# Sicherheits-Whitepaper von Verify Zero Trust

## Inhalt



## Einleitung

In diesem Dokument werden Informationen zu Zero Trust und dessen Verwendung zur Sicherung des Unternehmens beschrieben.

## Zusammenfassung

Zero Trust stellt ein Modell dar, das davon ausgeht, dass kein Benutzer, Gerät oder keine Anwendung, weder außerhalb noch innerhalb des Netzwerks, als sicher eingestuft werden kann und dass jeder Benutzer validiert werden muss, bevor er Zugriff auf Netzwerkressourcen erhält.

Dieses Konzept gewinnt bei der Virtualisierung und der schnellen Verlagerung von Ressourcen am Standort in Public, Private und Hybrid Clouds zunehmend an Bedeutung.

Der Begriff "Zero Trust" wurde 2010 von Forrester mit der Veröffentlichung des "Zero Trust Network Architecture Report" eingeführt.

Es ist wichtig zu verstehen, dass Zero Trust als Strategie auf Unternehmensebene beginnen muss, um wichtige Geschäftsinteressen und -initiativen zu schützen.


*Null-Vertrauen-Säulen*

## Was ist Zero Trust?

Zero Trust ist ein strategischer Ansatz, der verschiedene Technologien umfasst, um einen praxisnahen Schutz für die heutige Infrastruktur zu gewährleisten. Diese Sicherheitsarchitektur und Unternehmensmethodik ermöglicht eine effektive Orchestrierung der heutigen Technologien, Vorgehensweisen und Richtlinien.

Es stellt eine Weiterentwicklung unseres Sicherheitsansatzes dar und bietet einen umfassenden, interoperablen und ganzheitlichen Lösungsansatz, der die Produkte und Services mehrerer Anbieter umfasst.

Zero Trust basiert auf zahlreichen bewährten Technologien, wie Netzwerksegmentierung, Multifaktor-Authentifizierung und Netzwerkzugriffskontrolle.

## Warum ist Zero Trust wichtig?

Zero Trust schützt das Unternehmen vor nicht autorisierten Benutzern, Sicherheitsverletzungen und Cyber-Angriffen. Sie können die Identität von Benutzern und Geräten kontinuierlich überprüfen und ihnen nur die Berechtigungen gewähren, die sie für ihre Arbeit benötigen, um das Risiko eines Sicherheitsereignisses zu minimieren.

Marktuntersuchungen haben ergeben, dass das globale Volumen des Null-Trust-Sicherheitsmarktes von einem geschätzten Wert von 27 Mrd. USD im Jahr 2022 auf rund 60 Mrd. USD bis 2027/2028 ansteigen wird, bei einer jährlichen Wachstumsrate von rund 17 % zu diesem Zeitpunkt.

Motive:

- Häufigere zielbasierte Cyberangriffe
- Zunahme der behördlichen Vorschriften für Datenschutz und Informationssicherheit
- Höherer Bedarf zur Reduzierung geschäftlicher und organisatorischer Risiken
- Je mehr Services in die Cloud migriert werden, desto mehr Grenzen werden überschritten und Sicherheitsrisiken werden verstärkt durch die zentrale Datenbereitstellung.

- Die Notwendigkeit, die Identität des Benutzers während des gesamten Zugriffsprozesses und nicht nur anfangs zu bestätigen

Ein einziger Ransomware-Angriff kostet 5 Millionen US-Dollar. Cyberkriminelle diskriminieren nicht, wenn sie auf Unternehmen abzielen.

Aus aktuellen Umfragen von CIOs und CISOs geht hervor, dass Zero Trust zu den fünf obersten Prioritäten zählt. CISOs bestätigen, dass ein Wandel hin zu Remote-Arbeit, Arbeitskräftemangel und ein großer Anstieg von Cyberangriffen die Sicherung ihrer vorhandenen Systeme im Unternehmen erfordern.

## Herkömmliches und nicht vertrauenswürdiges Modell

In herkömmlichen Umgebungen wurde die Sicherheit nach dem Erstellen der Umgebung hinzugefügt. In der Regel handelt es sich um flache Netzwerke, bei denen die Abwehrmechanismen um den Netzwerk-Edge herum eingerichtet werden, um Angriffe aus dem Internet zu verhindern.

