Data Sheet

Zscaler Cloud Sandbox

The world's first AI-driven malware detection, prevention and quarantine engine

Zscaler Cloud Sandbox prevents patient-zero infections and blocks advanced persistent threats from gaining access to your network

In today's mobile- and cloud-first world, your users are accessing files on the go directly from the internet and SaaS applications. Long gone are the days of launching email clients from the corporate office surrounded with layers of security. As the demands for ease of use outpaces network-centric defenses, organizations are left with an expanded attack surface during a time when attacks are becoming more devious and adversaries taking advantage of legacy security stack gaps.

In an effort to protect sensitive business and personal data, nearly all internet traffic is now encrypted. While this has deterred some bad actors, encryption has created a false sense of security. Legacy sandboxes with passthrough architecture lack visibility and have unintentionally permitted malicious files to slip through the cracks by hiding in encrypted traffic, free from deep inspection or quarantine. Bolted-on SSL decryption devices can be deployed to help, however, as with most hardware, they fail to scale and add to administrative headaches and costly device sprawl. As a result, patient-zero infections from unknown malware continue to permeate networks and leave IT and security teams

Benefits of Zscaler Cloud Sandbox:

- **AI-driven malware prevention engine**
  Intelligently identify, quarantine, and prevent unknown or suspicious threats inline using advanced AI/ML without rescanning benign files.
- **Full inline inspection to find hidden attacks**
  Expose and prevent evasive threats and malware hiding in encrypted traffic across web and file transfer protocols without latency and capacity limits.
- **Consistent globally shared prevention**
  Get automated protection for previously unknown threats with integrated threat intelligence shared across all users in real-time.
- **SOC workflows augmented with threat intel**
  Accelerate investigation and response by sharing malware behavioral insights, threat intel, and advanced reporting using robust APIs.
- **No more costly physical appliances and software**
  Deploy in seconds with no hardware to buy or software to manage—simply configure and implement a sandbox policy to immediately see value.
- **Cloud-delivered protection with global edge presence**
  Get fully integrated, unmatched security and user experience with Zscaler Internet Access™ as part of the Zscaler Zero Trust Exchange™.

scrambling to stop lateral movement and data exfiltration, which should have been prevented in the first place.

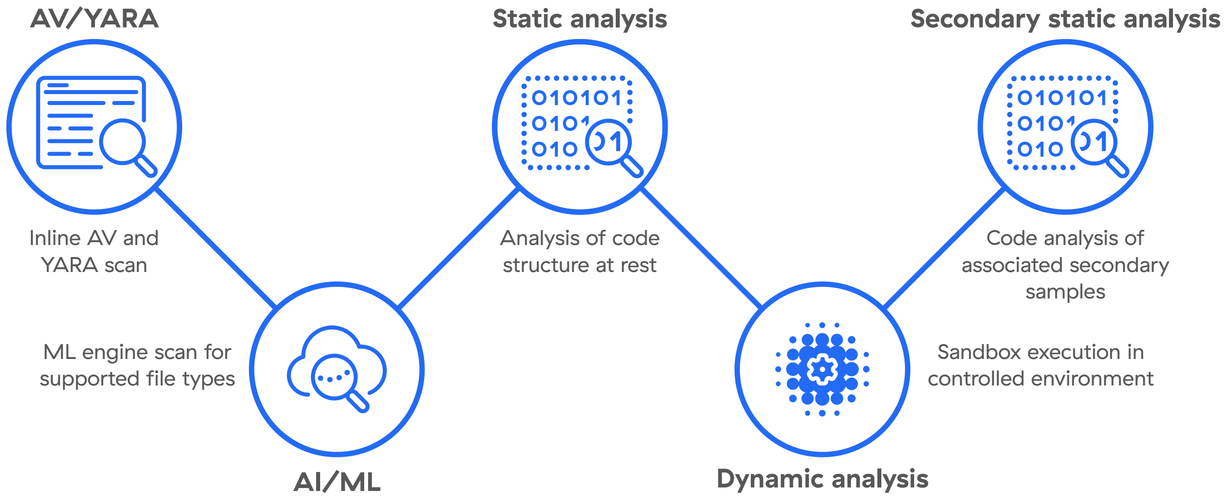
Zscaler Cloud Sandbox

As a critical function in the security stack, the goal of the sandbox is to provide preventative measures against malicious files and code executions. Unlike out-of-band sandboxes that provide protection only after the initial compromise, Zscaler Cloud Sandbox is purpose-built to catch and stop modern and elusive threats that leverage evasion techniques and exploit traditional sandbox weaknesses.

