ivanti

Cybersecurity
INSIDERS

Zero-Trust-Fortschrittsbericht 2023

ivanti.com

Überblick

Zero Trust, das auf der grundlegenden Prämisse „Niemals vertrauen, immer verifizieren“ aufbaut, wird zu einem Eckpfeiler der aktuellen Cybersicherheitspraxis.

Der Zero-Trust-Fortschrittsbericht 2023 basiert auf einer Umfrage unter 431 IT- und Cybersicherheitsfachleuten und bietet eine umfassende Analyse der steigenden Akzeptanz, der zentralen Herausforderungen und der effektiven Strategien im Zusammenhang mit Zero-Trust-Zugriffsmodellen in modernen Unternehmen.

Die Umfrage zeigt, dass 68 % der Befragten die Einführung eines Zero Trust-Zugriffsmodells planen oder bereits eingeleitet haben. Auf ihrem Weg zu Zero Trust konzentrieren sich die Unternehmen auf einen ganzheitlichen Sicherheitsansatz. 57 % setzen dabei auf Identitäts- und Zugriffsmanagement (IAM) und 52 % auf den sicheren Zugriff auf Cloud-Anwendungen. Zusammen mit der Ergänzung von Endpoint Detection and Response (EDR) und der Verbesserung der Beseitigung von Sicherheitslücken bestätigen diese Prioritäten die verstärkte Einführung von Zero-Trust-Sicherheitsverfahren.

Risikobehaftete Geräte, die auf Netzwerkressourcen zugreifen, wurden von 48 % der Befragten als größte Herausforderung genannt. Das zeigt, wie wichtig eine strenge Überprüfung der Geräte und eine kontinuierliche Überwachung sind. Der überprivilegierte Zugriff von Mitarbeitenden, das bei 47 % der Befragten Bedenken auslöst, zeigt die Notwendigkeit, das Prinzip der geringstmöglichen Privilegien im Rahmen von Zero Trust umzusetzen.

Investitionen in die Multi-Faktor-Authentifizierung (MFA) haben für 65 % der Befragten oberste Priorität, was deren Bedeutung im Rahmen eines Zero Trust-Systems unterstreicht. Die meisten Unternehmen (54 %) setzen zwei bis vier Produkte für Zero Trust ein, was auf einen mehrschichtigen Ansatz bei der Einführung hindeutet.

Da sich die Cybersicherheitslandschaft ständig weiterentwickelt, kommt es für Unternehmen darauf an, die Zero-Trust-Prinzipien zu beherzigen und ihre Sicherheitsvorgaben darauf abzustimmen, um Risiken wirksam zu verringern und ihre Ressourcen zu schützen.

Wir danken Ivanti für die Unterstützung dieser wichtigen Forschungsarbeit und hoffen, dass sie Ihnen als nützliche Ressource für den Schutz Ihrer IT-Umgebungen dient.

Vielen Dank,

Holger Schulze

Holger Schulze
CEO und Gründer
Cybersecurity Insiders

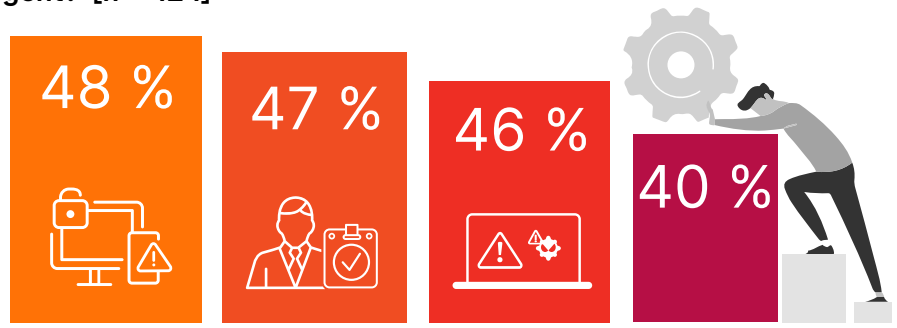
Cybersecurity INSIDERS

Herausforderungen für den sicheren Zugriff

Die größten Schwierigkeiten, mit denen Unternehmen bei der Sicherung des Zugriffs auf Anwendungen und Ressourcen zu kämpfen haben, stehen in engem Zusammenhang mit den Kernprinzipien von Zero Trust. Die seit dem letzten Jahr vorherrschende Sorge ist mit 48 % der Zugriff auf Netzwerkressourcen durch unsichere Geräte. Dieses Problem unterstreicht die Notwendigkeit einer strengen Geräteüberprüfung und fortlaufenden Überwachung nach Zero-Trust-Prinzipien, um sicherzustellen, dass nur vertrauenswürdige Geräte Zugriff auf sensible Ressourcen haben

