E-Book

Kaufratgeber zur Bedrohungsabwehr

Hinweise zur Auswahl der richtigen Lösung zum Schutz vor dateibasierten Bedrohungen

E-Book

Inhaltsverzeichnis

Neue Sicherheitskonzepte für die aktuelle Bedrohungslage **3**

Perimeterbasierte Sicherheit ist den Anforderungen digital aufgestellter Unternehmen nicht gewachsen 3

Bedrohungsakteure machen sich die Verlagerung in die Cloud zunutze 3

Höchste Zeit für die Umstellung auf Zero-Day-Malware-Schutz **4**

Anforderungen an eine Cloud Sandbox **5**

Entschlüsselung und Überprüfung in großem Maßstab 6

Zentrale Richtlinienverwaltung und Regeln 7

Anpassung von Richtlinien gemäß Risikotoleranz und Performance-Erwartungen 7

Intelligente Analyse und Bedrohungsinformationen 8

KI-gestützte Engine zur Abwehr von Malware 8

SOC-Workflows mit Threat Intelligence 8

Das MITRE ATT&CK Framework zur Unterstützung Ihres SOC 9

Wesentliche Fragen vor der Kaufentscheidung 10

Zscaler Cloud Sandbox mit Advanced Threat Protection **11**

Argumente für die Umstellung auf eine echte Cloud-native Inline-Sandbox 11

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. Häufig erfolgt der Zugriff auf Unternehmensressourcen über nicht verwaltete Geräte und ungesicherte Netzwerke wie öffentliches WLAN, um auch unterwegs bzw. an Remote-Standorten produktiv zu bleiben. Damit wird das Internet als Unternehmensnetzwerk verwendet und aus einem Netzwerkperimeter werden Tausende. Herkömmliche Sicherheitslösungen gewährleisten damit keinen ausreichenden Schutz mehr für User, Anwendungen und Daten. Organisationen, die sich weiterhin auf perimeterbasierte Kontrollen verlassen, gehen das Risiko ein, dass User diese netzwerkzentrierten Schutzmechanismen der Bequemlichkeit halber umgehen und stattdessen Direktverbindungen zum Internet herstellen.

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 Betriebstechnologie-/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 Organisationen 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:

- Ransomware-Angriffe haben im Vergleich zum Vorjahr um **80 % zugenommen**.[1]
- Mehrfacherpressungen nehmen ebenfalls zu — so stieg die Anzahl der Ransomware-Angriffe mit Doppelerpressung um **117 %**.[1]
- Die Anzahl der versuchten Phishing-Angriffe nahm von 2020 auf 2021 **um 29 %** zu.[2]
- **85 %** der Organisationen waren 2021 von einem erfolgreichen Cyberangriff betroffen.[3]
- **63 %** der Opfer von Ransomware-Angriffen zahlten 2021 Lösegelder, und diese Erfolgsquote bedingte eine Zunahme der Angriffe.[3]

1. https://www.zscaler.de/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.de/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

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

Bedrohungsakteure profitieren von einem doppelten Vorteil: **schnelle Entwicklung** und **schnelle Ausbreitung**. Neuartige Bedrohungen werden schneller entwickelt als effektive Gegenmaßnahmen zu ihrer Erkennung sowie Abwehr und breiten sich mit enormer Geschwindigkeit aus.

Die Mehrzahl aller Phishing-Angriffe wird über schädliche Anhänge bzw. Links ausgeliefert. Wenn Ihre Organisation nicht den gesamten — webbasierten ebenso wie nicht webbasierten — Traffic überprüft, einschließlich sämtlicher Dateiübertragungsprotokolle und SSL/TLS-verschlüsselter Dateien, können Bedrohungen im verschlüsselten Traffic ins Netzwerk gelangen. Das ermöglicht Angreifern die Exfiltration vertraulicher Daten bzw. die Erpressung der Organisation mit Lösegeldforderungen.

