E-BOOK

Kaufratgeber zur Bedrohungsabwehr

Finden Sie die beste KI-gesteuerte Bedrohungsschutzlösung, um dateibasierte Angriffe zu stoppen.

Inhalt

Neue Sicherheitskonzepte für die aktuelle Bedrohungslage

Perimeterbasierte Sicherheit ist den Anforderungen digital aufgestellter Unternehmen nicht gewachsen

Mit der Umstellung auf hybride Arbeitskonzepte und in der Cloud gehostete Anwendungen haben sich auch die Gewohnheiten und Bedürfnisse der User geändert. Mitarbeiter verwenden nicht verwaltete Geräte über ungesicherte Netzwerke wie öffentliches WLAN, um auch im Homeoffice, an anderen Remote-Standorten oder unterwegs produktiv zu bleiben, wodurch das Internet de facto zum neuen Unternehmensnetzwerk wird. Durch diese Ausweitung der Zugriffspunkte ist der herkömmliche Sicherheitsansatz nach dem Festung-mit-Burggraben-Prinzip nicht mehr ausreichend, um Ihre User, Anwendungen und Daten zu schützen. Unternehmen, die sich ausschließlich auf Perimeterschutzmaßnahmen verlassen, setzen sich Risiken aus, da netzwerkzentrierte Kontrollen für den direkten Internetzugriff umgangen werden und dabei häufig die Userfreundlichkeit Vorrang vor der Sicherheit hat.

Cyberangriffe der neuen Generation können Legacy-Sicherheitskontrollen mühelos umgehen. Um diesen Trends Paroli zu bieten, ist ein Umdenken erforderlich, damit Sicherheitskontrollen nicht mehr am Netzwerkperimeter, sondern in unmittelbarer Nähe der User, Workloads und OT-/IoT-Geräte implementiert werden.

Bedrohungsakteure machen sich die Verlagerung in die Cloud zunutze

Im Bestreben, einen Ausweg aus dieser Bredouille zu finden, versuchen die zuständigen Sicherheitsbeauftragten, Legacy-Kontrollen an die Anforderungen zunehmend mobil- und Cloud-orientierter Unternehmen anzupassen. Davon konnten Bedrohungsakteure massiv profitieren. Analysen des ThreatLabz-Teams von Zscaler haben ergeben, dass das Bemühen, mehrere Netzwerk-Edges zugleich zu schützen, zur Entstehung von Sicherheitslücken führt:

- **86 %** der Bedrohungen werden über verschlüsselte Kanäle übermittelt, wobei Malware 78 % der verschlüsselten Angriffe ausmacht.[1]
- Ransomware-Angriffe haben im Vergleich zum Vorjahr um **40 %** zugenommen.[2]
- Die in der Zscaler Sandbox beobachteten Payloads nahmen um **58 %** zu.[2]

Diese rasante Entwicklung digitaler Bedrohungen, verschärft durch die wachsende Angriffsfläche der Cloud macht deutlich, dass Sicherheitsteams ihre Strategien überdenken und ihre Abwehrmaßnahmen gegen moderne Cyberrisiken verstärken müssen.

1. Report von Zscaler ThreatLabz: Verschlüsselte Angriffe 2023
2. Report von Zscaler ThreatLabz: Ransomware 2023

Höchste Zeit für die Umstellung auf Zero-Day-Malware-Schutz

Angreifer haben zwei entscheidende Vorteile: **Geschwindigkeit** und **Verbreitung**. Malware-Entwickler erstellen Bedrohungen schneller, als Sicherheitsexperten sie erkennen und abwehren können. Dabei nutzen sie künstliche Intelligenz (KI), um Varianten zu erstellen, die herkömmliche Sicherheitsmaßnahmen und Erkennungsmethoden umgehen können.

Die Mehrzahl aller Phishing-Angriffe wird über schädliche Anhänge bzw. Links ausgeliefert. Die weitgehende Verschlüsselung des Traffics erschwert Abwehrstrategien zusätzlich. Heutige Bedrohungen verbergen sich oft im verschlüsselten Traffic. Dies unterstreicht die Bedeutung der Überprüfung des gesamten Web- und Nicht-Web-Traffics. Andernfalls kann es passieren, dass Sie unbeabsichtigt Malware in Ihr Netzwerk lassen.

