Datenblatt

# Zscaler Sandbox

## Die weltweit erste KI-gesteuerte Engine zur Malware-Erkennung, -Abwehr und -Quarantäne

### Zscaler Sandbox unterbindet Patient-Zero-Infektionen und verhindert, dass Advanced Persistent Threats Zugriff auf Ihr Netzwerk erhalten.

In der heutigen Mobile- und Cloud-first-Welt greifen User von unterwegs direkt über das Internet und SaaS-Anwendungen auf Dateien zu. Die Zeiten, in denen E-Mail-Clients von der Unternehmenszentrale aus gestartet wurden und mit verschiedenen Sicherheitsebenen geschützt waren, sind längst vorbei. Da die netzwerkzentrierten Abwehrmaßnahmen nicht mit den Anforderungen an die Anwenderfreundlichkeit Schritt halten können, haben Unternehmen in einer Zeit, in der Angriffe immer raffinierter werden und Angreifer Lücken im Legacy-Security-Stack ausnutzen, eine immer größere Angriffsfläche.

In dem Bemühen, sensible geschäftliche und persönliche Daten zu schützen, wird fast der gesamte Internet-Traffic verschlüsselt. Dieses Vorgehen hat zwar einige Angreifer abgeschreckt, aber zugleich ein falsches Gefühl der Sicherheit vermittelt. Legacy-Sandboxen mit Passthrough-Architektur bieten nur wenig Transparenz und lassen schädliche Dateien unbeabsichtigt ins Netzwerk gelangen, wenn sich diese im verschlüsselten Traffic — für den keine umfassenden Überprüfungen oder Quarantänemaßnahmen vorgesehen sind — verstecken. Nachgerüstete Geräte zur SSL-Entschlüsselung können zwar Abhilfe schaffen, sind aber wie die meiste Hardware nicht skalierbar, verursachen zusätzliche Verwaltungsprobleme und sind durch ihre schiere Menge kostspielig. Infolgedessen dringen Patient-Zero-Infektionen durch unbekannte Malware weiterhin in Netzwerke ein und führen dazu,

### Vorteile von Zscaler Sandbox:

- **KI-gestützte Engine zur Malware-Abwehr** Unbekannte Bedrohungen bzw. verdächtige Dateien werden mit erweiterten KI-/ML-Funktionen erkannt, isoliert und blockiert, ohne dass unschädliche Dateien erneut gescannt werden müssen.
- **Vollständige Inline-Überprüfung zur Erkennung verborgener Angriffe** Ausweichmanöver und im verschlüsselten Traffic versteckte Malware werden in sämtlichen Netzwerkprotokollen ohne Latenz und Kapazitätsbeschränkungen erkannt und blockiert.
- **Konsistente, global geteilte Sicherheit** Automatischer Schutz vor bisher unbekannten Bedrohungen mit integrierten Threat-Intelligence-Daten, die für alle User in Echtzeit verfügbar sind.
- **Mit Bedrohungsdaten angereicherte SOC-Workflows** Der Austausch von Informationen zu Malware-Verhalten, Threat Intelligence und erweiterten Berichten über robuste APIs unterstützt eine schnelle Ermittlung und Reaktion bei Sicherheitsvorfällen.
- **Keine kostspieligen physischen Appliances oder Software-** Sekundenschnelle Bereitstellung ohne Anschaffung von Hardware bzw. Verwalten von Software — Sandbox-Richtlinien lassen sich einfach konfigurieren und implementieren und bringen unmittelbaren Geschäftsnutzen.
- **Cloudbasierter Schutz mit globaler Edge-Präsenz**Die Integration mit Zscaler Internet Access™ im Rahmen der Zscaler Zero Trust Exchange™ gewährleistet unübertroffene Sicherheit und erstklassige Anwendererfahrungen.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

dass IT- und Sicherheitsteams verzweifelt versuchen, laterale Bewegungen und Datenexfiltrationen zu stoppen, die eigentlich von vornherein hätten verhindert werden müssen.

