ivanti

Cybersecurity
INSIDERS

2021 Zero Trust Lagebericht Übersetzungen

ivanti.com

Überblick

Die Einführung von Zero Trust Security gewinnt an Dynamik. Eine Mehrheit der Organisationen plant, Zero Trust-Funktionalitäten zu implementieren, um das wachsende Cyber-Risiko zu mindern - insbesondere im Zuge der massiven Verlagerung hin zur Remote-Arbeit. Mit seinem Prinzip der Benutzer- und Geräteüberprüfung vor der Gewährung eines bedingten Zugriffs mit den geringstmöglichen Privilegien, verspricht Zero Trust eine deutlich verbesserte Benutzerfreundlichkeit, Datenschutz und Governance.

Der Zero Trust Report 2021 zeigt, wie Organisationen Zero Trust-Sicherheit implementieren, einschließlich der wichtigsten Treiber, Trends, Technologien, Investitionen und Vorteile.and benefits.

Um diese Informationen zu erhalten,haben wir Cyber Security-Fachleute befragt, die von Führungskräften bis hin zu IT-Security-Experten reichen und einen ausgewogenen Querschnitt von Organisationen unterschiedlicher Größe und aus verschiedenen Branchen repräsentieren.

Zu den wichtigsten Ergebnissen gehören:

- Vertrauen, das durch die Verifizierung von Entitäten, einschließlich Nutzern, Geräten und Infrastrukturkomponenten erworben wird (64 %), führt die Liste der Kernkomponenten von Zero Trust an. Es folgen die Bereiche Datenschutz (63 %) und kontinuierliche Authentifizierung/ Autorisierung (61 %);

- Die Bestimmung der Zugriffsrechte für alle Benutzer kann eine schwierige Aufgabe sein, um sicherzustellen, dass die Anwender auf die entsprechenden Zugriffsebenen beschränkt sind. Mehr als drei Viertel der Unternehmen (88 %) räumen auf die Frage nach ihrer derzeitigen Sicherheit ein, dass Benutzer möglicherweise über mehr Zugriffsrechte verfügen als erforderlich;

- Auf die Frage nach ihren aktuellen Security-Prioritäten nannten die Experten am häufigsten die Verbesserung von IAM (68 %), gefolgt von Data Loss Prevention (56 %) und Secure Application Access (46 %).

Many thanks to Ivanti for supporting this important research project.

We hope you'll find this report informative and helpful as you continue your efforts in protecting your IT environments.

Thank you,

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

Zero Trust-Grundsätze

Wir haben die Unternehmen gefragt, welche Aspekte von Zero Trust sie am meisten überzeugen. Vertrauen, das durch die Verifizierung von Entitäten, einschließlich Nutzern, Geräten und Infrastrukturkomponenten, erworben wird (64%), führt die Liste der Kernkomponenten von Zero Trust an. Es folgen die Bereiche Datenschutz (63%) und kontinuierliche Authentifizierung/ Berechtigung (61%).

Welche Zero Trust-Grundsätze sind für Sie und Ihr Unternehmen am überzeugendsten?[1]

64%

Vertrauen durch Verifizierung der Entität
(z. B. Nutzer, Gerät, Infrastruktur)

63%

Datenschutz
(z.B. sichere Verbindung)