Als unverzichtbarer Bestandteil des Security-Stacks dienen Sandbox-Lösungen zur Abwehr schädlicher Dateien und zur Verhinderung der Ausführung von Malware. Sie sollen eine wirksame Abwehr gegen unbekannte dateibasierte Angriffe darstellen, deren Ziel darin besteht, EDR und andere Scans auf bekannte Malware zu umgehen. Leider werden viele Sandboxen Out-of-Band eingesetzt und funktionieren nur, wenn Malware-Samples von NGFWs, Cloud-Sicherheitsprodukten oder Endgerät-Agents an sie weitergeleitet werden.

Dies bedeutet häufig, dass die Erkennung erst erfolgt, nachdem die Malware auf das Gerät eines Users heruntergeladen wurde. Dies steht im Widerspruch zu den Grundsätzen des Zero-Trust-Konzepts und ermöglicht Patient-Zero-Infektionen mit Malware oder Ransomware. Darüber hinaus nutzen viele Sandboxen keine KI/ML-Analyse in großem Maßstab zum automatischen Erkennen und Isolieren unbekannter Bedrohungen und verdächtiger Dateien — ein Schlüsselfaktor für die Bereitstellung eines Inline-Schutzes vor Patient-Zero-Bedrohungen ohne Produktivitätsunterbrechung.

Signaturbasierte Viren- und Eindringschutzsysteme allein können keinen zuverlässigen Schutz vor Zero-Day-Angriffen und polymorphen Bedrohungen gewährleisten.

Anforderungen an eine Cloud Sandbox

Bislang hatten Bedrohungsakteure die Oberhand und konnten die Umstellung auf Cloud-Architekturen erfolgreich für ihre Zwecke nutzen.

Unternehmen, die hier gegensteuern wollen, benötigen unbedingt eine geeignete cloudbasierte Sandbox-Lösung zur Verhinderung von Patient-Zero-Infektionen und der Abwehr von Advanced Persistent Threats.

Im folgenden Abschnitt werden die spezifischen Anforderungen erläutert, auf die Sie bei der Auswahl der richtigen Cloud Sandbox unbedingt achten müssen.

Entschlüsselung und Überprüfung in großem Maßstab

Zum Schutz privater Kommunikation und vertraulicher Daten hat sich Verschlüsselung als gängige Sicherheitsmaßnahme etabliert. Leider profitieren auch Bedrohungsakteure von diesem Trend, da schädliche Payloads im verschlüsselten Traffic versteckt werden.

Das Entschlüsseln und Überprüfen des gesamten Traffics ist ein recheninteniver Prozess und kann leistungsstarke Sandbox-Geräte in Produktivitätshemmer verwandeln, die den Geschäftsbetrieb durch inakzeptable Latenzen unterbrechen.

Bei der Auswahl einer zukunftsfähigen Sandbox-Lösung sollten Sie sich stattdessen für einen Anbieter entscheiden, der unbegrenzte latenzfreie Inline-Entschlüsselung und -Überprüfung bereitstellt.

Die Bedrohungen über HTTPS nahmen im Vergleich zum Vorjahr um 24,3 % zu, was einem Anstieg auf 30 Milliarden verschlüsselte Angriffe im Jahr 2023 entspricht.[3]

Checkliste für einen Kauf:

- ☐ Entschlüsselung von SSL-Traffic ohne Installation zusätzlicher Hardware oder virtueller Maschinen (VM)
- ☐ Überprüfung und Analyse folgender Dateitypen ohne Latenzen oder Kapazitätslimits:

EXE	DOC(X)	TAR
DLL	XLS(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	Skriptdateien in ZIPs
SWF	BZ2	

3. Report von Zscaler ThreatLabz: Verschlüsselte Angriffe 2023

Checkliste für einen Kauf:

- ☐ Sofortige Durchsetzung von Richtlinien für alle User mit identischem Schutzniveau, unabhängig davon, ob sie sich innerhalb oder außerhalb des Unternehmensnetzwerks befinden
- ☐ Erweiterte Quarantäneregeln und -funktionen zur Isolierung sämtlicher Dateien verdächtigen Ursprungs
- ☐ Zentrales Richtlinienmanagement, das eine detaillierte Kontrolle über Sandboxing-Vorgänge ermöglicht, einschließlich der Zulassung von Datei-typen und der automatischen Sperrung verdächtiger Ziele