Zu umfangreiche Privilegien für Mitarbeitende sind eine weitere große Herausforderung: 47 % der Befragten sehen hier ein Problem. Im Zusammenhang mit Zero Trust zeigt dies, wie wichtig es ist, das Prinzip des geringsten Privilegs umzusetzen, das heißt sicherzustellen, dass Benutzer nur das Minimum an Zugriffsrechten haben, das für die Erfüllung ihrer Aufgaben erforderlich ist.

Welchen Herausforderungen steht Ihr Unternehmen gegenüber, wenn es um die Sicherung des Zugriffs auf Anwendungen und Ressourcen geht?[1] [n = 424]



Gefährdete Geräte Schatten-IT, die auf Netzwerkressourcen zugreifen (unbekannte, nicht zugelassene, nicht konforme Endpunkte)

Zugriff für überprivilegierte Mitarbeiter

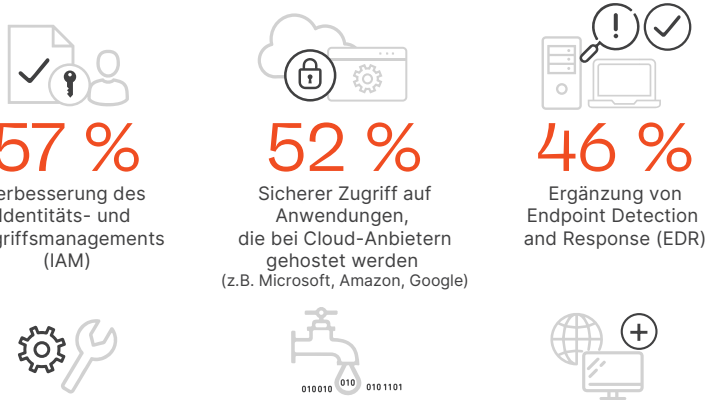
Cyber-Angriffe (z.B. Denial of Service, Cross-Site Scripting, Man-in-the-Middle, Phishing)

Schatten-IT

Die Sicherheitsprioritäten spiegeln die Zero-Trust-Schwerpunkte wider

Die gewählten Sicherheitsprioritäten lassen darauf schließen, dass die Unternehmen einen ganzheitlichen Sicherheitsansatz verfolgen, der mehrere Schutzebenen umfasst. Der starke Fokus auf IAM (57 %) und den sicheren Zugriff auf Cloud-Anwendungen (52 %) ist für die Zero-Trust-Sicherheit von großer Bedeutung, da diese Prioritäten mit den Grundsätzen übereinstimmen, Benutzer- und Geräteidentitäten zu verifizieren und den Zugriff auf Ressourcen zu kontrollieren. Darüber hinaus spiegelt die Schwerpunktsetzung auf die Ergänzung von EDR (46 %) und die Verbesserung der Behebung von Sicherheitslücken (45 %) das Zero-Trust-Prinzip der kontinuierlichen Kontrolle und schnellen Reaktion auf Sicherheitsbedrohungen wider. Insgesamt deuten diese Prioritäten darauf hin, dass Unternehmenzunehmend Zero-Trust-Sicherheitspraktiken anwenden, um ihre Cybersicherheit insgesamtzu verbessern.

Welches sind die aktuellen Sicherheitsprioritäten in Ihrem Unternehmen? [n = 421]



57 %
Verbesserung des Identitäts- und Zugriffsmanagements (IAM)

52 %
Sicherer Zugriff auf Anwendungen, die bei Cloud-Anbietern gehostet werden (z.B. Microsoft, Amazon, Google)

46 %
Ergänzung von Endpoint Detection and Response (EDR)

45 %
Verbesserung des Schwachstellenmanagements (z. B. Sicherheitslücken- und Patch-Management)