61%

kontinuierliche Authentifizierung /Berechtigung

Transparenz und Audit für End-to-End Access

Erleichterung des Zugangs mit minimalen Rechten

Zentralisierte, granulare Access Policy

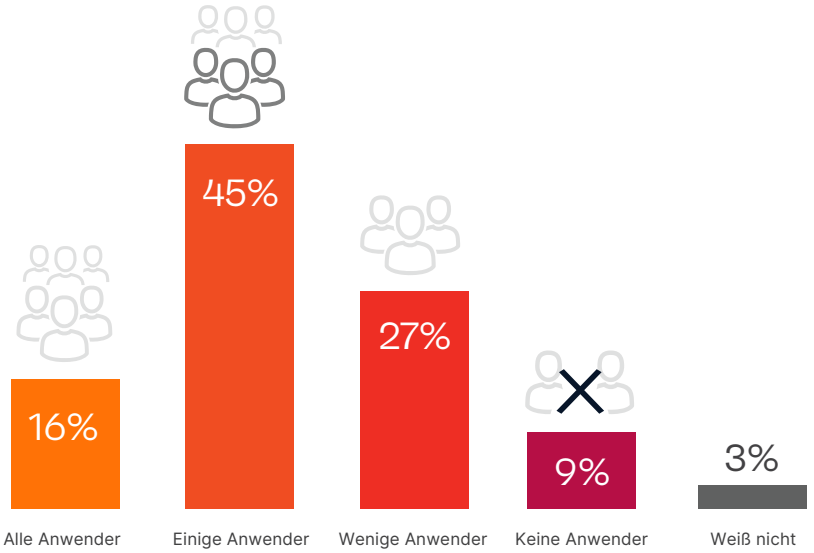
Keine Unterscheidung zwischen internem und externem Netz

Übermäßige Zugangsberechtigungen

Die Ermittlung der aktuellen Zugriffsrechte für alle Benutzer kann eine schwierige Aufgabe sein, um sicherzustellen, dass die Anwender auf die entsprechenden Zugriffsebenen beschränkt sind. Mehr als drei Viertel der Unternehmen (88 %) räumen ein, dass Benutzer möglicherweise über mehr Zugriffsrechte verfügen als erforderlich.

Inwieweit sind Sie der Meinung, dass Anwender in Ihrem Unternehmen Zugriffsrechte haben, die über das hinausgehen, was sie benötigen?

88% räumten ein, dass die Nutzer möglicherweise Zugriffsrechte haben, die über das hinausgehen, was sie benötigen.



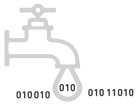
Security-Prioritäten

Auf die Frage nach ihren aktuellen Prioritäten nannten Cyber Security-Experten am häufigsten die Verbesserung von IAM (68%), gefolgt von der Data Loss Prevention (56%) und Secure Application Access (46%).

Welche sind die aktuellen Security-Prioritäten Ihres Unternehmens?[2]

68%

Verbesserung des Identity and Access Managements (IAM)

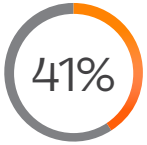


56%

Data Loss Prevention (DLP)

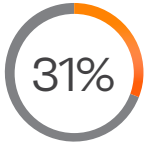
46%

Gewährleistung eines sicheren Zugangs zu Anwendungen, die bei Cloud-Anbietern gehostet werden
(z. B. Microsoft, Amazon, Google)



Einführung von Endpoint Mobile Management (EMM)/BYOD
(z.B. Benutzer, Geräte)

Durchführung einer tiefgehenden SSL-Prüfung
(z.B. sichere Sitzungsentschlüsselung für Malware -Scans und Web-/E-Mail-Filterung)



Einfachere Bereitstellung eines sicheren Zugangs
(z.B. Benutzerfreundlichkeit, Verwaltung)

Erweiterung oder Ersatz vorhandener Remote Access Tools
(z.B. VDI, VPN, RDP)

Prioritäten für Identity Access und Zero Trust

Wir haben Unternehmen gefragt, in welche Identity Access- und Zero Trust-Security Controls sie investieren. Aus Investitionssicht liegt die Priorität auf der Multi-Faktor-Authentifizierung (58%), gefolgt vom Identity Management sowie Governance (48%) und Single-Sign-On (45%).