Zentrale Richtlinienverwaltung und Regeln

Vermeiden Sie eine falsche Regelverwaltung und das manuelle Konfigurieren von Sand-boxen an jedem Gateway mit einer zentralisierten Richtlinienverwaltung und Regeln aus der Cloud. Erwägen Sie Lösungen mit adaptiven und dynamischen Richtlinien, die den Zero-Trust-Grundsätzen gemäß **NIST 800-207**. Durch kontextbasiertes Festlegen von Zugriffs- und Sicherheitsrichtlinien — einschließlich Rolle und Standort des Users, Gerätestatus und ange-forderter Daten — minimiert Zero Trust die Angriffsflächen. Aus der Cloud bereitgestellte Lösungen haben zusätzliche Vorteile, mit denen Sie Bedrohungen für alle User im Unternehmen blockieren können. Auf diese Weise entfallen Datei-Retrospektiven (Beispiele: Out-of-Band-Überprüfungen und nachträglich angewendete Schutzmaßnahmen) und die Sicherheit ist besser synchronisiert. Ein entscheidender Aspekt der Sandbox-Richtlinie ist, dass sie die Flexibilität bietet, das Geschäft zu unterstützen, mit granularen Regeln für unterschiedliche Usergruppen, Standorte, URL-Kategorien oder Aktionen. Mithilfe granularer Kontrollen können Sie Richtlinien an die Risikotoleranz und Leistungserwartungen Ihres Unternehmens anpassen.

Anpassung von Richtlinien gemäß Risikotoleranz und Performance-Erwartungen

Eine cloudbasierte Sandbox-Lösung sollte die Maßnahmen zur Risikokontrolle und Richtli-niendurchsetzung an den speziellen Anforderungen des jeweiligen Unternehmens ausrichten. Im Vorfeld muss das Risikoprofil des Unternehmens abgeklärt werden:

- **Geringe Toleranzschwelle gegenüber Schaddateien:** Unternehmen, die Risiken vermeiden möchten, können für unbekannte oder verdächtige Dateien die Option „Quarantäne für erst-malige Aktionen“ wählen. Dadurch lassen sich Patient-Zero Infektionen zuverlässig vermeiden, weil die Sandbox die Datei analysiert, bevor sie heruntergeladen werden kann.
- **Geringe Toleranzschwelle für das Isolieren von Dateien:** Risikotolerante Unternehmen, die Verzögerungen und Unterbrechungen vermeiden möchten, können als erste Aktion „Quarantäne und Isolierung“ wählen. Diese Aktion integriert die Sandbox mit Cloud-Browser-Isolationsfunktionen und bietet Usern sofortigen Zugriff auf eine schreibgeschützte PDF-Datei ohne aktiven Inhalt, während die Sandbox im Hintergrund potenziell schädliche Dateien analysiert.

Unabhängig von den speziellen Anforderungen des jeweiligen Unternehmens muss die Lösung eine unkomplizierte Durchsetzung von Richtlinien für alle User, Gruppen, Abteilungen, Standorte und Standortgruppen unterstützen.

Intelligente Analyse und Bedrohungsinformationen:

Es ist bekannt, dass Angreifer erfolgreiche Angriffe wiederverwenden. Daher ist es wichtig, Schutzmaßnahmen mit der Sicherheits-Community zu teilen, um Bedrohungen schnell zu stoppen. Cloud-Sandboxen spielen dabei eine wichtige Rolle, indem sie Telemetriedaten erfassen und Erkenntnisse aus neu identifizierten Bedrohungen mit Bedrohungs-Feeds und der Sicherheits-Community teilen.

KI-gestützte Engine zur Vorbeugung von Malware

Cloudbasierte Sandbox-Lösungen gewährleisten zuverlässigeren Schutz, da sie über die Kapazitäten zur Verwaltung rechenintensiver KI/ML-Modelle verfügen.

Die Sandbox-Lösung sollte unbekannte Bedrohungen bzw. verdächtige Dateien mit erweiterten KI/ML-Funktionen inline erkennen, isolieren und blockieren, ohne dass unschädliche Dateien erneut gescannt werden müssen.

- **Sofortige Dateibeurteilung:** Durch die sofortige Erkennung von Dateien, die höchstwahrscheinlich bösartig sind, müssen User nicht auf eine Beurteilung warten.
- **Zero-Day-Prävention:** Kaum zu glauben, aber wahr: Längst nicht jede Sandbox verhindert Patient-Zero-Infektionen, indem sie unbekannte Bedrohungen unter Quarantäne stellt, bevor sie deren Download zulässt.