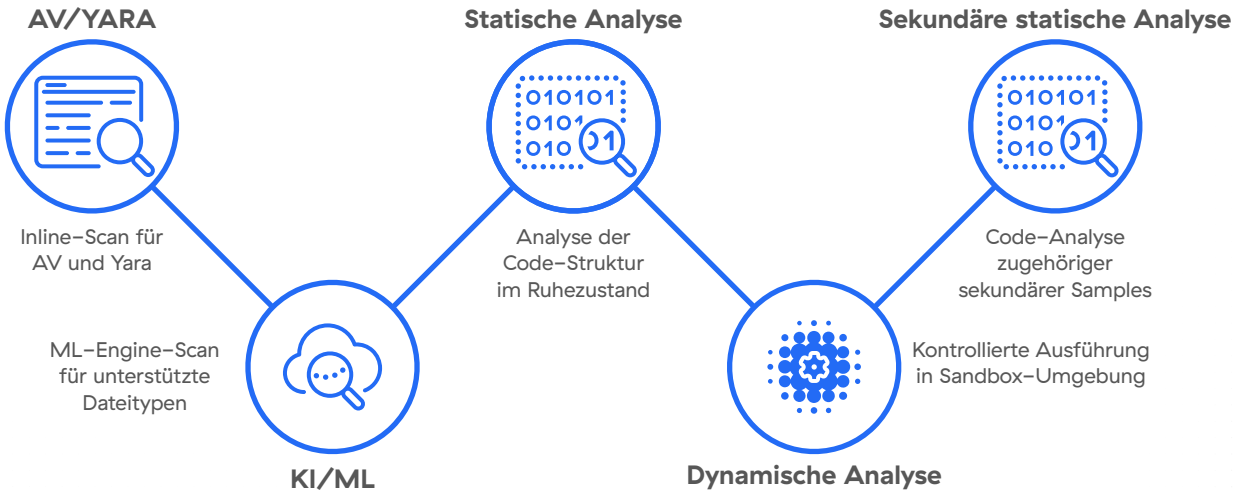
## Zscaler Sandbox

Als unverzichtbarer Bestandteil des Security-Stacks dienen Sandbox-Lösungen zur Abwehr schädlicher Dateien und zur Verhinderung der Ausführung von Malware. Im Gegensatz zu Out-of-Band-Sandboxen, die erst nach der ersten Kompromittierung Schutz bieten, wurde Zscaler Sandbox speziell dafür entwickelt, moderne und schwer fassbare Bedrohungen abzufangen und zu stoppen, die Umgehungstechniken nutzen und Schwachstellen herkömmlicher Sandboxen ausnutzen.

Als weltweit erste KI-gestützte Engine zur Abwehr von Malware baut Zscaler Cloud Sandbox auf einer cloud-nativen, proxybasierten Architektur auf und unterstützt Organisationen durch automatische Inline-Erkennung und intelligente Isolierung unbekannter Bedrohungen und verdächtiger Dateien. Mit Funktionen zur unbegrenzten latenzfreien Überprüfung sämtlicher Webprotokolle und Dateiübertragungsprotokolle, einschließlich SSL/TLS, verhindert die Sandbox der Cloud-Generation durch gründliche und dynamische Echtzeitanalyse, dass unbekannte und potenziell schädliche Dateien als Downloads bei Usern ankommen.

Die unbekannte oder verdächtige Datei wird zunächst durch eine vorfilternde Analyse-Engine geschickt, die den Dateiinhalt mit mehr als 40 Bedrohungs-Feeds, Antiviren-Signaturen, YARA-Regeln und KI-/ML-Modellen abgleicht, um ein schnelles Urteil zu fällen und ähnliche bekannte Bedrohungen zu blockieren. Nach der ersten Sichtung wird die Datei einer robusten statischen, dynamischen und sekundären Analyse unterzogen, die auch die Ausführung der Datei in einer kontrollierten, isolierten Umgebung umfasst, um zu einem aussagekräftigen Ergebnis zu kommen. Der letzte Schritt ist die Nachbearbeitung, bei der die Zscaler-Bedrohungsdatenbank und die Richtliniendurchsetzung des Kunden aktualisiert werden.

