



Sechs Schritte zur sofortigen Implementierung von Zero Trust

> Ein praktischer Leitfaden
zur kontinuierlichen
Überprüfung mit
WatchGuard



ANSWEREIT

Anwenderschutz Auch über das Netzwerk hinaus

Identitätsüberprüfung Wer stellt eine Verbindung her und von wo aus

Geräteüberprüfung Was ist verbunden

Zugriff auf Sitzungsebene erzwingen Was erreichen sie

Management und Visualisierung vereinheitlichen
Wie sehen und kontrollieren Sie alles?

Automatisierte Erkennung und Reaktion
integrieren Wie reagieren Sie in Echtzeit

Der Nutzen wächst ohne Grenzen



Einführung

Von der Peripherie zur Richtlinie. Die Peripherie existiert nicht mehr.

Anwender verbinden sich von überall – von zu Hause, von Flughäfen und über gemeinsam genutzte Netzwerke.

Anwendungen befinden sich auf SaaS-Plattformen und in hybriden Clouds. Angreifer nutzen gestohlene Anmeldeinformationen, nicht verwaltete Geräte und VPNs mit zu hohen Berechtigungen, um unbemerkt in Netzwerke einzudringen.

Noch ein weiteres Tool ist nicht die Lösung.

Es ist eine **neue Sicherheitsmentalität: Zero Trust**, basierend auf kontinuierlicher Verifizierung, Zugriff mit geringsten Privilegien und adaptiven Richtlinien, die den Anwendern überallhin folgen.

Dieser Leitfaden beschreibt **sechs praktische Schritte** zur sofortigen Umsetzung von Zero Trust durch die Vereinheitlichung von Identitätssicherheit, Endpoint-Sicherheit, hybrider Netzwerksicherheit und erweiterter Bedrohungserkennung und -reaktion unter einer cloudverwalteten Richtlinienkontrollebene.

> Zero Trust basiert auf kontinuierlicher Verifizierung, Zugriff mit geringsten Privilegien und adaptiven Richtlinien, die den Anwendern überallhin folgen.



01

Erweitern Sie den Schutz auf das Internet, wo immer Anwender hingehen

Zero Trust beginnt dort, wo die Gefährdung am größten ist, im Internet.

Remote- und Hybrid-Mitarbeiter verbringen die meiste Zeit online, weit über die traditionellen Grenzen der Peripherie hinaus.

Konsistente cloudbasierte Verteidigung bereitstellen

1. Firewall as a Service (FWaaS): Sicherheits- und Zugriffsrichtlinien ohne physische Geräte durchsetzen.
2. Secure Web Gateway (SWG): Den gesamten Web-Datenverkehr überprüfen und kontrollieren.
3. Schutz der DNS-Ebene: Verhindert Phishing- und Command-and-Control-Aktivitäten, bevor Verbindungen hergestellt werden.

> Richtlinien in der Praxis



Wenden Sie Zero-Trust-Richtlinien an, die sich an der Identität und dem Status des Geräts orientieren:

1. Erlauben Sie vertrauenswürdigen Benutzern auf konformen Geräten den Zugriff auf zugelassene SaaS-Anwendungen.
2. Blockieren oder beschränken Sie den Zugriff, wenn das Risiko des Geräts steigt oder Anwender sich aus unbekannten Netzwerken verbinden.

> Ergebnis



Der Schutz begleitet Ihre Mitarbeiter bei jedem Klick, jeder Verbindung und überallhin.

> Stellen Sie FireCloud bereit, um Netzwerksicherheit bis an den Rand des Netzwerks zu gewährleisten, mit cloudbasiertem Schutz, der Ihre Anwender überallhin begleitet.



02

Identität: Wer verbindet sich und von wo aus?

Jede Zero-Trust-Reise basiert auf Identität.

Bei herkömmlichen Sicherheitsmodellen wird davon ausgegangen, dass eine Person vertrauenswürdig ist, sobald sie sich anmeldet.

Zero Trust geht vom Gegenteil aus: Jede Anmeldung muss sich als vertrauenswürdig erweisen.

1. Setzen Sie adaptive Multifaktor-Authentifizierung durch
Schützen Sie alle Anwender und jede Anwendung mit MFA, SSO und risikobasierter Authentifizierung.
2. Integrieren Sie Anmeldedaten, um Anmeldeverhalten, Gerätesignale und Datenverletzungen zu korrelieren, bevor Sie Zugriff gewähren.
3. Fügen Sie Dark Web Credential Monitoring hinzu, um gefährdete Anmeldedaten zu erkennen, bevor Angreifer sie ausnutzen können. Wenn ein Passwort in Daten zu Sicherheitsverletzungen auftaucht, löst AuthPoint eine verstärkte Überprüfung aus oder sperrt das Konto.