SOC-Workflows mit Threat Intelligence

Analysten können viele Stunden am Tag damit verbringen, eine einzige Bedrohung zu untersuchen. Suchen Sie nach einer Cloud-Sandbox, die diese Belastung reduziert und die Untersuchung und Reaktion beschleunigt, indem sie Verhaltenseinblicke und Bedrohungsinformationen zu schädlichen Payloads teilt. Sicherheitsteams sollten in der Lage sein, Untersuchungen mit direkter Dateianalyse in der Sandbox über Out-of-Band-API-Übermittlungen zu unterstützen. Stellen Sie sicher, dass Bedrohungs-Feeds in Ihre vorhandenen Sicherheitstools integriert sind. Sie sollten Folgendes enthalten: aktualisierten Kontext zu gemeldeten URLs, extrahierte Indikatoren für Kompromittierung (IoCs) sowie Taktiken, Techniken und Verfahren (TTPs), die auf Cybersicherheits-Frameworks wie MITRE ATT&CK® abgestimmt sind.

Checkliste für einen Kauf:

- ☐ KI-basierte Quarantänefunktionen, die KI/ML nutzen, um eine sofortige Bewertung vedächtiger Dateien abzugeben und Bedrohungen zu stoppen, ohne dass eine Dateianalyse erforderlich ist
- ☐ Autonomer Beitrag zur Bereitstellung von Abwehrmechanismen zum Schutz vor neuartigen Bedrohungen, die täglich allen Usern und Netzwerken weltweit verfügbar gemacht werden
- ☐ Integration von Bedrohungsinformationen mit vorhandenen Sicherheitstools
- ☐ Programmatische, API-gesteuerte „Out-of-Band"-Sandbox-Dateiübermittlung mit separater Warteschlange für über die API übermittelte Dateien

Eine effektive Sandbox-Lösung muss aussagekräftige Erkenntnisse liefern, die über die Bereitstellung eines Threat Scores hinausgehen. So sollte sie in der Lage sein, detaillierte Informationen zu beobachteten Ausweichtechniken zu dokumentieren, u. a.:

- Verzögerte Code-Ausführung zur Vermeidung der Sandbox-Erkennung
- Erfassung und Anzeige des durch das Netzwerk fließenden Traffics
- Öffnen von Ports zur Ermöglichung von Remote-Konnektivität
- Versuchte laterale Bewegungen zur Identifizierung lukrativer Angriffsziele
- Versuchte Zulassung von Remote-Zugriffen

Berichterstellung

Sicherheitslösungen mit Berichterstellung sind nur dann nützlich, wenn sie umsetzbar sind. Cloud-Sandbox-Berichte sollten folgende Bedingungen erfüllen:

- Berücksichtigung des gesamten Angriffszyklus
- Einfache Bedienung und Navigation
- Unkomplizierte Verarbeitung und Umsetzung der gelieferten Erkenntnisse
- Verfügbar über eine Programmierschnittstelle (API) zur unkomplizierten Korrelation mit vorhandenen Logs
- Bereitstellung im Rahmen einer ganzheitlichen Plattform, die auch Compliance-Reporting unterstützt

Das MITRE ATT&CK Framework zur Unterstützung des SOC

Bei der Bewertung der Reporting-Funktionen sollte auch darauf geachtet werden, ob bzw. inwieweit eine Ausrichtung der gelieferten Informationen am **MITRE ATT&CK Framework** gegeben ist. Eine engmaschige Zuordnung unterstützt SOC-Teams beim Aufbau taktischer Abwehrmechanismen in anderen Bereichen des Security-Stacks, sodass die Sandbox einen unmittelbaren Beitrag zu SOC-Workflows leistet.

Je nach Reifegrad im Umgang mit dem Framework können die Reporting-Funktionen zu verschiedenen Zwecken genutzt werden:

- Reduzierter Arbeitsaufwand durch Anwendung der bereitgestellten Taxonomie
- Erkennung von Stealth-Techniken, die EDR-Lösungen (Endpoint Detection and Response) möglicherweise umgehen
- Vergleichende Bewertung anderer Kontrollmaßnahmen
- Gezielte Fokussierung der Abwehrmaßnahmen auf unternehmensrelevante Taktiken, Techniken und Verfahren
- Erstellung von Reverse-Engineering-Berichten

Wesentliche Fragen vor der Kaufentscheidung

Zur Unterstützung der Entscheidungsfindung haben wir nachstehend alle wesentlichen Fragen im Überblick zusammengefasst, die vor dem Kauf geklärt werden sollten:

Lässt die Sandbox eine anfängliche Patient-Zero-Infektion zu?