Mithilfe der KI-basierten Entscheidungen werden ungefährliche Dateien sofort freigegeben, während schädliche Dateien für alle globalen Zscaler-User aufgrund des gemeinsamen Schutzes durch den Cloud-Effekt blockiert werden. So werden Patient-Zero-Infektionen und neuartige Bedrohungen für alle User unabhängig von Gerät und Standort abgewehrt.




© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

## Vorteile der Sandbox der Cloud-Generation

Neben der Inline-Quarantäne verdächtiger Dateien, der KI-basierten Echtzeitanalyse und der sofortigen Beurteilung ohne Verzögerungen kann das detaillierte, erweiterte Reporting von Zscaler Sandbox das Sandboxing von der letzten Abwehrmaßnahme in den ersten Schritt einer intelligenten Verteidigungsstrategie umwandeln. Durch die Anwendung von Verhaltensinformationen echter Malware, die auf Ihr Unternehmen abzielt, können Sie SecOps-Workflows bereichern, um Ihre Verteidigungsmaßnahmen im gesamten Security-Stack zu stärken.

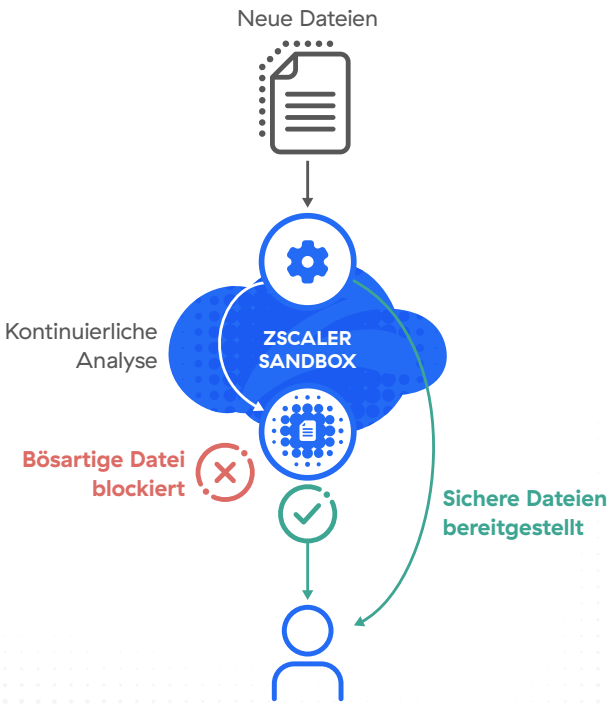
**Intelligente Abwehr neuartiger Bedrohungen und Patient-Zero-Infektionen**
Angreifer nutzen Verschlüsselung und vertrauenswürdige Cloud-Anwendungen, um unbemerkte Angriffe auszuführen. In einem kürzlich veröffentlichten Report von ThreatLabZ wurde Malware beobachtet, die über Google Drive, AWS und OneDrive verbreitet wurde. Die Möglichkeit, Dateien in Web und FTP zu scannen, insbesondere verschlüsselten Traffic, sorgt für Transparenz und verhindert, dass sich Angreifer Zugang zu Ihrem Netzwerk verschaffen.