Als unverzichtbarer Bestandteil des Security-Stacks dienen Sandbox-Lösungen zur Abwehr schädlicher Dateien und zur Verhinderung der Ausführung von Malware. Sie sind als letzte Verteidigungslinie und zugleich als Ausgangspunkt für die Erkennung und Untersuchung neuartiger Bedrohungen konzipiert. Legacy-Sandbox-Appliances können indes keinen Inline-Schutz gewährleisten und machen den Einsatz von Add-on-Geräten zur Entschlüsselung und Überprüfung des SSL-Traffics erforderlich. Die nachträgliche Anwendung von Schutzmechanismen, wenn die Malware bereits zum User oder Gerät weitergeleitet wurde, entspricht nicht den Grundsätzen des Zero-Trust-Konzepts.

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.

Organisationen, die hier gegensteuern wollen, benötigen unbedingt eine geeignete Cloud-basierte 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.

Die Entschlüsselung und Überprüfung des Traffics verspricht hier Abhilfe, ist jedoch sehr rechenintensiv. Legacy-Sandbox-Lösungen mit Passthrough-Architekturen können nicht verhindern, dass Malware im nicht untersuchten Traffic ins Netzwerk gelangt. Die Nachrüstung mit Appliances zur SSL-Überprüfung ist nicht skalierbar und führt zu einer teuren ausufernden Anzahl von Geräten. Gleichzeitig dringen Patient-Zero-Infektionen weiter in das Netzwerk ein.

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

HTTPS-basierte Bedrohungen haben im Vergleich zum Vorjahr um gut 314 % zugenommen und verzeichneten damit im zweiten Jahr hintereinander einen Zuwachs von über 250 %.[4]

Die gewählte Lösung muss folgende Voraussetzungen erfüllen:

- ☐ 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	XLX(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	Skript-dateien in ZIPs
SWF	BZ2	

4. *https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks-de*

Die gewählte Lösung muss folgende Voraussetzungen erfüllen:

- 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
- Zentrale Richtlinienverwaltung
- Granulare Kontrollen für Greyware– und Adware–Dateien

Zentrale Richtlinienverwaltung und Regeln

Die in der Cloud bereitgestellte zentrale Richtlinienverwaltung und Regelerstellung verhindert Fehler und erspart Ihnen die manuelle Konfiguration von Sandbox–Lösungen an jedem einzelnen Gateway. Sie sollten Lösungen mit adaptiven und dynamischen Richtlinien in die engere Auswahl ziehen, die die Zero–Trust–Grundsätze gemäß **NIST 800–207** erfüllen. Durch konsequente Anwendung kontextbasierter Zugriffs– und Sicherheitsrichtlinien minimiert eine Zero–Trust–Lösung die Angriffsfläche. Berücksichtigt werden dabei sowohl die Rolle und der Standort des Users als auch der Sicherheitsstatus des Geräts und die jeweils angeforderten Daten. Cloud–basierte Lösungen bieten zusätzliche Vorteile in Bezug auf die sofortige Blockierung neu erkannter Bedrohungen: Anstelle nachträglicher Schutzmaßnahmen, wie sie bei der Out–of–Band–Untersuchung üblich sind, kann so zuverlässiger Echtzeitschutz für sämtliche User der Organisation gewährleistet werden.

Granulare Kontrollen ermöglichen die Anpassung von Richtlinien gemäß der Risikotoleranz und den Performance–Erwartungen der jeweiligen Organisation.

Anpassung von Richtlinien gemäß Risikotoleranz und Performance–Erwartungen

Eine Cloud–basierte Sandbox–Lösung sollte die Maßnahmen zur Risikokontrolle und Richtliniendurchsetzung an den speziellen Anforderungen der jeweiligen Organisation ausrichten. Im Vorfeld muss das Risikoprofil der Organisation abgeklärt werden:

- **Geringe Risikotoleranz für schädliche Dateien:** Organisationen mit geringer Risikotoleranz sollten die Option wählen, unbekannte und potenziell verdächtige Dateien beim erstmaligen Herunterladen in Quarantäne zu setzen.
- **Hohe Risikotoleranz bei geringer Toleranz für Verzögerungen:** Organisationen mit höherer Risikotoleranz können Verzögerungen und Betriebsstörungen vermeiden, indem für unbekannte Dateien beim erstmaligen Herunterladen stattdessen die Option „Zulassen und scannen“ gewählt wird. Zusätzlichen Schutz bietet die Integration mit Funktionen zur Cloud Browser Isolation, die Dateien als Bilder anzeigen — dadurch werden sowohl Datenverluste als auch die Auslieferung aktiver Bedrohungen verhindert.