> Implementieren Sie **Total Identity Security** mit Dark Web Credential Monitoring für MFA, SSO und risikobasierte Authentifizierung.

> Richtlinien in der Praxis

Nutzen Sie Standort-, Zeit- und Geräte-DNA-Bedingungen in Zero-Trust-Richtlinien, um die Authentifizierungsstärke dynamisch anzupassen.

> Ergebnis

Nur verifizierte, kompromisslose Identitäten können Vertrauen schaffen.

03

Geräteüberprüfung: Was ist verbunden?

Ein vertrauenswürdiger Anwender auf einem unsicheren Gerät stellt weiterhin ein Risiko dar.

Die Endpoint Detection and Response stellt sicher, dass Geräte vor und während jeder Sitzung Vertrauen verdienen.

Kontinuierliche Überprüfung des Gerätestatus

EDR sollte überprüfen, dass:

1. Endpoint-Agenten ausgeführt werden.
2. Patches und Schutzmaßnahmen auf dem neuesten Stand sind.
3. Keine kritischen Bedrohungen aktiv sind.
4. Keine unbekannten oder riskanten Anwendungen ausgeführt werden.

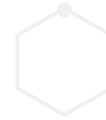
> Setzen Sie **WatchGuard Endpoint Security 360** ein um sicherzustellen, dass Geräte vor und während jeder Sitzung Vertrauen verdienen.

> Richtlinien in der Praxis

Legen Sie Regeln fest, die den Zugriff nur dann zulassen, wenn das Gerät die Sicherheitsanforderungen erfüllt, und isolieren Sie nicht konforme Systeme automatisch.

> Ergebnis

Nur sichere, verifizierte Geräte nehmen an vertrauenswürdigen Sitzungen teil.



04

Zugriff auf Sitzungsebene erzwingen: Was erreichen sie?

Ersetzen Sie implizites Vertrauen durch dynamische sitzungsbezogene Kontrollen.

Ältere VPNs gewähren vollständigen Netzwerkzugriff, sobald sich Anwender authentifizieren. Verwenden Sie Zero Trust Network Access (ZTNA), um sichere, sitzungsbasierte Verbindungen zu bestimmten Anwendungen herzustellen, niemals zum gesamten Netzwerk.

Durchsetzung pro Sitzung

1. Authentifizierung mit AuthPoint.
2. Überprüfen Sie den Gerätestatus über Endpoint Security 360.
3. ZTNA wendet Richtlinien an, die den Zugriff ausschließlich auf für diese Sitzung genehmigte Anwendungen zulassen.

> Richtlinien in der Praxis

Legen Sie ressourcenspezifische Regeln fest: Beispielsweise können Finanzanwender während der Geschäftszeiten nur von kompatiblen Geräten aus auf Buchhaltungs-Apps zugreifen.

> Ergebnis

Ein VPN-freier Zugriff, der granular, verschlüsselt und in Echtzeit widerrufbar ist.

> Aktivieren Sie Sie FireCloud ZTNA, um anwendungsspezifische, sitzungsbasierte Konnektivität durchzusetzen.



05

Management und Visualisierung vereinheitlichen

Zero Trust sollte die Sicherheit vereinfachen, nicht komplizierter machen.

Stellen Sie zentralisierte Identitäts-, Geräte- und Netzwerkdurchsetzung mit einem einheitlichen Zero-Trust-Richtlinien-Framework bereit. Vermeiden Sie unterschiedliche Produkte, die mehrere nicht miteinander verbundene Richtlinien erfordern und zu Lücken in Zero-Trust-Prozessen führen.

Zentralisierte Abläufe

1. Definieren und implementieren Sie Zero-Trust-Richtlinien für alle Dienste über eine einheitliche Schnittstelle.
2. Überwachen Sie Authentifizierungsereignisse, Endpoint-Risiken und Sitzungsdaten in Dashboards.

