Resource Allocation	One (1) Professional Services Consultant	Assigned to deliver as per scope of deployment offering
Staffing	Resource assignment may take up to 2 weeks	
Duration	Up to 10 weeks; Not to exceed 90 days/3 Months	Upon the start of the project, all efforts should be completed within 10 weeks. In total the project will not exceed 3 months of engagement from Professional Services, based on the service start date
Delivery Method	Remote	Assigned PS Resources will be remote for the duration of the engagement
Non Technical Prerequisites	The Customer: • Must provide appropriate lead resources to attend technical Kick–off and design sessions on the commencement date • Must provide Zscaler representatives with information and resources to successfully execute the Project. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing project resources, and attendance in planning, execution, or Knowledge Transfer meetings • Will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review • Must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third–parties and other customer vendors, suppliers, and Consultants	

Technical Prerequisites	• Authentication has been configured on the customer IdP and in the Zscaler Portal
	• Zscaler Client Connector has been rolled out to users and working properly
	• ZPA environment is fully provisioned and operational
	• Customer is subscribed to ZPA AppProtection and Browser Protection
	• Customer to ensure CPU and Memory Utilization for App Connectors are <40% prior to enabling App Protection.
	• Auto AppProtection Signing CA has been properly configured by the customer on ZPA Tenant environment
	• The following should be provisioned via Zscaler Support in advance of project start:
	  • AppProtection on App Connectors
	  • Auto AppProtection Feature
	  • Active Directory Protection
	  • ThreatLabz Controls, OWASP Control, WebSocket Control and Custom Controls	

ZPA AppProtection	
Project Expectations	• Customer has all technical information to be able to define App Segments • Customers should have an advanced understanding of their applications and the APIs that the applications leverage. • Customer to identify and provide a list of their target mission critial applications
Project Constraints	• This Project covers the deployment of only Zscaler licensed solutions. Additional product offerings may be purchased as add-ons, otherwise additional consulting work not contained in this Project is deemed out of scope • Zscaler is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities • Zscaler is not responsible for impacts to schedule caused by customer internal processes
Terms & Conditions	Zscaler Deployment and Professional Services Terms and Conditions

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