Data Sheet

Zscaler Cloud Sandbox—Security and Privacy

The intent of the Security and Privacy Datasheet is to provide Zscaler Cloud Sandbox customers information detailing how data is collected, processed, and stored by and within Zscaler Cloud Sandbox and subprocessors.

Product Summary

Zscaler Cloud Sandbox, a fully integrated capability of Zscaler Internet Access and part of the Zscaler Zero Trust Exchange, is the industry's first AI-driven malware detection, prevention and quarantine engine. Cloud Sandbox delivers inline, patient-zero defense by performing unlimited, latency-free inspection for HTTP/HTTPS and FTP for Sandbox extraction and analysis. Using trillions of daily signals and thousands of actively blocked threat information, users gain insight into every request and file—by user, location, and device around the world—in seconds.

Information processed by Zscaler Cloud Sandbox

Zscaler takes great responsibility as a data controller and processor seriously, integrating four key components for control, enforcement, analysis and logging: the Central Authority (CA), ZIA Public Service Edge, Advanced Cloud Sandbox Analysis nodes and Nanolog Servers.

As part of the unified Zero Trust Exchange platform and leveraging the principle of least-privileged access, files and data processed by the Cloud Sandbox operates solely in memory. Files identified as unknown and suspicious are stripped of customer identifiable information and forwarded to an AI-driven quarantine service for deeper analysis. After the completion of analysis, benign files are immediately purged from memory while malicious files are stored in an encrypted form without attribution to the submitting organization.

The Cloud Sandbox analyzes unknown files entering an organization based on customer-defined policies by user, group and location. Customer policy dictates which file types and in what context will be forwarded to the Cloud Sandbox service for analysis, providing complete granular control to the administrator.

Privacy protection at the web transaction level

- The ZIA Public Service Edge never stores any web transaction content or personal data
- Web transaction content, including files, are never written to disk; all content inspection takes place in memory
- Customer transaction logs (customer logs) are transferred to Zscaler Nanolog clusters in a compressed and tokenized format
- Customer logs are only available via the Zscaler web user interface by authorized administrators with appropriate privileges
- User identifiers can be obfuscated within Zscaler's web user interface

Privacy protection at the facilities level

- Security standards on par with world-class financial and data centers for hub facilities (ISO27001, SOC 2 Type 2, or similar local certification)
- Authorized personnel must pass through multiple levels of security and biometric scanning to gain access
- All data centers are hosted in secure telecommunications centers at major internet exchange points globally
- 24x7x365 security management and site access via security operations center

Privacy protection at the network and storage level

- Customer logs are never stored in clear text
- Files deemed benign by the Advanced Cloud Sandbox are purged from memory, while files deemed malicious are stored in an encrypted form
- Customer logs are transmitted as indexed, compressed, and differential logs
- A single log is meaningless without a complete string of historic logs
- All communications between a ZIA Public Service Edge and a Nanolog cluster are encrypted using TLS

Access and Disclosure

Zscaler employee access to the production Advanced Cloud Sandbox analysis environment is restricted to the specific engineering teams that develop and deploy the service in addition to analyzing malicious files for common attributes and additional protections.

All access to the environment is governed by strict least-privileged principles and all activity is logged and audited.

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