Built on a cloud-native, proxy-based architecture, Zscaler Cloud Sandbox is the world's first AI-driven malware prevention engine that automatically detects, prevents, and intelligently quarantines unknown threats and suspicious files inline. The unlimited, latency-free inspection across web and file transfer protocols (FTP), including SSL/TLS, allows the cloud-gen sandbox to perform in-depth, real-time dynamic analysis to ensure that no unknown file reaches the user as a malicious file download.

The unknown or suspicious file is first sent through a prefiltering analysis engine that checks the file contents against 40+ threat feeds, antivirus signatures, YARA rules, and AI/ML models to render a quick verdict, blocking similarly known threats. After the initial triage, the file then undergoes robust static, dynamic, and secondary analysis that includes file execution in a controlled, isolated environment to reach an actionable verdict. The final step is post-processing, which updates the Zscaler threat database and customer's policy enforcement.

With AI-based verdicts, benign files are delivered instantly while malicious files are blocked for all Zscaler global users as a result of the shared protection from the cloud effect. This stops patient-zero infections and emerging threats for all users regardless of device or location.


AV/YARA
Inline AV and YARA scan
ML engine scan for supported file types
AI/ML
Static analysis
010101
0101
010
01
Analysis of code structure at rest
Dynamic analysis
Sandbox execution in controlled environment
Secondary static analysis
010101
0101
010
01
Code analysis of associated secondary samples

Cloud-gen sandbox benefits

Beyond quarantining suspicious files inline, performing real-time AI-based analysis, and issuing instant verdicts without delays, Zscaler Cloud Sandbox's detailed advanced reporting can take sandboxing from the last line of defense to the first step in intelligence-driven action. By applying behavioral insights from real malware targeting your organization, you can enrich SecOps workflows to strengthen your defenses throughout the security stack.

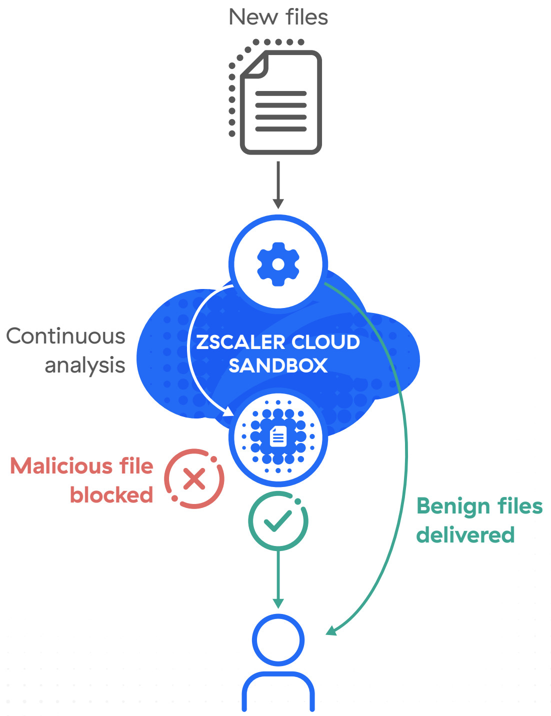
Intelligently stop emerging threats and patient-zero infections
Adversaries are taking advantage of encryption and trusted cloud apps to deliver stealthy attacks. In fact, a recent ThreatLabZ report observed malware being delivered from Google Drive, AWS, and OneDrive. The ability to scan files across web and FTP, particularly encrypted traffic, assures visibility and stops attackers from gaining access to your network.

Before an employee accidentally downloads and opens a new malicious Office document (Maldocs) with a hidden macro, Zscaler Cloud Sandbox's AI-driven, inline quarantine function kicks in. When the deep file analysis returns a high threat rating, the file is blocked for the employee and cannot be accessed by other Zscaler users. The instant file verdicts without rescanning files prevents disruption to productivity for employees while automatic quarantining and blocking of unknown or malicious files prevents what would otherwise be a barrage of IT help desk tickets.