Zero Trust konzentriert sich allgemein auf die Notwendigkeit, die Systeme und Daten einer Organisation auf mehreren Ebenen mit einer Mischung aus Verschlüsselung, sicheren Computerprotokollen, dynamischer Arbeitslast sowie Authentifizierung und Autorisierung auf Datenebene zu schützen, und verlässt sich nicht nur auf eine externe Netzwerkgrenze.

Die herkömmliche perimeterorientierte Sicherheitsarchitektur ist weniger effektiv, da Workloads zunehmend aus der Cloud bereitgestellt werden und mobile Endgeräte die Norm für den Anwendungs- und Datenzugriff werden.

## Architektur-Framework ohne Vertrauen

Ein Architektur-Framework ohne Vertrauen behandelt die Einschränkung des Zugriffs auf Systeme, Anwendungen und Datenressourcen für Benutzer und Geräte, die speziell darauf zugreifen müssen und validiert wurden. Sie müssen fortlaufend anhand ihrer Identität und ihres Sicherheitsstatus authentifiziert werden, um sicherzustellen, dass jede Ressource für den Zugriff autorisiert ist.

Das Framework stellt eine Roadmap für die Migration und Bereitstellung von Zero Trust-Sicherheitskonzepten in Unternehmensumgebungen bereit und basiert auf der NIST-Sonderpublikation 800-207.

Ein effektives Architektur-Framework ohne Vertrauen koordiniert und integriert diese sieben Hauptkomponenten.

- Zero Trust Networks sind ein wichtiges Merkmal einer Zero Trust-Strategie, die sich auf die Fähigkeit bezieht, Netzwerke zu segmentieren, Netzwerkressourcen zu isolieren und die Kontrolle über die Kommunikation zwischen ihnen zu behalten. Darüber hinaus werden vertrauenswürdige Verbindungen gesichert, um den Arbeitsplatz für den Remote-Einsatz zu erweitern.
- Zero Trust Workforce umfasst Methoden zur Beschränkung und Durchsetzung des Benutzerzugriffs, darunter Technologien zur Authentifizierung von Benutzern und zur kontinuierlichen Überwachung und Steuerung ihrer Zugriffsberechtigungen. Dieser Zugriff wird durch Technologien wie DNS, Multifaktor-Authentifizierung und Netzwerkverschlüsselung

gesichert.
- Zero Trust Devices bewältigt die Notwendigkeit, alle mit dem Netzwerk verbundenen Geräte zu isolieren, zu sichern und zu verwalten, die durch die zunehmende Mobilität und das Internet of Things entstanden sind. Angreifern entsteht so eine immense Verwundbarkeit, die sie ausnutzen können.
- Zero Trust-Workloads sichern die Front-to-Back-Anwendungs-Stacks, die kritische Geschäftsprozesse ausführen. Sichert Ost-West-Datenverkehr zwischen Anwendungen, Daten und Services in einem Rechenzentrum für einen besseren Schutz kritischer Anwendungen.
- Zero Trust Data bezeichnet Methoden zur Klassifizierung und Kategorisierung von Daten, kombiniert mit Technologielösungen zur Sicherung und Verwaltung von Daten, einschließlich Datenverschlüsselung.
- Transparenz und Analysen beziehen sich auf Technologien, die Automatisierungs- und Orchestrierungsfunktionen bereitstellen und es Administratoren ermöglichen, nicht nur die Aktivitäten in ihren Umgebungen zu erkennen, sondern diese auch zu verstehen. Dazu gehört auch das Vorhandensein von Echtzeit-Bedrohungen.
- Automatisierung und Orchestrierung umfassen Tools und Technologien wie Algorithmen für maschinelles Lernen und künstliche Intelligenz, um Netzwerk- und Rechenzentrumsressourcen automatisch zu klassifizieren sowie Segmentierungs- und Sicherheitsmaßnahmen, Richtlinien und Regeln vorzuschlagen und anzuwenden, die automatisch angewendet werden. So wird der Aufwand für Sicherheitsteams reduziert und die Eindämmung von Angriffen beschleunigt.

## Keinerlei Vertrauen und Segmentierung

Jede netzwerkbasierte Ressource muss gesichert und nach dem Prinzip der geringsten Rechte segmentiert werden. Dies lässt sich am besten über ein Asset-Management-System erreichen, das Anmeldeinformationen und den Zugriff für jeden Zweck steuert.

