

Zero Trust. Für optimale Ergebnisse.

Eine Zero-Trust-Architektur ist die unabdingbare Voraussetzung für sicheres Wirtschaften in der digitalen Geschäftswelt. Die erfolgreiche Implementierung ist jedoch nur der erste Schritt. Die nächste Frage lautet: Wie maximieren Sie das Potenzial Ihrer Architektur, um noch bessere Ergebnisse zu erzielen?

26%

Der weltweit befragten Vollzeitbeschäftigten haben die Möglichkeit zur Hybridarbeit¹

61%

Der Unternehmen verfügen bereits über eine definierte Zero-Trust-Sicherheitsinitiative²

Die Vorteile von Zero Trust.

Sicherheit ist das Fundament für Inklusion, Vernetzung und selbstständiges Arbeiten.

Für die Netzwerk- und Servicedesk-Beauftragten, die die Umstellung auf Hybridarbeit bewältigen, wird es zunehmend schwieriger, Probleme zu beheben, die die Anwendererfahrung und Produktivität der User beeinträchtigen. Zur Bewältigung dieser Herausforderungen nutzen Unternehmen die öffentliche Cloud, SaaS-Apps und hybride Infrastrukturen. Das Skalieren einer Architektur für ein komplex strukturiertes Großunternehmen braucht jedoch Zeit, und die Beschleunigung der Transformation führt zu Leistungseinbußen.

30%

Höhere Kosten für die Bearbeitung dieser Tickets³

35%

Mehr Support-Tickets⁴

LÖSUNG

Mithilfe von KI kann die Zero-Trust-Transformation beschleunigt werden.

Zero Trust bietet Unternehmen unglaubliche Vorteile, die durch den Einsatz maschinellen Lernens noch vervielfacht werden können.

Weichen Einfluss hat maschinelles Lernen (ML) auf Sicherheit und Produktivität? Als Unterkategorie der KI kann ML bestimmte Aufgaben ohne ausdrückliche Programmierung ausführen. ML-Algorithmen sind darauf ausgelegt, riesige Datenmengen zu analysieren und aus den gewonnenen Erkenntnissen zu lernen, um fundierte Entscheidungen zu treffen. Durch laufende Fütterung mit neuen Daten können sie ihre Erkenntnisse weiter präzisieren und so die Entscheidungsfindung optimieren.

Die leistungsstärksten Lösungen sind einfach zu bedienen, können auf die spezifischen Anforderungen bestimmter Unternehmen zugeschnitten werden und beschleunigen oder rationalisieren zeitaufwendige manuelle Prozesse. Um die Erkenntnisse aus ML optimal zu nutzen, ist jedoch eine effektive Zusammenarbeit zwischen Mensch und Maschine erforderlich.



Mehr Agilität



Erhöhte Produktivität



Reduzierte Komplexität



Kostensenkung

Profitieren Sie von maschinellen Lernalgorithmen, die mit Daten aus der größten Sicherheits-Cloud der Welt trainiert wurden.

400b

Transaktionen pro Tag abgesichert

20x

Volumen der täglichen Google-Suchanfragen

150

Cloud-Rechenzentren auf sechs Kontinenten

ERGEBNIS

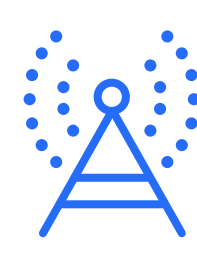
Die Vorteile des maschinellen Lernens unter menschlicher Leitung.

Die Kombination menschlichen Fachwissens mit maschinellem Lernen liefert Unternehmen hochwertige Ergebnisse.

Unternehmen, die einen Zero-Trust-Ansatz verfolgen, können ML nutzen, um die Ursachenanalyse zu automatisieren und den Prozess von Stunden, Tagen oder sogar Wochen auf nur wenige Minuten zu beschleunigen.

Zscaler Digital Experience™ (ZDX) wird als Modul der Zscaler Zero Trust Exchange™-Plattform bereitgestellt und nutzt ML, um Netzwerkverantwortliche und Servicedesk-Mitarbeiter dabei zu unterstützen, Leistungsprobleme in der gesamten IT-Umgebung zu isolieren und zu beheben. IT-Teams können Probleme proaktiv lösen, bevor die Enduser sie überhaupt bemerken.

ZDX sucht im gesamten Unternehmen proaktiv nach Problemen.



