DATA SHEET

Zscaler Professional Services

Cloud Sandbox

Zscaler Cloud Sandbox is the world's first AI-driven malware prevention engine, delivering inline patient zero defense by performing unlimited latency-free inspection across web and file transfer protocols, including SSL/TLS.

Built on a unique cloud native proxy platform, our Cloud Sandbox automatically detects, prevents, and intelligently quarantines unknown threats and suspicious files, preventing compromise, lateral movement, and data loss across all users
and devices.

Our professional services team will work with you to deploy the Cloud Sandbox capabilities within your existing Zscaler Internet Access Environment, including creation of security policies to ensure they provide the protection you need. This offering is best suited for organizations with existing ZIA deployments who are seeking to further bolster their security posture by using Zscaler's Sandbox technology. This offering serves organizations that have purchased Zscaler Cloud Sandbox that want to proactively defend against malicious attacks and threats, reduce time to value and build a solid foundation for their transformation efforts.

Benefits of Professional Services:

- **Real World 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

Cloud Sandbox		
Professional Services Scope	SCOPE: • Creation of up to 20 rules INCLUDED: • Design and definition of Cloud Sandbox policies, including alerting and mitigation actions • Integration with Crowdstrike APIs to provide endpoint detection and response (EDR) visibility for Cloud Sandbox-detected malware. EXCLUDED: • All other ZIA & ZPA policies DELIVERABLES: • Implementation plan, Rollout planning and assistance,Zscaler Recommendations, Conversion of Cloud Sandbox policies from the current solution, if any (up to product capability) PROJECT CLOSURE: • Provide a deployment overview and respective deliverables due at Project Completion	
Credits	20	Redemption of sufficient credits for fulfillment of service offering per unit required
Maximum # of Units recommended	8	The maximum number of units recommended for this offering. For organizations requiring more than the 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 4 weeks; Not to exceed 90 days/3 Months	Upon the start of the project, all efforts should be completed within 4 weeks. In total, the project will not exceed 3 months of engagement from Professional Services, based on the project start date
Delivery Method	Remote	Assigned PS Resources will be remote for the duration of the engagement
Non Technical Prerequisites	The Customer: • To provide detailed Project and Stakeholder Management, if required. • 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 training 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 customer's other vendors, suppliers, and consultants.	

Cloud Sandbox	
Technical Prerequisites	• Traffic Forwarding method configured – Client Connector installed on the desired user groups • Authentication configured on customer Identity Provider (IdP & Zscaler Admin Portal), tested to function as expected. • User objects and groups are synchronized using SCIM or Auto-provisioning to use them in Policy creation. • SSL Inspection is enabled and all prerequisites associated for the desired group of users/ locations where Cloud Sandbox policies need to be applied are complete (i.e., like Zscaler/customer root cert is installed) .
Project Expectations	• Professional Services team to help with the recommendations on industry baseline. • The file types to be protected & scanned by Cloud Sandbox should be known to Customer. • The Cloud Sandbox policies are configured, validated per customer use cases and requirements.
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 • Availability and support for Hypervisor (ESXi, etc) solution. • Lead time for whitelisting the required ZPA Cloud IP subnets at the customer perimeter level firewall.
Terms and Condiitions	Zscaler Deployment and Professional Services Terms and Conditions

zscaler™ | 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.

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