Die Zero Trust-Segmentierung erfordert Markenschutz, eine begrenzte Angriffsfläche, verbesserte Netzwerkstabilität und eine schnelle Servicebereitstellung.

Um einen weiteren Schutz einzelner Ressourcen zu erreichen, kann eine Mikrosegmentierung verwendet werden. SGTs (Scalable Group Tags) können verwendet werden, wenn ein Tag-Wert in den Ethernet-Frame eingefügt wird, um eine Ressource eindeutig zu identifizieren. Darüber hinaus umfassen Infrastrukturgeräte intelligente Switches, Router oder Firewalls der nächsten Generation, die als Gateway-Geräte zum Schutz der einzelnen Ressourcen verwendet werden können.

## Transparenz, Analysen und Automatisierung

Es ist wichtig, dass alle Ressourcen der Organisation und alle damit verbundenen Aktivitäten vollständig transparent sind. Dies ist die Grundlage von Zero Trust.

Um dynamische Richtlinien und Vertrauensentscheidungen zu ermöglichen, ist eine fortlaufende Sammlung von Analysen erforderlich. Unser Zero Trust-Architekturansatz konzentriert sich auf die zentralen logischen Komponenten einer SDN-Strategie mit einer Policy Engine und einem Policy Administrator, um eine Kontrollebene zu bilden, um den Zugriff auf Ressourcen über Policy

Enforcement Point(s) in einer Datenebene zu beschränken.

Die Funktionen, die für eine Zero Trust-Architektur erforderlich sind, um Netzwerkkontext, Lerninhalte und Sicherheit zu erweitern und so die Mission sicher zu erfüllen:

- Präzise Mikrosegmentierung des Zugriffs auf Benutzer, Geräte, Anwendungen, Workloads und Daten
- Durchsetzung von Sicherheitsrichtlinien überall dort, wo sie funktionieren, z. B. in LANs, WANs, Rechenzentren, Clouds und am Edge.
- Umfassendes Identitätsmanagement - zur Erweiterung des Identitäts- und Zugriffsmanagements auf die Identitäten von Benutzern, Geräten, Anwendungen, Workloads und Daten, die durch einen softwaredefinierten Zugriff zu neuen Mikroperimetern werden.
- Integrierter Schutz vor Bedrohungen, der globale Threat-Intelligence und Feeds nutzt
- Vollständig automatisierte, flexible Steuerung des Netzwerks Ihres Unternehmens für einen sicheren Betrieb in der gewünschten Größe, Leistung und Zuverlässigkeit, die zur Erreichung des Ziels erforderlich sind.

## Schritte ohne Vertrauen

Der Schlüssel zu umfassender Zero Trust-Sicherheit ist die Erweiterung der Sicherheit auf die gesamte Netzwerkumgebung, ob im LAN, Rechenzentrum, Cloud-Edge oder in der Cloud. Die Einhaltung ist natürlich zwingend vorgeschrieben.

Diese Sicherheit muss vollständige Transparenz der Netzwerkumgebung Ihres Unternehmens beinhalten. Die wichtigsten Schritte für ein umfassendes Zero Trust-Zentrum:

- Identifizierung von Geräten und vertraulichen Daten Identifizierung und Klassifizierung von Geräten, vertraulichen Daten und Workloads
- Verstehen des Datenflusses sensibler Daten
- Erstellen Sie Ihre Zero Trust-Segmentierungsrichtlinie. Jede netzwerkbasierte Ressource muss nach dem Prinzip der geringsten Rechte und streng durchgesetzten, präzisen Kontrollen geschützt und entsprechend segmentiert werden, damit Benutzer nur auf die Ressourcen zugreifen können, die sie für ihre Arbeit benötigen.
- Implementieren Sie Richtlinien und Sicherheitsstatus. Dies kann mit Plattformen wie Cisco DNAC oder ISE erfolgen.
- Kontinuierliche Überwachung der Umgebung ohne Vertrauen. Implementieren Sie Sicherheitsanalysen, um Sicherheitsvorfälle in Echtzeit zu überwachen und zu analysieren und schädliche Aktivitäten schnell zu identifizieren. Überprüfen und protokollieren Sie den gesamten Datenverkehr intern und extern.

