



Zscaler Professional Services

Data Protection Offerings: Endpoint

Zscaler Endpoint Data Protection takes a focused approach to securing sensitive at rest on endpoint devices. By enforcing policy controls, organizations reduce risk, prevent data loss and ensure visibility for compliance.

Zscaler's Endpoint Data Loss Prevention (DLP) service provides visibility and control over sensitive data at rest and in motion on user devices. This service engagement is designed for organizations that have licensed Zscaler Endpoint DLP and are ready to activate device-based policies such as blocking file transfers to network shares, removable storage (such as USB), personal cloud storage, or printers.

With the shift to hybrid work and an increasingly mobile workforce, securing data on the endpoint has never been more critical. Zscaler Endpoint DLP extends protection beyond the network.

Our Professional Services (PS) Consultant will deploy Zscaler Endpoint Data Protection in your existing Zscaler Internet Access (ZIA) environment. This ensures your organization can quickly operationalize real-time data protection policies across endpoint devices.

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.

Data Protection: Endpoint

Professional Services Scope	<p>SCOPE:</p> <ul style="list-style-type: none"> • Predefined/Custom Dictionaries & Engines - Up to 5 dictionaries (4 predefined & 1 custom), Up to 5 custom DLP Engines & Up to 5 DLP policies, Up to 10 DLP resources over supported channels (Removable storage, printer, network paths, personal storage), Up to 5 Endpoint DLP End User Notifications, Up to 5 Auditor Notifications (hosted/external), Up to 5 Device Control Rules for printers and removable storage. • Please note: Rules will remain in "Allow" mode for this deployment. Blocking actions may be discussed during Pilot but won't be implemented in Production. <p>INCLUDED:</p> <ul style="list-style-type: none"> • Expert guidance to protect your data using Zscaler Endpoint DLP capabilities including policy enforcement across local storage, removable media and device control features. • Consultative Kick-off Meeting & Design Workshop with Key Stakeholders • Pilot - Monitor and Enforcement mode • Production - Monitor mode only • Transition Meeting <p>EXCLUDED:</p> <ul style="list-style-type: none"> • Advanced ZIA policy configurations and inspection services are not included. • Custom feature tracking or change requests must be made via the Enhancement process and are not part of this delivery. • Anything not explicitly stated is deemed out of scope. <p>DELIVERABLES:</p> <ul style="list-style-type: none"> • Prerequisites Checklist • Design Deliverable <p>PROJECT CLOSURE:</p> <ul style="list-style-type: none"> • Provide a deployment overview and respective deliverables due at project completion. 	
Credits	40	Redemption of sufficient credits for fulfillment of service offering per unit required.
Maximum # of Units recommended	4	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.
Duration	Designed to be implemented in 8 weeks; Not to exceed 90 days/3 Months	Upon the start of the project, all efforts should be completed within 8 weeks. In total the project will not exceed 3 months of engagement from Professional Services, based on the service start date.

Data Protection: Endpoint		
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	
Delivery Method	Remote	Designated PS Resources will be remote for the duration of the engagement. Resources are not dedicated.
Non-Technical Prerequisites	<p>The customer:</p> <ul style="list-style-type: none"> • Must provide appropriate lead resources and attend Kick-off and design workshops on the commencement date. • Must provide Zscaler representatives with information and resources to successfully execute the Project. This can include, but not limited to, 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 customer's other vendors, suppliers, and Consultants. • Must outline compliance and regulatory alignment with documentation where applicable. • Will handle any activity relative to internal change management processes. 	
Technical Prerequisites	<ul style="list-style-type: none"> • Authentication has been configured on customer identity provider (IdP) and connected to Zscaler ZIA • Zscaler Client Connector must be deployed and functioning without error 	
Project Expectations	<ul style="list-style-type: none"> • Authentication configuration has been configured and successfully tested. • Customer knows what rules they want implemented. 	
Project Constraints	<ul style="list-style-type: none"> • 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. 	
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 SSE-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/ 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.