Welche der folgenden Identity Access-/Zero-Trust-Controls haben in Ihrem Unternehmen in den nächsten 12 Monaten Vorrang bei Investitionen?[3]

58%

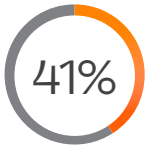
Multi-Faktor-Authentifizierung (MFA)

48%

Identity Management und Governance

45%

Single Sign-On (SSO)



Privileged Access Management (PAM), Mikrosegmentierung

Virtuelle Private Netzwerke (VPN)

Mikrosegmen-tierung

Network Access Control – NAC, Web Application Firewall (WAF)

Secure Access-Prioritäten

Wenn wir die Prioritäten für den sicheren Zugang genauer betrachten, stellen Unternehmen erneut die Multi-Faktor-Authentifizierung und das Privileged Account Management in den Vordergrund. (69%). Es folgen die Erkennung und Reaktion anormaler Aktivitäten (58%) sowie der sichere Zugang von persönlichen, nicht verwalteten Geräten (55%).

Was sind die Secure Access-Prioritäten Ihrer Organisation in den nächsten ein bis zwei Jahren?

69%

Multi-Faktor-Authentifizierung/Privileged Account Management

58%

Erkennung und Reaktion auf anomale Aktivitäten

55%

Sicherer Zugang von persönlichen, nicht verwalteten Geräten

Neubewertung der bestehenden Sicherheitsinfrastruktur und Überlegungen hin zum software-defined Access

Bessere Transparenz und Sicherheitsmetriken für Führungskräfte

Mikrosegmen-tierung

Secure Access-Herausforderungen

Die größte Sorge bei der Sicherung des Zugriffs auf Anwendungen und Ressourcen ist der überprivilegierte Zugriff (60%), gefolgt von der Bereitstellung eines sicheren Zugriffs für Partner (50%) – beide Herausforderungen werden von Zero Trust direkt angegangen.

Welches sind die größten Herausforderungen für Ihre Organisation, wenn es darum geht, den Zugriff auf Anwendungen und Ressourcen zu sichern?

60%

Überprivilegierter Mitarbeiterzugang

50%

Partner greifen unsicher auf Anwendungen und Ressourcen zu

47%

Cyber-Angriffe
(z.B. Denial of Service, Cross-Site Scripting, Man-in-the-Middle, Phishing)

Schatten-IT

Manuelle Prozesse sind komplex und verlangsamen die Fähigkeit, schnell zu reagieren

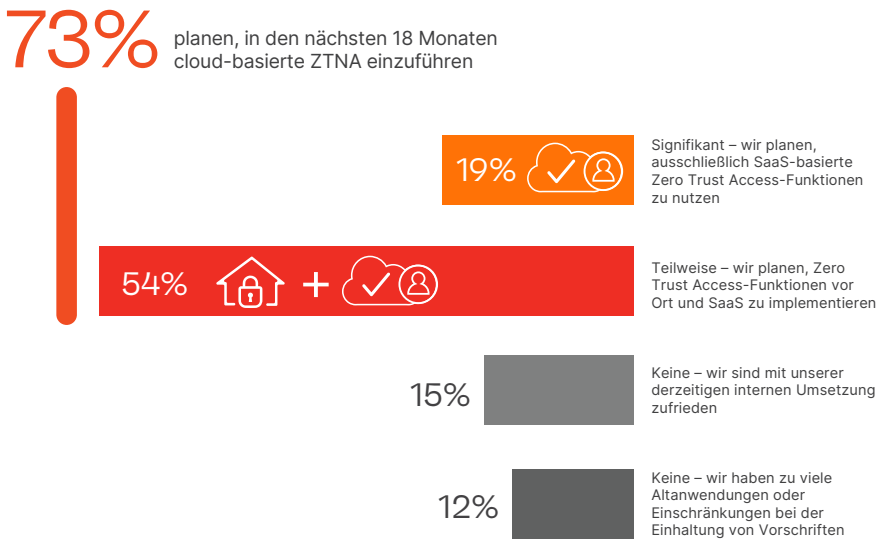
Anfällige, mit Jailbreaks versehene oder verlorene mobile Geräte, die auf Ressourcen zugreifen

Gefährdete Geräte, die auf Netzressourcen zugreifen
(unbekannte, unzulässige, nicht-sicherheitskonforme Endpunkte)

Zero Trust SAAS

Die Sicherheit verlagert sich in die Cloud, und ZTNA ist da keine Ausnahme. Fast drei Viertel der Befragten planen, in den nächsten 18 Monaten eine cloud-basierte ZTNA-Lösung einzuführen.