After a quick twenty-minute deployment of Zscaler Cloud Sandbox, a customer's IT and security team was able to safely and instantly deliver 91% of benign files to users after receiving an AI-based verdict. The remaining unknown files were forwarded for in-depth, dynamic analysis which revealed that 5% of the files contained malware or malicious intent. The files are blocked for the intended users and for all Zscaler's global users and devices regardless of locations for shared, consistent protection.

AI-driven quarantine stops never-before-seen malware

Inline protection with instant benign file delivery, patient-zero defense, and granular policy controls



Enhance SOC workflows with malware insights and MITRE ATT&CK

After deep file analysis and the safe detonation of unknown malware, the cloud-gen sandbox automatically generates an analysis report. The controlled, isolated sandbox environment captures analysis screenshots and informs analysts of polymorphism and obfuscation evasion techniques, callback behavior, and other actions. This report details the attack lifecycle and event killchain, malware behavior, and payload intent, mapping them back to the MITRE ATT&CK framework.

By operationalizing the contextual sandbox findings with the ATT&CK framework, security and IT teams can share insights across the security stack. This allows the cloud-gen sandbox to not only be the last line of defense against malware, but also the first step in detection, accelerating investigation and response while supporting threat hunting exercises.

Simplified policy management with granular controls

As a cloud-delivered product, there is no hardware to buy and configure and there is no software to manage, reducing complexity and resources. Without needing to be on location to set up and connect each device, you can be up and running with Zscaler Cloud Sandbox with a simple two-step configuration: **criteria** and **action**. As a bonus, policies are easy to manage, configure, and deploy. Within a few clicks, admins can implement policies, including rule order for precise execution and other policies that follow users or user groups regardless of location.

For more granular controls, the cloud-gen sandbox can enhance static and dynamic file analysis with automated JA3 fingerprinting detection and configure custom hash blocklists and YARA rules. Additionally, score-based blocking policies can take action on annoying or suspicious greyware and adware files that don't typically pass the threat score threshold.

Built on an cloud-native zero trust platform

Zscaler Cloud Sandbox is a fully integrated capability of Zscaler Internet Access and part of the Zscaler Zero Trust Exchange. The unique, proxy-based architecture protects users inline, not after the fact, by directing traffic to the industry's largest cloud security stack to deliver in-depth, intelligent protections to every user regardless of location or network. Get shared, global protection with real-time updates sourced from 300 trillion daily threat signals combined with cloud-gen protection and least-privilege principles of zero trust.

Standard vs Advanced Cloud Sandbox

	Standard Cloud Sandbox	Advanced Cloud Sandbox	
ZIA editions	Professional Edition Business Edition	Transformation Edition ELA Edition	**Advanced Cloud Sandbox can be an add-on to ZIA Professional and Business Edition**
File support	.exe, .dll	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, script files in zips	
AI-driven quarantine	—	✓	
Granular policies	—	✓	
Reporting	—	✓	
API	—	✓	