Bevor ein Mitarbeiter versehentlich ein neues schädliches Office-Dokument (Maldocs) mit einem versteckten Makro herunterlädt und öffnet, tritt die KI-gesteuerte Inline-Quarantänefunktion von Zscaler Sandbox in Aktion. Wenn die umfangreiche Dateianalyse eine hohe Risikobewertung ergibt, wird die Datei für den Mitarbeiter gesperrt und kann von anderen Zscaler-Usern nicht geöffnet werden. Die sofortige Beurteilung von Dateien ohne erneutes Scannen verhindert, dass die Produktivität der Mitarbeiter beeinträchtigt wird, während die automatische Quarantäne und Sperrung unbekannter oder bösartiger Dateien dazu führt, dass weniger Helpdesk-Tickets erstellt werden.

Nach der schnellen, zwanzigminütigen Bereitstellung von Zscaler Sandbox war das IT- und Sicherheitsteam eines Kunden in der Lage, 91 % der ungefährlichen Dateien nach Erhalt einer KI-gestützten Beurteilung sofort und sicher an die User weiterzuleiten. Die verbleibenden unbekannten Dateien wurden zur ausführlichen, dynamischen Analyse weitergeleitet, die ergab, dass 5 % der Dateien Malware oder anderweitigen Schadcode enthielten. Die Dateien werden für die vorgesehenen User und für alle globalen User und Geräte von Zscaler blockiert, unabhängig vom Standort, um einen gemeinsamen, konsistenten Schutz zu gewährleisten.

### KI-basierte Quarantäne zur Abwehr neuartiger Malware

Inline-Schutz mit sofortiger Bereitstellung sicherer Dateien, Abwehr von Patient-Zero-Angriffen und granularen Policy-Controls




© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

**Verbesserte SOC-Workflows mit Malware-Informationen und MITRE ATT&CK** Nach einer detaillierten Dateianalyse und der sicheren Entschärfung unbekannter Malware erstellt die Sandbox automatisch einen Analysebericht. Die kontrollierte, isolierte Sandbox-Umgebung erfasst Analyse-Screenshots und informiert Analysten über Umgehungstechniken (Polymorphismus und Obfuskation), Callback-Verhalten und andere Aktionen. In diesem Bericht werden der Lebenszyklus des Angriffs und die Killchain, das Verhalten der Malware und die Absicht der Payload detailliert beschrieben und mit dem MITRE ATT&CK-Framework abgeglichen.

Durch die Übertragung der kontextbezogenen Sandbox-Ergebnisse auf das ATT&CK-Framework können Sicherheits- und IT-Teams Erkenntnisse über den gesamten Security-Stack austauschen. Dadurch kann die Sandbox der Cloud-Generation nicht nur die letzte Abwehrmaßnahme gegen Malware sein, sondern auch der erste Schritt bei der Erkennung, was die Überprüfung und Reaktion beschleunigt und gleichzeitig die Bedrohungssuche unterstützt.

**Vereinfachte Richtlinienverwaltung mit granularen Kontrollen**
Da es sich um ein Cloud-Produkt handelt, muss keine Hardware gekauft und konfiguriert und keine Software verwaltet werden, was die Komplexität und die benötigten Ressourcen reduziert. Sie müssen nicht vor Ort sein, um jedes Gerät einzurichten und anzuschließen, sondern können die Zscaler Sandbox in zwei einfachen Schritten konfigurieren: **Kriterien** und **Maßnahmen**. Ein weiterer Vorteil ist, dass die Richtlinien einfach zu verwalten, zu konfigurieren und bereitzustellen sind. Mit nur wenigen Klicks können Administratoren Richtlinien implementieren, einschließlich der Reihenfolge der Regeln, damit diese präzise ausgeführt werden, und weiterer Richtlinien, die Usern oder Usergruppen unabhängig vom Standort folgen.

Für noch präzisere Kontrollen kann die Sandbox der Cloud-Generation die statische und dynamische Dateianalyse mit automatischer JA3-Fingerprinting-Erkennung verbessern und userdefinierte Hash-Blocklisten und YARA-Regeln konfigurieren. Darüber hinaus können Blockierungsrichtlinien auf Grundlage von Bewertungen Maßnahmen bei störenden oder verdächtigen Greyware- und Adware-Dateien ergreifen, die den Grenzwert der Bedrohungsbewertung normalerweise nicht überschreiten.