Sandboxen, die anfängliche Infektionen zulassen, während eine Datei analysiert wird, können die Sicherheit des Unternehmens nicht gewährleisten.

Deckt die Lösung alle User und ihre Geräte ab, unabhängig vom Standort?

Ihre User greifen möglicherweise unterwegs, auf ihren eigenen Geräten oder über ungesicherte Netzwerke auf Unternehmensressourcen zu. Deswegen müssen unbedingt alle Geräte gesichert werden, die für ihre Arbeit unverzichtbar sind.[4]

Erkennt die Lösung Angriffe inline oder erfordert sie Out-of-Band-Dateiübermittlungen?

Inline-Lösungen können Bedrohungen erkennen und direkt blockieren, ohne auf NGFW-Netzwerkflüsse angewiesen zu sein oder EDR-Software für Endpunkte zu verwenden.

Untersucht die Sandbox den Traffic über alle HTTP-, HTTPS-, FTP- und FTP-über-HTTP-Protokolle? Gibt es Einschränkungen?

Eine cloudbasierte Sandbox eignet sich gegebenenfalls besser zur latenzfreien Überprüfung des gesamten Traffics als unverzichtbare Voraussetzung zur Erkennung versteckter Malware.

Entspricht sie den geltenden Gesetzen und Vorschriften, einschließlich der Zero-Trust-Anforderungen?

Compliance-Vorschriften enthalten teilweise strenge Anforderungen für den Umgang mit Sandboxing, die Aufbewahrung von Dateien und den Datenschutz. Mit einer Lösung, die nur im Speicher arbeitet und während der Analyse identifizierbare Informationen entfernt, können Sie diese Anforderungen erfüllen. Überlegen Sie außerdem, ob Lösungen den Grundsätzen von Zero Trust entsprechen, wie sie in den globalen Standards NIST 800-207 festgelegt sind, und verwenden Sie diese als Leitfaden zur Reduzierung der Angriffsfläche und zum Schutz von Daten.

Mit welchen anderen Sicherheitsmodulen ist die Sandbox-Lösung kompatibel?

Kein Einzelprodukt kann zuverlässigen Schutz vor sämtlichen Advanced Persistent Threats (APTs) gewährleisten. Daher ist ein mehrschichtiger Ansatz erforderlich, der Funktionen zur Bedrohungsabwehr, Risikominderung, Erkennung und Vorfallbehebung kombiniert. Als unverzichtbarer Bestandteil eines derartigen Ansatzes muss die Sandbox-Lösung unbedingt mit allen weiteren Lösungen und Modulen kompatibel sein.

---

4. us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox mit Advanced Threat Protection

Argumente für die Umstellung auf eine echte Cloud-native Inline-Sandbox

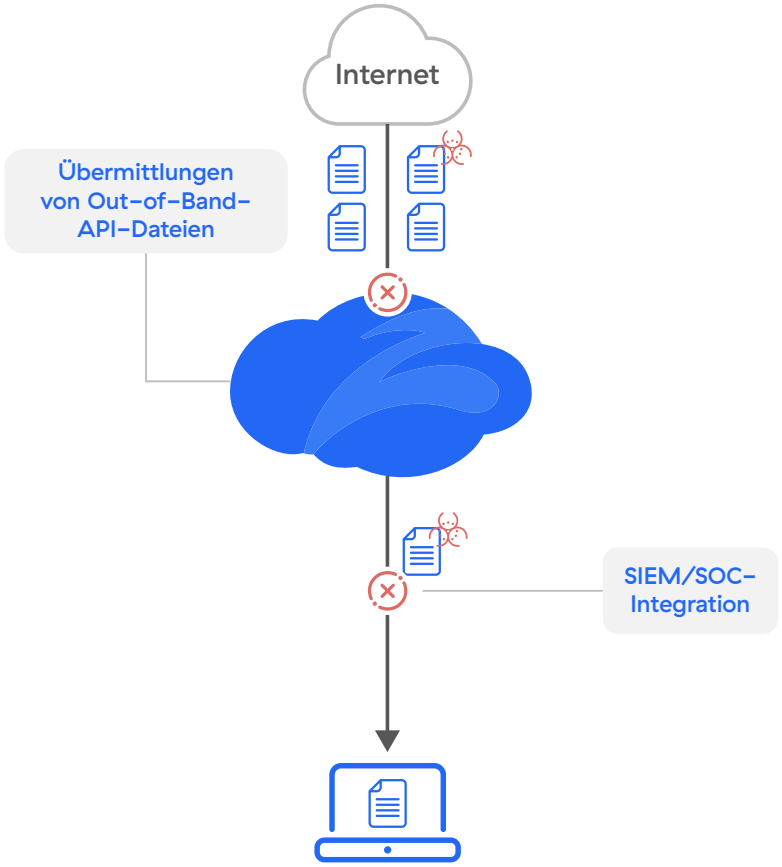
Expandierende Angriffsflächen und Sicherheitslücken in herkömmlichen Security-Stacks setzen Unternehmen einem erhöhten Angriffsrisiko aus. Eine Cloud-native Inline-Sandbox kann hier wirksam Abhilfe schaffen. Zscaler Cloud Sandbox wurde speziell zur Erkennung und Blockierung aktueller Bedrohungen entwickelt und gewährleistet zuverlässigen Schutz vor Zero-Day-Malware für alle User an allen Standorten.