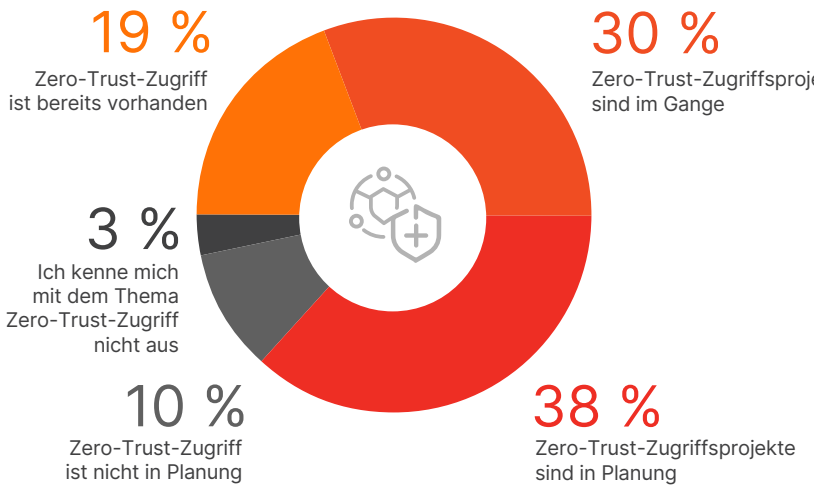
43 %
Schutz vor Datenverlust (Data Loss Prevention – DLP)

40 %
Ergänzung oder Ersatz bestehender Fernzugriffstools (z. B. VDI, VPN, RDP)

Pläne zur Einführung von Zero Trust

Jedes fünfte Unternehmen(19 %) hat Zero Trust bereits eingeführt. Ein erheblicher Teil der Befragten (38 %) plant die Umsetzung von Zero-Trust-Zugriffsprojekten, und 30 % haben bereits Projekte auf den Weg gebracht. Dies deutet darauf hin, dass die meisten der befragten Unternehmen(68 %) die Einführung eines Zero-Trust-Zugriffsmodells entweder planen oder aktiv darauf hinarbeiten.

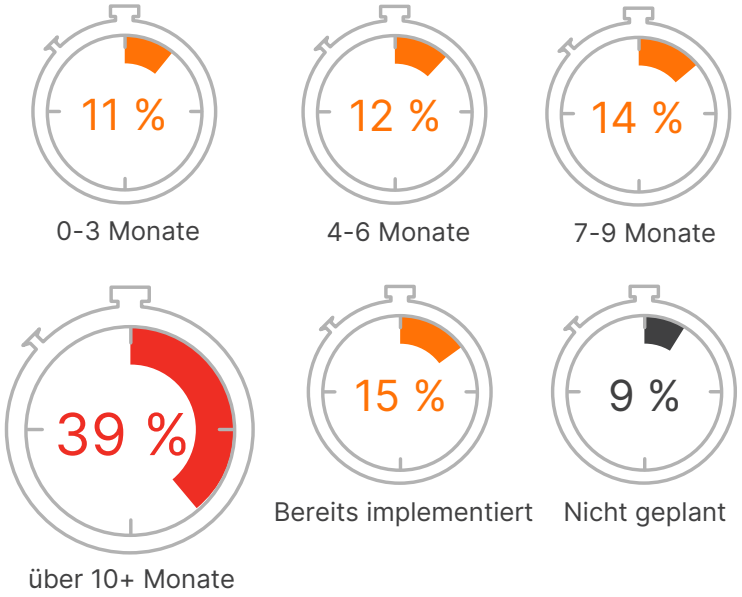
Welche Pläne haben Sie bezüglich der Einführung eines Zero-Trust-Zugriffsmodells in Ihrem Unternehmen? [n = 424]



Zeitrahmen für die Einführung von Zero Trust

Die Einführung der Zero-Trust-Sicherheit erfolgt in den Unternehmenin unterschiedlichem Tempo. Während ein beträchtlicher Teil das Framework bereits implementiert hat (15 %), planen andere, Zero Trust relativ bald einzuführen (37 % innerhalb von 9 Monaten), und eine beträchtliche Gruppe räumt ein, dass es 10 oder mehr Monate dauern könnte, bis die Zero-Trust-Sicherheit vollständig eingeführt ist (39 %).