## Zuverlässiger Zugriff

Um eine umfassende Zero Trust-Sicherheit zu erreichen, müssen Unternehmen ihren Zero Trust-Ansatz auf ihre gesamte Belegschaft, ihren gesamten Arbeitsplatz und alle Workloads ausdehnen.

- Mitarbeiter ohne Vertrauen - Benutzer und Geräte müssen authentifiziert und autorisiert werden. Zugriff und Berechtigungen werden kontinuierlich überwacht und verwaltet, um Ressourcen zu schützen.

- Zero Trust Workplace - Der Zugriff muss über den gesamten Arbeitsplatz, einschließlich Cloud und Edge, gesteuert werden.
- Zero Trust Workloads: Eine präzise Zugriffskontrolle muss für alle Anwendungs-Stacks durchgesetzt werden, d. h. für Container, Hypervisoren und Mikroservices in der Cloud sowie für herkömmliche Rechenzentren.

Cisco, ein von Forrester anerkannter Zero Trust Leader, befürwortet die Implementierung von Zero Trust in Ihrem gesamten Netzwerk - sowohl vor Ort als auch in der Cloud. Sie können Ihre Cisco Netzwerkinfrastruktur nicht nur als wichtige Grundlage Ihrer Zero Trust-Architektur nutzen, sondern sich auch mit anderen wichtigen Cisco Zero Trust-Sicherheitsfunktionen vertraut machen, die Ihr Unternehmen auf dem Weg zur Zero Trust-Lösung unterstützen können.

## Cisco Secure-Portfolio

Diese können verwendet werden, um ein erfolgreiches Zero Trust Framework aufzubauen:

- Reibungsloser, sicherer Zugriff für Benutzer, Geräte und Anwendungen über **Cisco Duo**
- Flexible Cloud-Sicherheit durch **Cisco Umbrella**
- Intelligente Paketprüfung durch **Cisco Secure Firewall**
- Advanced Malware Protection über **Secure Endpoint** (ehemals AMP)
- Sicheres VPN und sicherer Remote-Zugriff über **Cisco AnyConnect**
- Ganzheitlicher Workload-Schutz durch **Cisco Tetration**
- Geschützte Netzwerksegmentierung mit der **Cisco Identity Services Engine** (ISE)
- Anwendungstransparenz und Mikrosegmentierung durch **Cisco Secure Workload**
- Integrierte Sicherheitsplattform über **Cisco SecureX**
- Unified SASE-Lösung mit As-a-Service-Abonnement über **Cisco Secure Connect**
- Fachkundige Unterstützung durch den **Cisco Zero Trust Strategy Service**
- Support und End-to-End-Services über **Consulting, Beratung und Solution Services**

## Zusammenfassung

Eine der einfachsten Möglichkeiten, über Zero Trust nachzudenken, ist "Never Trust AND Always Verify". Dies gilt für alle Netzwerkverbindungen, Sitzungen und Zugriffsanforderungen auf kritische Anwendungen, Workloads und Daten.

Zero Trust Sicherheits-Frameworks schaffen lokalisierte Abwehrmechanismen am Mikroperimeter rund um jede Ressource im Netzwerk des Unternehmens. Wenn sie richtig konzipiert sind, können die Frameworks Ressourcen schützen, unabhängig davon, wo sie sich befinden.

Eine effiziente Methode zur Risikominderung besteht darin, den Zugriff auf privilegierte und gemeinsam genutzte Daten zu kontrollieren und das Prinzip der geringsten Rechte zu übernehmen. Dieses Sicherheitsmodell ermöglicht die Orchestrierung über APIs sowie die Integration mit Workflow-Automatisierungsplattformen, die Transparenz für Benutzer und Anwendungen bieten.

Mit der erfolgreichen Implementierung von Zero Trust kann ein sicherer und nahtloser Betrieb in der gesamten IT-Umgebung eines Unternehmens gewährleistet werden. So wird ein kontinuierlicher, vertrauenswürdiger Zugriff auf die kritischen Workloads, Anwendungen und Daten eines Unternehmens gewährleistet, um die Aufgaben Ihres Unternehmens zu verbessern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.