Konnektivitätsprobleme und instabile Verbindungen



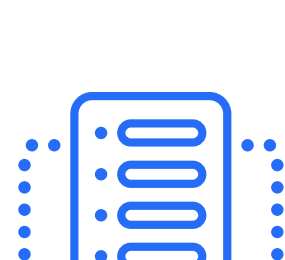
VPN-Latenz



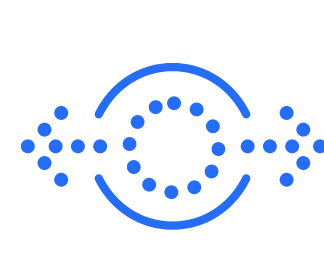
Egress-Latenz



Problem in einer bestimmten Region



Langsame Internetverbindung



Traffic-Backhauling

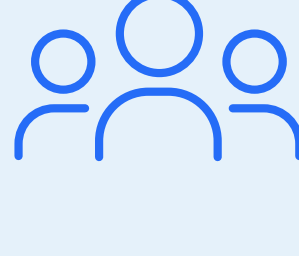


Anwendungsausfälle

Steigern Sie die IT Ops-Produktivität mit blitzschnellen Berechnungen.



Schnellere Diagnose und Problembewegung



Erhöhte Mitarbeiterproduktivität



Gesteigerte Performance des IT-Ökosystems



Kosteneinsparungen für das Unternehmen

Nutzen Sie KI zur Bewältigung von Herausforderungen

Entdecken Sie, wie Zscaler KI nutzt, um die Grundursachen von Problemen zu identifizieren.

Erfahren Sie, wie ein KI-gestützter Erkenntnisansatz menschlichen Einfallsreichtum mit maschineller Intelligenz kombiniert, um hochwertige Ergebnisse zu erzielen.

Verbessern Sie die User Experience mit weniger Ticket-Eskalationen.

E-BOOK HERUNTERLADEN

Quellenangaben

¹Working from Home Around the Globe: 2023 Report, EconPol, 2023.

²The State of Zero Trust Security 2023, Okta, 2023.

³Helpdesk meltdown due to absenteeism, low morale and increased workload", Computer Weekly, Februar 2021.

⁴American Opportunity Survey, Third Edition, McKinsey & Company, Dezember 2022.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt unzählige Kunden mit standortunabhängig sicheren Verbindungen zwischen Usern, Geräten und Anwendungen vor Cyberangriffen und Datenverlusten. Die in 150 Rechenzentren auf der ganzen Welt verfügbare SSE-basierte Zero Trust Exchange ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf <https://www.zscaler.com/de>. Folgen Sie uns unter @zscaler

+1 408 533 0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134, USA.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter <https://www.zscaler.com/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.

Zero Trust. Für optimale Ergebnisse.

Eine Zero-Trust-Architektur ist die unabdingbare Voraussetzung für sicheres Wirtschaften in der digitalen Geschäftswelt. Die erfolgreiche Implementierung ist jedoch nur der erste Schritt. Die nächste Frage lautet: Wie maximieren Sie das Potenzial Ihrer Architektur, um noch bessere Ergebnisse zu erzielen?

26%

Der weltweit befragten Vollzeitbeschäftigten haben die Möglichkeit zur Hybridarbeit¹

61%

Der Unternehmen verfügen bereits über eine definierte Zero-Trust-Sicherheitsinitiative²

Die Vorteile von Zero Trust.

Sicherheit ist das Fundament für Inklusion, Vernetzung und selbstständiges Arbeiten.

Für die Netzwerk- und Servicedesk-Beauftragten, die die Umstellung auf Hybridarbeit bewältigen, wird es zunehmend schwieriger, Probleme zu beheben, die die Anwendererfahrung und Produktivität der User beeinträchtigen. Zur Bewältigung dieser Herausforderungen nutzen Unternehmen die öffentliche Cloud, SaaS-ApPs und hybride Infrastrukturen. Das Skalieren einer Architektur für ein komplex strukturiertes Großunternehmen braucht jedoch Zeit, und die Beschleunigung der Transformation führt zu Leistungseinbußen.

30%

Höhere Kosten für die Bearbeitung dieser Tickets³

35%

Mehr Support-Tickets⁴

LÖSUNG

Mithilfe von KI kann die Zero-Trust-Transformation beschleunigt werden.

Zero Trust bietet dem Unternehmen unglaubliche Vorteile, die durch den Einsatz maschinellen Lernens noch vervielfacht werden können.