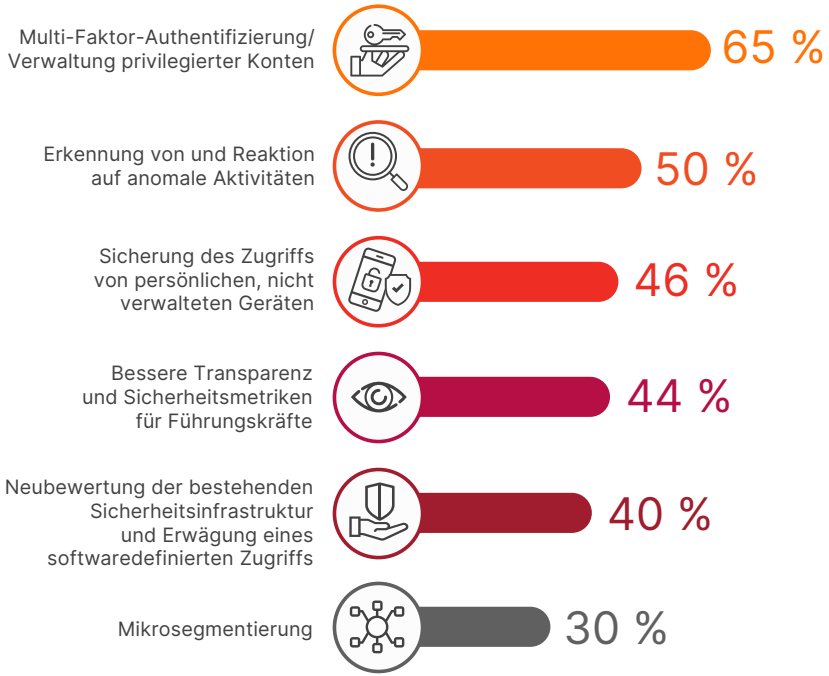
In welchem Zeitrahmen werden Sie Zero-Trust-Sicherheit aller Voraussicht nach einführen?
[n = 423]



Prioritäten für sicheren Zugriff

Die Unternehmen konzentrieren sich auf mehrere Prioritäten für den sicheren Zugriff, die eng mit den Zero-Trust-Prinzipien verbunden sind, wie z.B. die Multi-Faktor-Authentifizierung (MFA) (65 %), die Erkennung von Bedrohungen in Echtzeit (50 %) und die Sicherung des Zugriffs von persönlichen Geräten (46 %). Dies entspricht dem Zero-Trust-Prinzip „Niemals vertrauen, immer verifizieren“, das sicherstellt, dass Benutzer ordnungsgemäß authentifiziert und autorisiert sind, bevor sie Zugriff auf sensible Ressourcen erhalten.

Was sind die Prioritäten Ihres Unternehmens für sicheren Zugriff in den nächsten 1–2 Jahren? [n = 430]

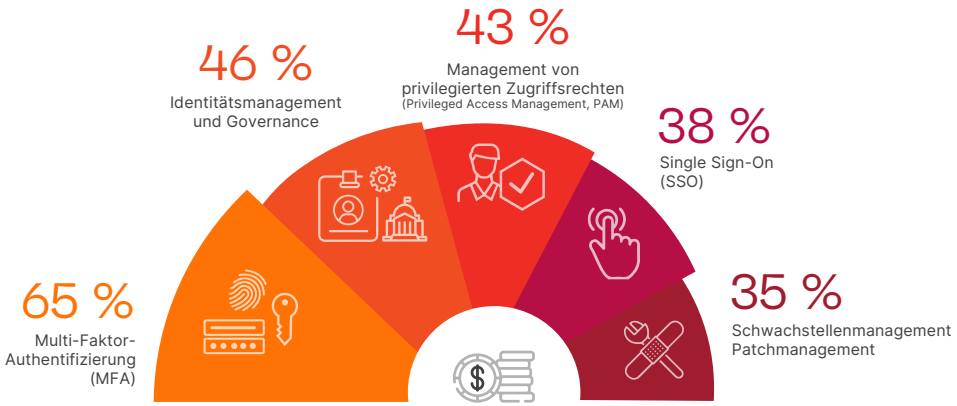


Investitionspläne

Die Investitionsschwerpunkte von Unternehmen im Bereich Identitätsprüfungen beim Zugriff und Zero-Trust-Kontrollen liegen auf der Verbesserung der Benutzerauthentifizierung, der Verwaltung von Zugriffsrechten und der Aufrechterhaltung der allgemeinen Systemsicherheit. Die Multi-Faktor-Authentifizierung (MFA) – eine Schlüsselkomponente von Zero Trust – hat oberste Priorität: 65 % der Befragten planen Investitionen in diesem Bereich.

Diese Prioritäten entsprechen den Kernprinzipien von Zero Trust, was darauf hindeutet, dass die Einführung dieses Sicherheitsrahmens in Unternehmen zunehmend in den Vordergrund rückt.