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

Intelligente Analyse und Bedrohungsinformationen

Erfolgreiche Angriffstaktiken werden von Bedrohungsakteuren gerne mehrfach verwendet. Zur schnellen Blockierung neuer Bedrohungen ist ein effektiver Austausch von Informationen und Schutzmaßnahmen zwischen Sicherheitsexperten daher unerlässlich. Cloud-basierten Sandbox-Lösungen, die Telemetriedaten erfassen und Erkenntnisse aus der Analyse neu erkannter Bedrohungen über entsprechende Feeds weiterleiten, kommt dabei eine entscheidende Funktion zu.

KI-gestützte Engine zur Malware-Abwehr

Cloud-basierte 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.
Dadurch ist ein zweifacher Vorteil gewährleistet:

- **Schnellere Beurteilung von Dateien:** Durch sofortige Weiterleitung unschädlicher Dateien und Analyse verdächtiger bzw. unbekannter Dateien reduzieren Sie den manuellen IT-Aufwand.
- **Zero-Day-Prävention:** Durch automatische Isolierung unbekannter Bedrohungen wird das Risiko von Zero-Day-Angriffen in der IT-Umgebung minimiert.

SOC-Workflows mit Threat Intelligence

Häufig ist die Analyse einer einzigen Bedrohung mit stundenlanger Arbeit verbunden. Eine Cloud-basierte Sandbox sollte hier für Entlastung sorgen und die Untersuchung und Behebung von Sicherheitsvorfällen durch effizienten Austausch von Informationen — sowohl von Erkenntnissen zum User-Verhalten als auch Threat Intelligence zu schädlichen Payloads — beschleunigen. Bei der Auswahl einer Lösung sollte auch darauf geachtet werden, dass die Integration von Threat Feeds mit vorhandenen Sicherheitstools unterstützt wird. Insbesondere betrifft dies folgende Arten von Informationen: Kontextdaten zu gemeldeten URLs auf dem jeweils aktuellen Stand, extrahierte Kompromittierungsindikatoren sowie Taktiken, Techniken und Verfahren gemäß Cybersicherheits-Frameworks wie MITRE ATT&CK®.

Die gewählte Lösung muss folgende Voraussetzungen erfüllen:

- ML/KI-Kapazitäten, die eng mit den Analysefunktionen integriert sind
- KI-basierte Quarantänekapazitäten mit Einsatz von ML/KI zum Abfangen und Analysieren potenziell schädlicher Dateien sowie zur schnellen Ausgabe umsetzbarer Beurteilungen
- Autonomer Beitrag zur Bereitstellung von Abwehrmechanismen zum Schutz vor neuartigen Bedrohungen, die täglich allen Usern und Netzwerken weltweit verfügbar gemacht werden
- Optionen zum Austausch forensischer Daten und Dateibeurteilungen über eine Plattform
- Integration von Bedrohungsinformationen mit vorhandenen Sicherheitstools

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

Reporting

Der Nutzen von Sicherheitslösungen mit Reporting-Funktionen steht und fällt mit der Umsetzbarkeit der gelieferten Ergebnisse. Insbesondere müssen die Reporting-Funktionen einer Cloud Sandbox folgende Voraussetzungen 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 organisationsrelevante 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:

Schützt die Lösung alle User und Geräte unabhängig vom jeweiligen Standort?

Möglicherweise greifen User von unterwegs über Privatgeräte bzw. ungesicherte Netzwerke auf Unternehmensressourcen zu. Deswegen muss unbedingt Schutz für sämtliche Geräte gewährleistet sein, die sie im Zuge ihrer Arbeit benötigen.[5]

Funktioniert die Lösung im Inline- oder im TAP-Modus (Test Access Point)?

Inline-Lösungen können Bedrohungen nach der Erkennung unmittelbar blockieren, ohne dass neue Regeln über Drittanbieter-Geräte wie Firewalls erstellt werden müssen.

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

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

Erfüllt die Lösung die geltenden gesetzlichen und behördlichen Vorschriften, einschließlich Zero-Trust-Verpflichtungen?