> Richtlinien in der Praxis



MSP-fähige Mandatenfähigkeit

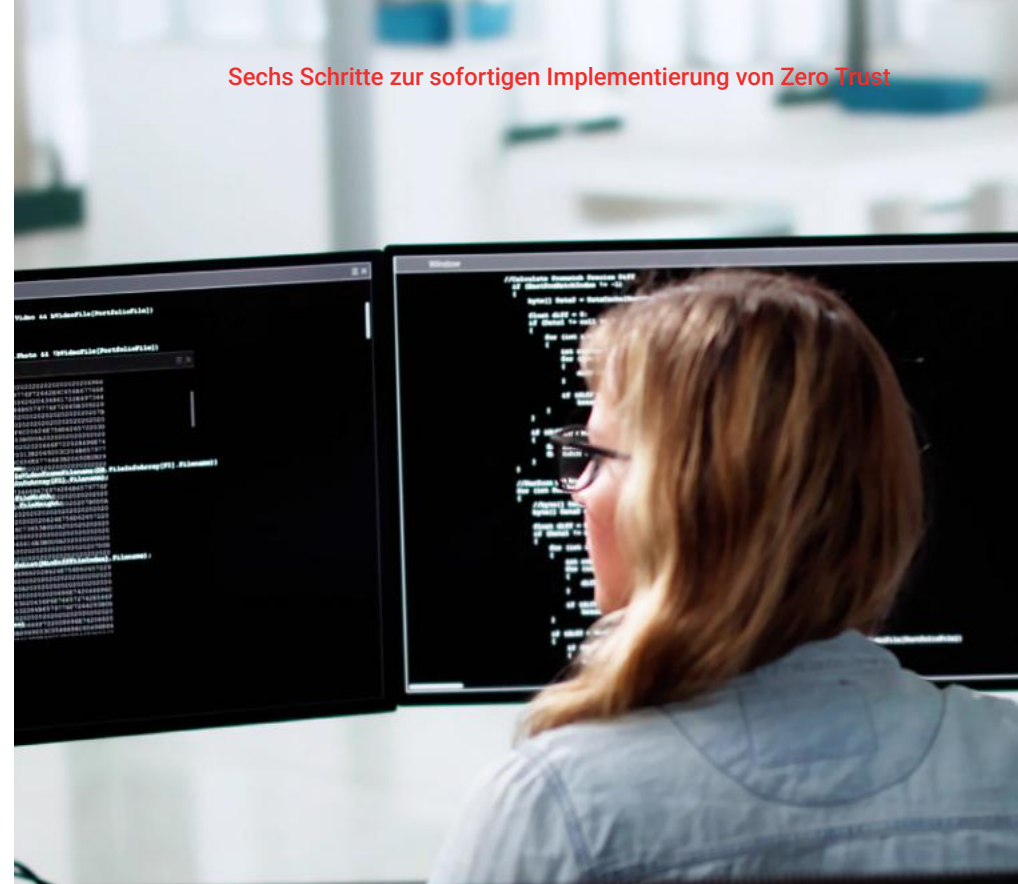
Partner verwalten mehrere Kunden, Vorlagen und automatisierte Berichte über dieselbe Konsole und liefern Zero-Trust-as-a-Service effizient.

> Ergebnis



Eine Plattform, ein Richtlinienmodell, vollständige Transparenz.

> Erstellen Sie einheitliche Richtlinien im Zero Trust Identity Framework von **WatchGuard Cloud** für den Schutz von Identität, Endpoints und hybriden Netzwerken.



06

Automatisierte Erkennung und Reaktion integrieren

Zero Trust ist nicht auf den Zugriff beschränkt, sondern erstreckt sich auch auf die Erkennung von und Reaktion auf Bedrohungen.

Beim Aufbau von Zero Trust geht es nicht nur darum, zu kontrollieren, wer Zugriff erhält. Es geht auch darum, was passiert, wenn sich nach der Zugriffsgewährung das Verhalten ändert, das Risiko steigt oder ein Gerät kompromittiert wird. Hier schließt Threat Detection & Response den Zero-Trust-Kreislauf.

Adaptive Automatisierung

1. Wenn EDR eine Gerätekompromittierung meldet, widerruft ZTNA den Sitzungszugriff.
2. Wenn das Identitätsmanagement unmögliche Bewegungen erkennt, werden das Gerät und die Zugriffsrichtlinien automatisch angepasst.
3. Warnungen und Behebungsmaßnahmen werden über Zero-Trust-Richtlinien hinweg synchronisiert.

> Nutzen Sie **ThreatSync XDR** und Bedrohungsanalysen, die in WatchGuard Zero Trust Solutions integriert und in diesen enthalten sind.