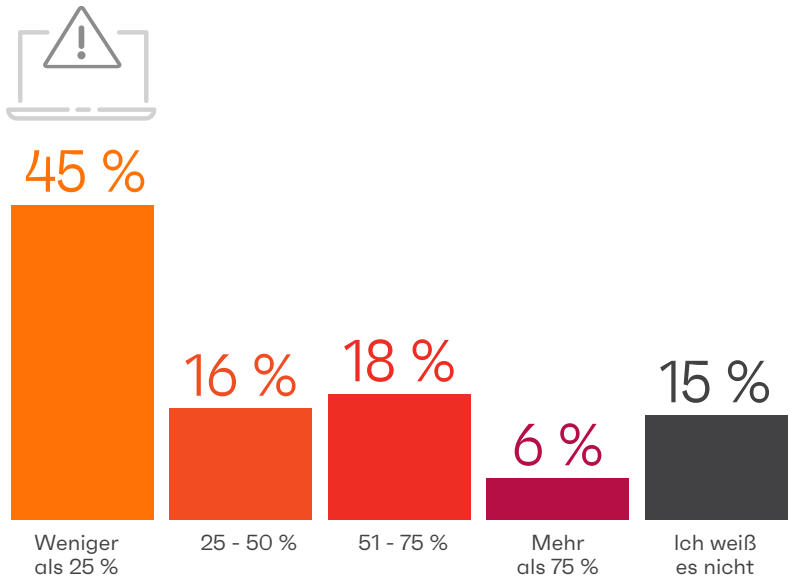
In welche der folgenden Identitätszugriffs-/Zero-Trust-Kontrollen wollen Sie in Ihrem Unternehmen in den nächsten 12 Monaten vorrangig investieren?[2] [n = 431]



Gefahren übermäßiger Zugriffsrechte

Bei fast der Hälfte der Befragten (45 %) waren weniger als 25 % der Sicherheitsvorfälle auf überprivilegierten Zugriff zurückzuführen. Dies deutet darauf hin, dass der überprivilegierte Zugriff zwar ein Problem darstellt, aber nicht die Hauptursache für Sicherheitsvorfälle in vielen Unternehmen ist. Ein Drittel der Unternehmen (34 %) erlebte 25–75 % der Vorfälle aufgrund von übermäßigen Zugriffsrechten. Diese Ergebnisse machen deutlich, wie wichtig es ist, das Zero-Trust-Prinzip des geringsten Privilegs umzusetzen, um Sicherheitsrisiken im Zusammenhang mit übermäßigen Zugriffsprivilegien zu minimieren.

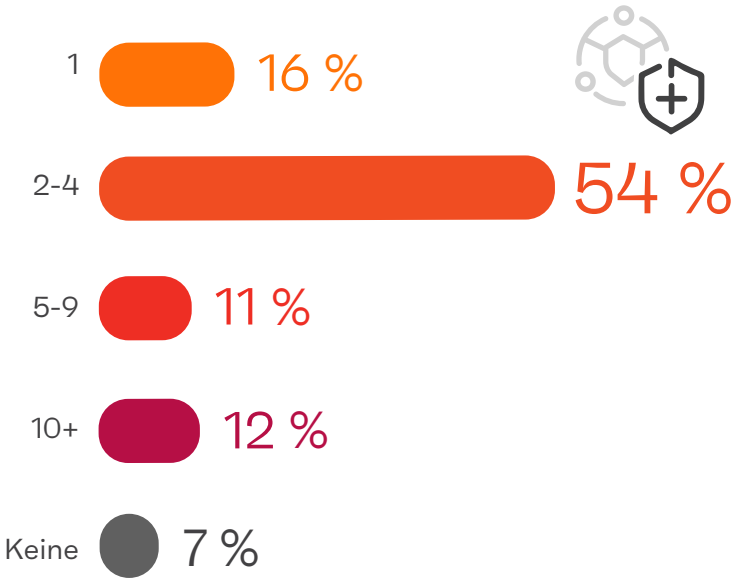
Wie viel Prozent der Sicherheitsvorfälle in Ihrem Unternehmen in den letzten 12 Monaten wurden Ihrer Meinung nach dadurch verursacht, dass Endbenutzer Zugriffsrechte besaßen, die sie nicht für ihre tägliche Arbeit benötigten? [n = 431]