Inwieweit planen Sie und Ihr Unternehmen in den nächsten 18 Monaten, Zero Trust Access-Funktionen auf SaaS umzustellen?



Zugang zu privaten Apps

Wir haben Organisationen nach ihren größten Herausforderungen bei der Sicherung privater Anwendungen gefragt. Für mehr als die Hälfte der Befragten ist der sichere Zugriff auf Anwendungen, die in public Cloud-Umgebungen bereitgestellt werden, derzeit das größte Problem (54%).

Wenn es um die Sicherung des Zugriffs auf private Anwendungen geht, was ist für Sie derzeit die größte Herausforderung?

54% Zugang zu Anwendungen in der public Cloud

29% Zugang zu Anwendungen in meinem Rechenzentrum

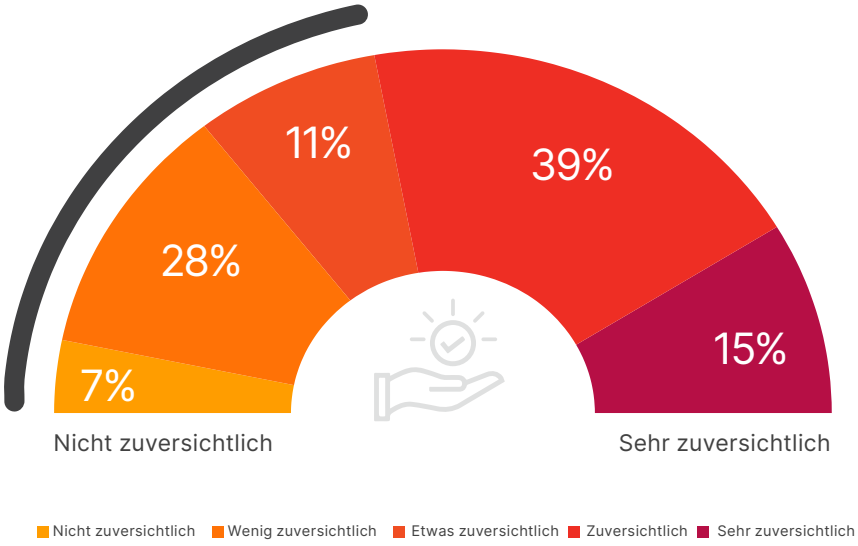
17% Zugang zu Anwendungen in meiner Firmenzentrale

Vertrauen in Zero Trust

Auf die Frage nach ihrem Vertrauen in die Fähigkeit, Zero Trust anzuwenden, zeigt sich, dass fast die Hälfte der IT-Security-Teams keine Zuversicht hat (46%).

Wie zuversichtlich sind Sie, dass Sie in Ihrer Secure Access-Architektur ein vollständiges Zero Trust-Modell anwenden können?

46% der IT-Security-Teams haben kein Vertrauen in ihre Fähigkeit, Zero Trust zu gewährleisten



Zugang zu Anwendungen in der Public Cloud

Herkömmliche Remote Access-Lösungen werden den Anforderungen der heutigen dynamischen und verteilten Cloud-Umgebungen nicht mehr gerecht. Auf die Frage nach den Szenarien, auf die Cyber Security-Experten bei der Bereitstellung eines sicheren Zugriffs stoßen, ist der am häufigsten genannte Workaround das „Hairpinning" von Remote- und mobilen Usern durch Rechenzentren, um auf public App-Clouds zuzugreifen (47%). Besorgniserregende 37% müssen Cloud-Anwendungen öffentlich zugänglich machen, um Remote- und mobile Nutzern den Zugang zu ermöglichen, was ein erhebliches Risiko darstellt.