Welchen Einfluss hat maschinelles Lernen (ML) auf Sicherheit und Produktivität? Als Unterkategorie der KI kann ML bestimmte Aufgaben ohne ausdrückliche Programmierung ausführen. ML-Algorithmen sind darauf ausgelegt, riesige Datenmengen zu analysieren und aus den gewonnenen Erkenntnissen zu lernen, um fundierte Entscheidungen zu treffen. Durch laufende Fütterung mit neuen Daten können sie ihre Erkenntnisse weiter präzisieren und so die Entscheidungsfindung optimieren.

Die leistungsstärksten Lösungen sind einfach zu bedienen, können auf die spezifischen Anforderungen bestimmter Unternehmen zugeschnitten werden und beschleunigen oder rationalisieren zeitaufwendige manuelle Prozesse. Um die Erkenntnisse aus ML optimal zu nutzen, ist jedoch eine effektive Zusammenarbeit zwischen Mensch und Maschine erforderlich.



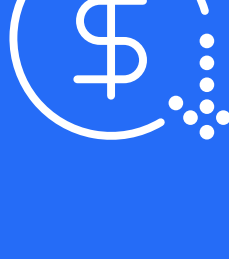
Mehr Agilität



Erhöhte Produktivität



Reduzierte Komplexität



Kostensenkung

Profitieren Sie von maschinellen Lernalgorithmen, die mit Daten aus der größten Sicherheits-Cloud der Welt trainiert wurden.

400b

Transaktionen pro Tag abgesichert

20x

Volumen der täglichen Google-Suchanfragen

150

Cloud-Rechenzentren auf sechs Kontinenten

ERGEBNIS

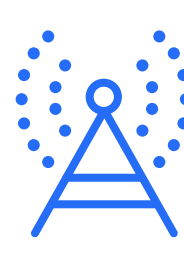
Die Vorteile des maschinellen Lernens unter menschlicher Leitung.

Die Kombination menschlichen Fachwissens mit maschinellem Lernen liefert Unternehmen hochwertige Ergebnisse.

Unternehmen, die einen Zero-Trust-Ansatz verfolgen, können ML nutzen, um die Ursachenanalyse zu automatisieren und den Prozess von Stunden, Tagen oder sogar Wochen auf nur wenige Minuten zu beschleunigen.

Zscaler Digital Experience™ (ZDX) wird als Modul der Zscaler Zero Trust Exchange™-Plattform bereitgestellt und nutzt ML, um Netzwerkverantwortliche und Servicedesk-Mitarbeiter dabei zu unterstützen, Leistungsprobleme in der gesamten IT-Umgebung zu isolieren und zu beheben. IT-Teams können Probleme proaktiv lösen, bevor die Enduser sie überhaupt bemerken.

ZDX sucht im gesamten Unternehmen proaktiv nach Problemen.



Konnektivitätsprobleme und instabile Verbindungen



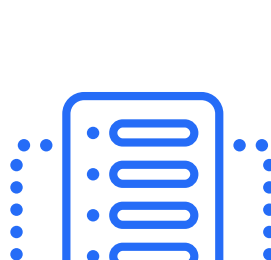
VPN-Latenz



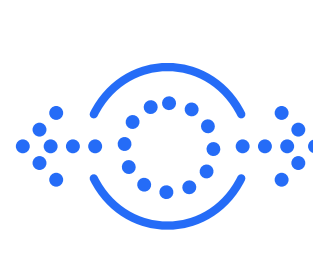
Egress-Latenz



Problem in einer bestimmten Region



Langsame Internetverbindung



Traffic-Backhauling



Anwendungsausfälle

Steigern Sie die IT Ops-Produktivität mit blitzschnellen Berechnungen.



Schnellere Diagnose und Problembehebung



Erhöhte Mitarbeiterproduktivität



Gesteigerte Performance des IT-Ökosystems



Kosteneinsparungen für das Unternehmen

Wie kann Ihr Unternehmen dies erreichen?

Ermitteln Sie mit der fachkundigen Anleitung von Zscaler den aktuellen Stand Ihrer Zero-Trust-Transformation.

Vom Verständnis von Zero Trust bis zur Anwendung von ML und darüber hinaus zeigt Ihnen den Zero-Trust-Blueprint die richtigen nächsten Schritte.

Erstellen Sie noch heute Ihren Zero Trust Blueprint.

BLUEPRINT ERSTELLEN