Mehrschichtiger Zero-Trust-Ansatz

Die Mehrheit der Befragten (54 %) verwendet zwei bis vier Produkte für Zero Trust/sicheren Zugriff, was darauf hindeutet, dass die meisten Unternehmen einen mehrschichtigen Ansatz für die Zero-Trust-Implementierung verfolgen und mehrere Produkte verwenden, um verschiedene Aspekte des Frameworks, wie z. B. Zugriffsmanagement, Geräteüberprüfung und Netzwerksegmentierung, zu berücksichtigen. Im Zusammenhang mit Zero Trust deuten diese Ergebnisse darauf hin, dass Unternehmen bei der Umsetzung eines Programms zum sicheren Zugriff unterschiedliche Strategien und Komplexitätsgrade wählen.

Wie viele Produkte würden Sie für ein sicheres Zero-Trust-Zugriffsprogramm in Ihrem Unternehmen verwenden (oder verwenden Sie derzeit)? [n = 429]



Bewährte Zero-Trust-Verfahren

Zero Trust ist ein Sicherheitsmodell, das kein immanentes Vertrauen in das Netzwerk eines Unternehmens voraussetzt, sondern eine strenge Überprüfung aller Benutzer, Geräte und Zugriffe erzwingt. Um Zero Trust effektiv einzuführen, sollten Unternehmen diese grundlegenden bewährten Verfahren berücksichtigen:

Einrichtung einer Multi-Faktor Authentifizierung (MFA): Stärken Sie die Authentifizierung, indem Sie zusätzlich zu den üblichen Benutzernamen und Passwörtern mehrere Methoden verwenden, etwa biometrische Daten oder Token.

Wenden Sie den Grundsatz des geringsten Privilegs (Principle of Least Privilege – POLP): Gewähren Sie Benutzern nur das Minimum an Zugriffsrechten, das für die Erfüllung ihrer Aufgaben erforderlich ist, und minimieren Sie so Gefahren durch Insider und Datenmissbrauch.

Überprüfen und überwachen Sie Geräte fortlaufend: Stellen Sie sicher, dass nur vertrauenswürdige Geräte Zugriff auf sensible Ressourcen haben, indem Sie eine strenge Geräteüberprüfung und fortlaufende Überwachung durchführen.

Machen Sie den Zugriff auf Cloud-Anwendungen sicherer: Wenden Sie bei der Genehmigung des Zugriffs auf Cloud-Ressourcen Zero-Trust-Prinzipien an und nutzen Sie Sicherheitsmaßnahmen wie Verschlüsselung, Zugriffskontrolle und Protokollierung.

Überprüfen und aktualisieren Sie regelmäßig die Zugriffskontrollen: Überprüfen Sie fortlaufend die Zugriffskontrollen und passen Sie sie an, damit sie stets relevant und sicher sind und bleiben und mit den sich ändernden Rollen und Zuständigkeiten in Ihrem Unternehmen Schritt halten.

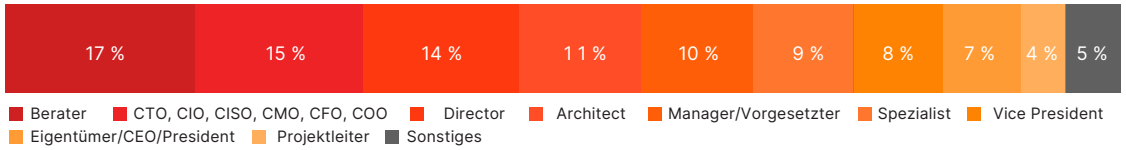
Implementieren Sie Anomalie-Erkennung und -Reaktion: Integrieren Sie moderne Erkennungs- und Reaktionstechnologien wie EndpointDetection and Response (EDR) und Extended Detection and Response (XDR), um Bedrohungen schnell zu erkennen und zu entschärfen.

Führen Sie Schulungen zur Sensibilisierung für Sicherheitsthemen durch: Schulen Sie Ihre Mitarbeitende hinsichtlich Zero-Trust-Prinzipien, sicheren Onlinepraktiken sowie der Erkennung und Meldung potenzieller Sicherheitsrisiken, um die Wahrscheinlichkeit sicherheitsrelevanter Zwischenfälle zu verringern, die auf menschliches Versagen zurückzuführen sind.