**Cloudnative Zero-Trust-Plattform als Grundlage**
Zscaler Sandbox ist eine vollständig integrierte Funktion von Zscaler Internet Access und Teil der Zscaler Zero Trust Exchange. Die einzigartige, proxybasierte Architektur schützt User inline und nicht erst nach einem Vorfall, indem sie den Traffic an den branchenweit größten Cloud-Security-Stack weiterleitet, um jedem User unabhängig von Standort oder Netzwerk umfassende, intelligente Schutzmechanismen zu bieten. Sie erhalten gemeinsamen, globalen Schutz mit Echtzeit-Updates, die aus 300 Billionen täglichen Bedrohungssignalen stammen, kombiniert mit Sicherheit der Cloud-Generation und dem Zero-Trust-Prinzip der minimalen Zugriffsrechte.

## Standard und Advanced Sandbox im Vergleich

| | Standard Sandbox | Advanced Sandbox | |
|---|---|---|---|
| ZIA-Editionen | Professional Edition<br>Business Edition | Transformation Edition<br>ELA Edition | **Advanced Sandbox kann als Add-on zur ZIA Professional und Business Edition erworben werden.** |
| Unterstützte Formate: | .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, Skriptdateien in Zips | |
| KI-basierte Quarantäne | — | ✓ | |
| Granulare Richtlinien | — | ✓ | |
| Reporting | — | ✓ | |
| API | — | ✓ | |

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

## Kernfunktionen der Sandbox der Cloud-Generation

| | |
|---|---|
| **Vorfilternde Analyse-Engine** | AV, Hash-Blocklisten, YARA-Regeln, automatisierte JA3-Fingerprinting-Erkennung und ML-/KI-Modelle |
| **Statische, dynamische und sekundäre Analyse** | Statische Analyse und dynamische Analyse, einschließlich Code-Analyse und sekundärer Payload-Analyse |
| **Unterstützte Formate:** | .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, Skriptdateien in Zips |
| **SSL-Inspektion** | Unbegrenzte Kapazität für SSL-/TLS-Überprüfung |
| **Aufbewahrung von Dateien** | Zscaler Cloud Sandbox läuft ausschließlich im Speicher. Identifizierbare Informationen werden während der Analyse aus den Dateien entfernt. Nach Abschluss der Analyse werden ungefährliche Dateien aus dem Speicher gelöscht, während bösartige Dateien verschlüsselt und auf unbestimmte Zeit gespeichert werden. So können die Erkenntnisse allen Zscaler-Usern zur Verfügung gestellt werden, damit kontinuierlicher Schutz gewährleistet wird. |
| **OS-Support** | Windows XP, Windows 10, Android |
| **Protokoll-Support** | HTTP, HTTPS, FTP, FTP über HTTP |
| **Dateien pro Tag** | Unbegrenzt |
| **Maximale Dateigröße** | 20 MB für Windows und 50 MB für Android |
| **Bereitstellungsmethode** | Cloudnativ |
| **Integrierte Threat Intelligence** | Threat-Intelligence-Feeds von über 40 Sicherheitspartnern |
| **Verwaltung und Reporting** | Vollständiges Reporting einschließlich Malware-Verhalten und -Absicht, IOCs (Indicators of Compromise), abgelegte Dateien, PCAPs |
| **Forensische Analyse** | Sample, sekundäre Payloads, PCAPs |
| **API-Support** | Robuste API-Unterstützung, Berichtsabruf über API im JSON-Format |
| **Granulare Richtlinien** | Einfach zu verwendende und zu konfigurierende Richtlinien für User, Standorte, Standortgruppen, Dateitypen, Usergruppen, Abteilungen, URL-Kategorien und Protokolle |
| **Data Protection- und Compliance-Zertifizierungen** | Die Zscaler Cloud Firewall entspricht strengen weltweiten handelsrechtlichen und staatlichen Rahmenvorschriften in Bezug auf Risiko, Data Protection und Compliance. |
| **Branchen- und Datenschutz-vorschriften** | Die Zscaler Cloud Firewall ist konform mit branchenspezifischen und nationalen Datenschutzvorschriften. |