Welche der folgenden Szenarien sind Ihnen bei der Bereitstellung eines sicheren Zugriffs auf public Cloud-Anwendungen für Remote- oder mobile User schon begegnet?

47%

Ich bin gezwungen, Remote-User durch mein(e) Rechenzentrum/ zentren zu leiten, um auf Anwendungen in der public Cloud zuzugreifen

37%

Ich muss meine privaten Anwendungen in der public Cloud öffentlich zugänglich machen, um den Zugang zu ermöglichen

35%

Ich kann meine bevorzugte Remote-VPN-Anwend-ung nicht in public Cloud-Umgebungen einsetzen

Zero Trust-Treiber

Was motiviert Organisationen dazu, den Zero Trust-Ansatz einzuführen oder auszubauen? Die Datensicherheit steht mit 82% an erster Stelle, gefolgt von der Verhinderung von Sicherheitsverletzungen (68%) und der Reduzierung von Bedrohungen für Endgeräte (53%).

Was sind die wichtigsten Faktoren, die Ihr Unternehmen dazu veranlassen, Identity Access/ Zero Trust einzuführen/ auszubauen?[4]

82%

Security/Datenschutz

68%

Prävention von Sicherheitsverletzungen

53%

Verringerung der Cyber-Bedrohungen für Endgeräte und IoT

Reduzierung von Insider-Bedrohungen

Compliance (z. B. HIPAA, DSGVO, PCI DSS)

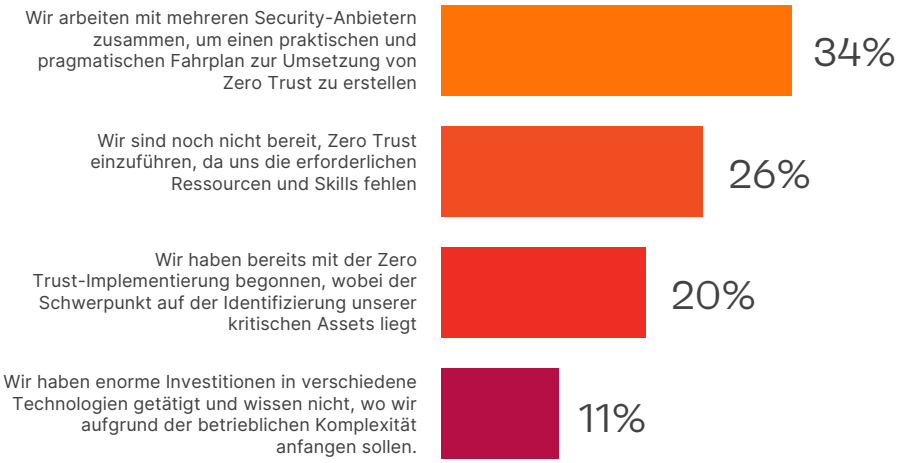
Adressierung von hybriden IT-Sicherheitsprobleme

Operative Effizienz

Implementierung von Zero Trust

Zero Trust gewinnt schnell an Bedeutung. Die Organisationen gehen bei der Einführung dieser Technologie unterschiedliche Wege. Der am häufigsten gewählte Ansatz ist die Zusammenarbeit mit mehreren Anbietern, um einen praktischen und pragmatischen Fahrplan für die Implementierung von Zero Trust zu erstellen (34%). Der Mangel an Ressourcen und den erforderlichen Skills (26%) ist jedoch nach wie vor ein wesentliches Hindernis auf dem Weg zu Zero Trust.