Methodik und Demografie

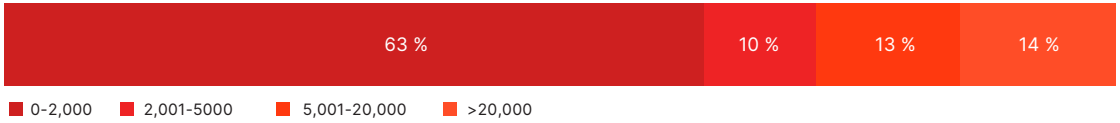
Dieser Bericht basiert auf den Ergebnissen einer umfassenden Online-Umfrage unter 431 IT- und Cybersicherheitsfachleuten in den USA, die im März 2023 durchgeführt wurde, um die neuesten Trends, Herausforderungen, Lücken und Lösungspräferenzen im Zusammenhang mit Zero-Trust-Sicherheit in Unternehmen zu ermitteln. Die Befragten reichen von technischen Führungskräften bis hin zu IT-Sicherheitsprofis und repräsentieren einen ausgewogenen Querschnitt von Unternehmen unterschiedlicher Größe und verschiedener Branchen.

Karrierestufe

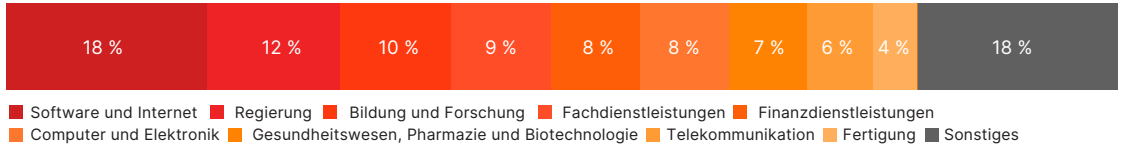


Abteilung

Unternehmensgröße



Branche



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

ivanti

Ivanti macht den EverywhereWorkplace möglich. Im EverywhereWorkplace nutzen Mitarbeiter unzählige Geräte, um über verschiedene Netzwerke auf IT-Anwendungen und Daten zuzugreifen und so von überall aus produktiv arbeiten zu können.

Die Automatisierungsplattform Ivanti Neurons verbindet die branchenführenden Lösungen des Unternehmens für Unified Endpoint Management, Zero Trust Security und Enterprise Service Management und bietet so eine einheitliche IT-Plattform, durch die sich selbstreparieren und abzusichern können, und Anwender die Möglichkeit haben, sich selbst zu helfen.

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 www.ivanti.com und folgen Sie @GoIvanti.

1 Manuelle Verfahren sind komplex und verlangsamen die Fähigkeit, schnell zu reagieren 37 % | Partner greifen ungesichert auf Apps und Ressourcen zu 33 % | Anfällige, mit Jailbreakverfahren geknackte oder verlorene Mobilgeräte greifen auf Ressourcen zu 17 %

2 Mikro-Segmentierung 34 % | Virtuelle Private Netzwerke (VPN) 33 % | Enterprise Mobile Management (EMM) 29 % Anti-Phishing 28 % | Cloud Access Security Broker (CASB) 28 % | VollständigeKontrolleüber den Zero Trust NetzwerkZugriff 27 % Web Application Firewall (WAF) 26 % | Network Access Control (NAC) 2 5% | Identity analytics 24 % | Software Defined Perimeter (SDP) 24 % | Unsichtbarkeit von Netzwerkgeräten für Bedrohungen 20 % | Data Loss Prevention (DLP) 17 % | Abwehr mobilerBedrohungen 16 % | Unternehmensverzeichnisdienste 13 % | Digital Rights Management (DRM) 9 % | Sonstige 5 %

Cybersecurity
INSIDERS

Cybersecurity Insiders ist eine Online-Community für Informationssicherheitsexperten mit mehr als 500.000 Mitgliedern, die die besten Köpfe zusammenbringt, die sich für die Förderung der Cybersicherheit und den Schutz von Unternehmen aller Branchen, Unternehmensgrößen und Sicherheitsfunktionen einsetzen.

Wir bieten Cybersecurity-Vermarktern einzigartige Marketingmöglichkeiten, um diese qualifizierte Zielgruppe zu erreichen und faktenbasierte, von Dritten validierte Thought-Leadership-Inhalte, Programme zur Nachfragegenerierung und Markensichtbarkeit auf dem Cybersecurity-Markt zu liefern.

Für weitere Informationen besuchen Sie bitte www.cybersecurity-insiders.com