Unter Umständen gelten strenge Vorschriften für den Einsatz von Sandbox-Lösungen bzw. für die Aufbewahrung von Daten und es gibt andere datenschutzrechtliche Vorschriften. Eine Lösung, die Daten ausschließlich im Arbeitsspeicher verarbeitet und Informationen, die Rückschlüsse auf die Identität einer Person zulassen, bei der Analyse entfernt, unterstützt Organisationen bei der Erfüllung dieser Auflagen. Außerdem sollte darauf geachtet werden, ob die ausgewählte Lösung den Zero-Trust-Grundsätzen gemäß NIST 800-207 entspricht.

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.

Lässt sich die Lösung mit anderen Sandbox-Lösungen (EDR-Sandboxing bzw. von Anbietern bereitgestellte Lösungen) kombinieren?

Im Rahmen einer mehrschichtigen Defense-in-Depth-Strategie ist möglicherweise eine Kombination aus verschiedenen Lösungen bzw. Schutzschichten erforderlich, um die Kill Chain effektiv zu unterbrechen und schwerwiegende Schäden zu verhindern. Voraussetzung dafür ist ein harmonisches Zusammenwirken sämtlicher Sicherheitslösungen zum Schutz von Endgeräten und Netzwerk sowie Kontrollmechanismen zur Richtliniendurchsetzung, sodass auch bei Ausfall einer Schicht ein ausreichendes Schutzniveau gewährleistet ist.

5. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox mit Advanced Threat Protection

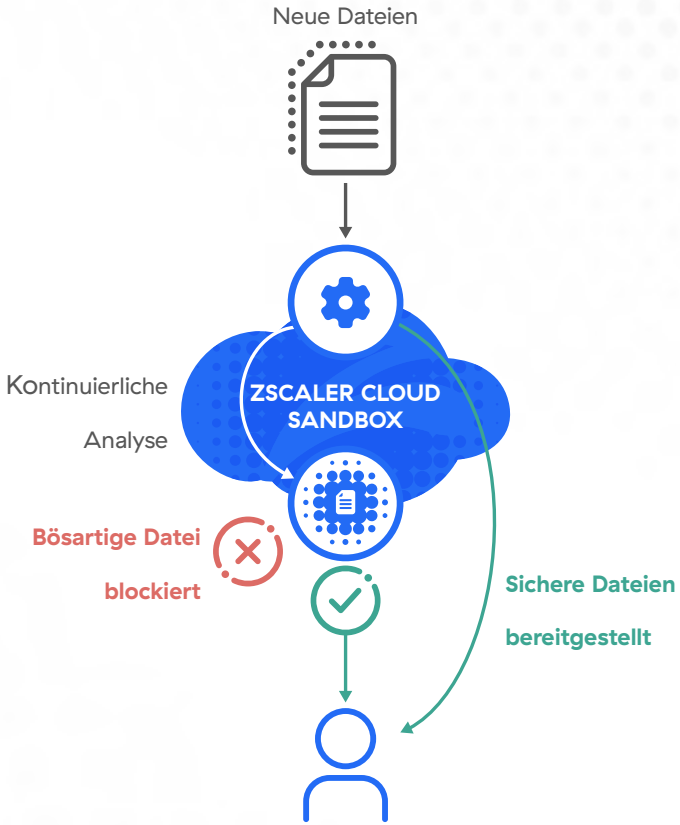
Argumente für die Umstellung auf eine echte Cloud-native Inline-Sandbox

Expandierende Angriffsflächen und Sicherheitslücken in herkömmlichen Security-Stacks setzen Organisationen 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 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 Cloud Sandbox durch gründliche und dynamische Echtzeitanalyse, dass unbekannte und potenziell schädliche Dateien als Downloads bei Usern ankommen.

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
- Sofortige 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-Studie zum wirtschaftlichen Nutzen erbrachte den Nachweis, dass die Zscaler Zero Trust Exchange eine Reduzierung der Sicherheitsappliances um 90 % ermöglichte.[6]

- 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.de/custom-product-demo**.

6. https://info.zscaler.com/resources-industry-report-esg-economic-validation-de

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. 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 die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.

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