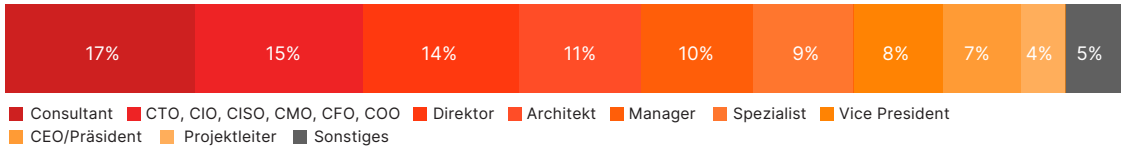
Wenn die Implementierung von Zero Trust ein schrittweiser Prozess ist, wie planen Sie die Einführung von Zero Trust in Ihrer erweiterten Umgebung?[5]



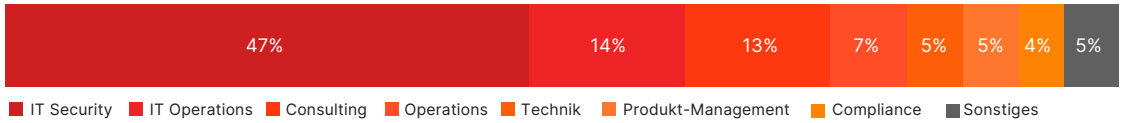
Methodik und Demografie

Dieser Bericht basiert auf den Ergebnissen einer umfassenden Online-Umfrage unter 443 IT- und Cyber Security-Experten in den USA, die im Juli 2021 durchgeführt wurde, um die neuesten Trends, Herausforderungen, Lücken und Lösungspräferenzen im Zusammenhang mit Zero Trust Security zu ermitteln. Die Befragten reichen von technischen Führungskräften bis hin zu IT-Security-Profis und repräsentieren einen ausgewogenen Querschnitt von Unternehmen unterschiedlicher Größe und verschiedener Branchen.

Karriere-Level



Abteilung



Unternehmensgröße

Branche

ivanti.com
1 800 982 2130
sales@ivanti.com

ivanti

Ivanti macht den Everywhere Workplace möglich. Im Everywhere Workplace verwenden Mitarbeiter eine Vielzahl von Geräten, um über verschiedene Netzwerke auf IT-Anwendungen und Daten zuzugreifen und von überall aus produktiv zu arbeiten.

Die Automatisierungsplattform Ivanti Neurons verbindet Unified Endpoint Management, Zero Trust Security und Enterprise Service Management und bietet so eine einheitliche IT-Plattform.

Mehr als 40.000 Kunden, darunter 78 der Fortune 100, haben sich für Ivanti entschieden, um ihre IT-Assets von der Cloud bis zum Edge zu erkennen, zu verwalten, zu sichern und zu warten und ihren Mitarbeitern ein hervorragendes Endbenutzererlebnis zu bieten, egal wo und wie sie arbeiten.

Für weitere Informationen besuchen Sie ivanti.com und folgen Sie @GoIvanti.

1 Ressourcen-Trennung 40% | Sonstige 2%

2 Ergänzung von Endpoint Detection and Response (EDR) 28% | Verbesserung der SD-WAN-Sicherheitsfunktionen 27% | Verbesserung der Schwachstellen-Behebung (z. B. Schwachstellen-Management, Patch-Management) 5% | Besserer Schutz vor mobilen Bedrohungen (Abwehr mobiler Bedrohungen/ Anti-Phishing) 2% | Keine 2% | Sonstige 4%

3 Web Application Firewall (WAF) 35% | Enterprise Mobile Management (MDM) 31% | Cloud Access Security Broker (CASB) 30% | Identitätsanalyse 27% | Software Defined Perimeter (SDP) 26% | Enterprise Directory Services 17% | Vollständige Kontrolle über den Zero Trust-Netzwerkzugang 12% | Schwachstellen-Management/ Patch-Management 9% | Unsichtbarkeit von Netzwerkgeräten für Bedrohungen 7% | Anti-Phishing 7% | Abwehr mobiler Bedrohungen 5% | Sonstiges 2%

4 Interne Compliance 28% | Reaktion auf Audit oder Sicherheitsvorfall 28% | Sonstige 5%

5 Sonstige 9%