> Richtlinien in der Praxis

ThreatSync korreliert ungewöhnliche Berechtigungsaktionen, ungewöhnliche Geodaten und ungeschützte blockierte Geräte mit Zero-Trust-Telemetriedaten, warnt vor Bedrohungen, isoliert Geräte und blockiert Zugriffsversuche.

> Ergebnis

Bedrohungen werden innerhalb von Sekunden statt Stunden eingedämmt. Zero Trust entwickelt sich parallel zu Ihrer Umgebung weiter.

Der Nutzen: Zero Trust ohne Grenzen

Die Bereitstellung von Zero Trust bedeutet nicht, bei Null anzufangen; es bedeutet, dass Sie Ihre bestehende Infrastruktur um eine kontinuierliche Überprüfung ergänzen.

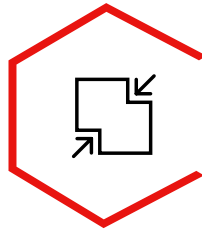
> Mit dem WatchGuard Zero Trust Bundle können Sie:



VPNs durch
sitzungsbasierten
Zugriff ersetzen



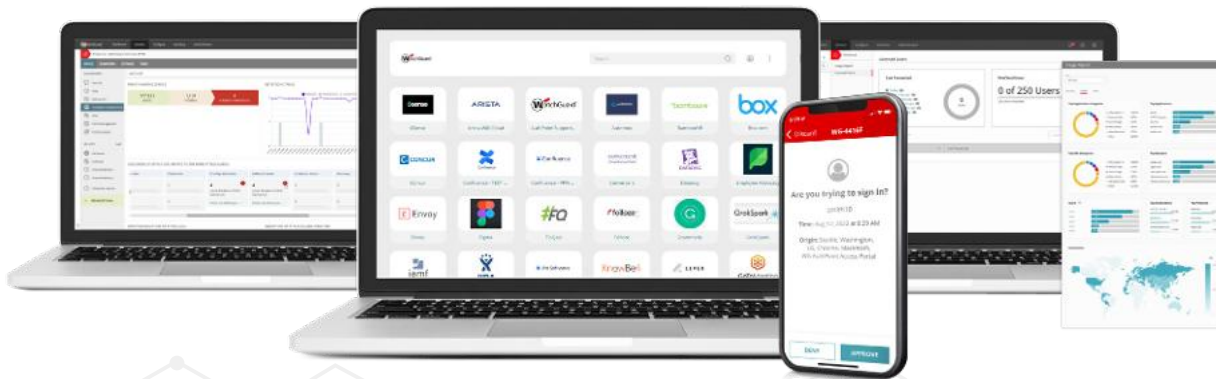
Alle Anwender,
jedes Gerät und jede
Verbindung schützen



Compliance und
Transparenz
vereinfachen



Bereitstellung von
Zero-Trust-as-a-Service
über eine Cloud-Plattform



Zero-Trust-Bundle

AuthPoint



Dark Web Credential-
Monitoring



Endpoint Security 360



FireCloud Total Access
für die Durchsetzung
von Zero Trust



Mehr erfahren

Weitere Details erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter www.watchguard.com/de.

Informationen zu WatchGuard

WatchGuard Technologies gehört zu den weltweit führenden Anbietern im Bereich Cybersicherheit für Managed Service Provider. Im Gegensatz zu anderen Anbietern bietet WatchGuard über seine Unified Security Platform *echte Sicherheit für reale Umgebungen*. Auf der Grundlage von künstlicher Intelligenz und Zero-Trust-Ansätzen bietet das Unternehmen starken und skalierbaren Schutz für Netzwerke, Endpoints und Identitäten. WatchGuard genießt das Vertrauen von mehr als 17.000 Vertriebspartnern und Managed Service Providern, die über 250.000 Unternehmen schützen. Das Unternehmen hilft Partnern, schnell zu wachsen, betriebliche Belastungen zu beseitigen und starke Ergebnisse zu erzielen – ohne zusätzliche Anbieter, Konsolen oder Komplexität. WatchGuard hat seinen Hauptsitz in Seattle, Washington, und unterhält Niederlassungen weltweit. Weitere Informationen finden Sie unter WatchGuard.com/de

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001

INTERNATIONALER VERTRIEB: +1 206 613 0895

WEB www.watchguard.com/de

Mit diesem Dokument werden keine ausdrücklichen oder stillschweigenden Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. © 2026 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox, ThreatSync, Unified Security Platform und AuthPoint sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilnr. WGCE67896_082526