Cloud-gen Core Features

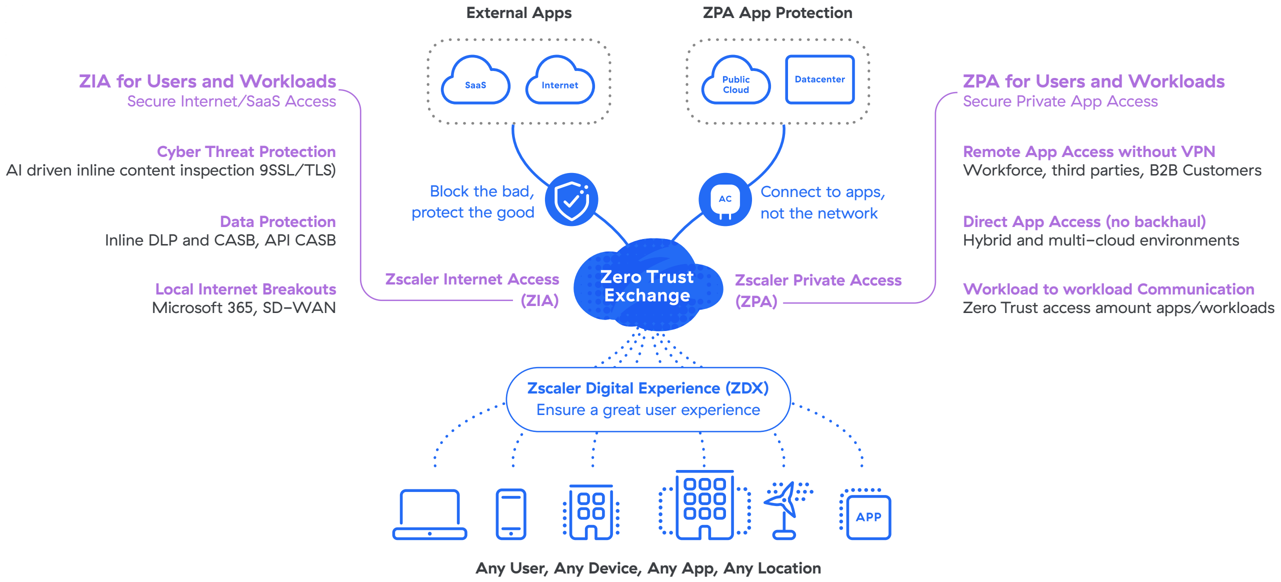
Prefiltering Analysis Engine	AV, hash blocklists, YARA rules, automated JA3 fingerprinting detections, and ML/AI models
Static, dynamic, and secondary analysis	Static analysis and dynamic analysis, including code analysis and secondary payload analysis
File support	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, script files in zips
SSL inspection	Unlimited capacity for SSL/TLS inspection
File retention	Zscaler Cloud Sandbox operates solely in memory. Files are stripped of identifiable information during analysis. After analysis is completed, benign files are purged from memory while malicious files are encrypted and stored indefinitely, sharing insights across all Zscaler's users for continuous protection.
OS support	Windows XP, Windows 10, Android
Protocol support	HTTP, HTTPS, FTP, FTP over HTTP
Files per day	Unlimited
Maximum file size	20 MB for Windows and 50 MB for Android
Deployment method	Cloud-native
Threat intel integration	40+ security partner threat intel feeds
Management and reporting	Full reporting including malware behavior and intent, indicators of compromise (IOCs), dropped files, PCAPs
Forensics	Initial sample, secondary payloads, PCAPs
API Support	Robust API support, report retrieval via API in JSON format
Granular policies	Easy to use and configure policies for users, location, location groups, file types, user groups, departments, URL categories, and protocols
Privacy and compliance certifications	Compliant with rigorous global Commercial and Government risk, privacy, and compliance CSA cloud security alliance ISO 27701 AICPA SOC FedRAMP StateRAMP
Industry and data privacy regulations	Compliance adherence to industry-specific and in-country data privacy regulations PCI Security Standards Council HIPAA GDPR NIST 800-63C

Zscaler Cloud Sandbox is fully integrated with Zscaler Internet Access™ and part of the holistic Zero Trust Exchange

The Zscaler Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.

How Zscaler delivers zero trust for users, workload, and OT

Deploy in weeks to enhance cyber protection and user experience



External Apps

ZPA App Protection

ZIA for Users and Workloads
Secure Internet/SaaS Access

Cyber Threat Protection
AI driven inline content inspection 9SSL/TLS)

Data Protection
Inline DLP and CASB, API CASB

Local Internet Breakouts
Microsoft 365, SD-WAN

Block the bad, protect the good

Connect to apps, not the network

Zscaler Internet Access (ZIA)

Zero Trust Exchange

Zscaler Private Access (ZPA)

ZPA for Users and Workloads
Secure Private App Access

Remote App Access without VPN
Workforce, third parties, B2B Customers

Direct App Access (no backhaul)
Hybrid and multi-cloud environments

Workload to workload Communication
Zero Trust access amount apps/workloads

Zscaler Digital Experience (ZDX)
Ensure a great user experience

Any User, Any Device, Any App, Any Location

Gartner

Zscaler named a Leader in Gartner's SSE MQ, positioned highest in Ability to Execute.

Learn More →

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