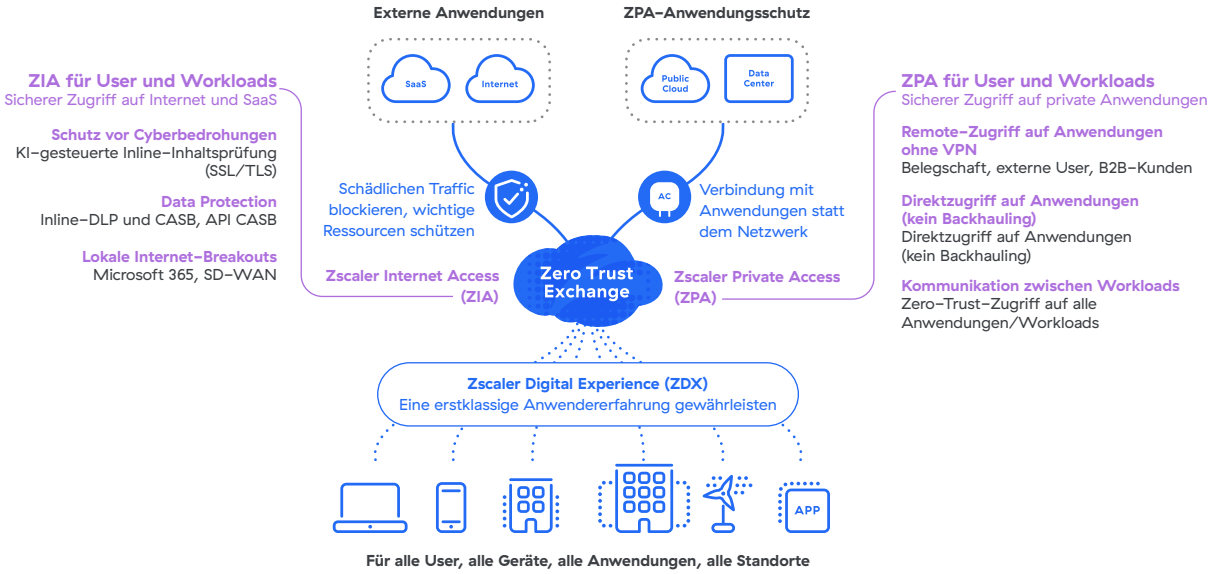
© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

## Zscaler Sandbox ist vollständig mit Zscaler Internet Access™ integriert und Teil der ganzheitlichen Zero Trust Exchange

Die Zscaler Zero Trust Exchange ermöglicht es Mitarbeitern, mit schnellen und sicheren Verbindungen von überall auf Anwendungen zuzugreifen, sodass das Internet effektiv als Unternehmensnetzwerk fungiert. Die Plattform beruht auf dem Zero-Trust-Prinzip der minimalen Rechtevergabe und gewährleistet ganzheitliche Sicherheit mithilfe einer kontextbasierten Identitäts- und Policy-Durchsetzung.

### Zero Trust für User, Workloads und IIoT/Betriebstechnologie (OT) — mit Zscaler

Bereitstellung innerhalb weniger Wochen zur Verbesserung der Cybersicherheit und Anwendererfahrung




**Gartner**

**Zscaler wurde im Gartner MQ für SSE als Leader ausgezeichnet und erzielte die höchste Bewertung bei der „Fähigkeit zur Umsetzung“.**

**Weitere Informationen →**

zscaler™ | Experience your world, secured.™

**Über Zscaler**
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ und ZPA™ sowie weitere unter **zscaler.de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de