Als weltweit erste KI-gestützte Engine zur Abwehr von Malware baut Zscaler Cloud Sandbox auf einer Cloud-nativen, proxybasierten Architektur auf und unterstützt Unternehmen 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 Cloud Sandbox durch gründliche und dynamische Echtzeitanalyse, dass unbekannte und potenziell schädliche Dateien als Downloads bei Usern ankommen.

KI-Vorteil der Zscaler Sandbox: Trainiert anhand von über 500 Millionen Samples, mit Echtzeit-Sicherheitsupdates auf Basis von 300 Billionen täglicher Signale.

KI-basierte Quarantäne zur Abwehr neuartiger Malware

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



Geringere Komplexität und Kosten

- Einfache Bereitstellung ohne Verwaltung von Hardware oder Software
- Verzicht auf redundante bzw. separate Einzelprodukte
- Kein Backhauling des Internet-Traffics über MPLS oder VPN

Sofortiger adaptiver Schutz für alle User und Standorte

- Zentrale Managementoberfläche zur Festlegung global gültiger Richtlinien
- Sofortige Durchsetzung von Richtlinienänderungen
- Umgehende Blockierung neu entdeckter Bedrohungen für alle Kunden

Erkennung versteckter Bedrohungen

- KI-gestützte Quarantäne zur Verhinderung von Patient-Zero-Infektionen durch bekannte und neuartige Bedrohungen
- Heraufladen von Dateien zur Analyse (Dateiüberprüfungsportal)

Integrierter Plattform-Service

- Vorfilterung aller bekannten Bedrohungen mithilfe von Virenschutz, Hash-Blocklists, YARA-Regeln zur Klassifizierung von Malware, automatischer JA3-Fingerabdruck-Erkennung und ML/KI-Modellen
- CIF-Feeds (Collective Intelligence Framework) ermöglichen die Integration der Zscaler-Lösung mit über 60 Threat-Feeds zusätzlich zum eigenen Feed, der Informationen aus Milliarden von Transaktionen sämtlicher Zscaler-Kunden bezieht.
- Durch Kombinieren einer Cloud Sandbox mit einer EDR-Lösung verbessern Sie die Zuverlässigkeit Ihrer Cybersicherheit und mindern das Risiko von unbefugten Zugriffen, Malware-Ausführung und persistenten Angriffen

Eine ESG Economic Validation Study ergab, dass Zscaler Zero Trust Exchange zu einer 90-prozentigen Reduzierung der Sicherheitsanwendungen führte.[5]

- Statische, dynamische und sekundäre Analyse, einschließlich Code-Analyse und sekundäre Payload-Analyse
- Unbegrenzte latenzfreie SSL-Überprüfung
- Schutz für eingehenden und ausgehenden Traffic
- Umfassende forensische Informationen (User, Ausgangspunkt, Umgehungstaktiken usw.) zur Verbesserung der Untersuchungs- und Behebungsmaßnahmen bei Sicherheitsvorfällen

Zscaler Cloud Sandbox™ wird als vollständig integrierte Funktion von Zscaler Internet Access™ im Rahmen der Zscaler Zero Trust Exchange™ bereitgestellt.

Weitere Informationen finden Sie unter
zscaler.com/de/technology/cloud-sandbox

5. info.zscaler.com/resources-industry-report-esg-economic-validation

zscaler™ | Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen überall vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist weltweit in 150 Rechenzentren verfügbar und ist somit die größte Inline-Cloud-Sicherheitsplattform der Welt. Weitere Informationen finden Sie unter **www.zscaler.com/de**.

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

zscaler.com/de