Microsoft

Zero Trust-Businessplan

Ein praktischer Leitfaden zur Implementierung des Zero Trust-Frameworks im Unternehmen

Inhalt

Die digitale Transformation prägt die neue Normalität

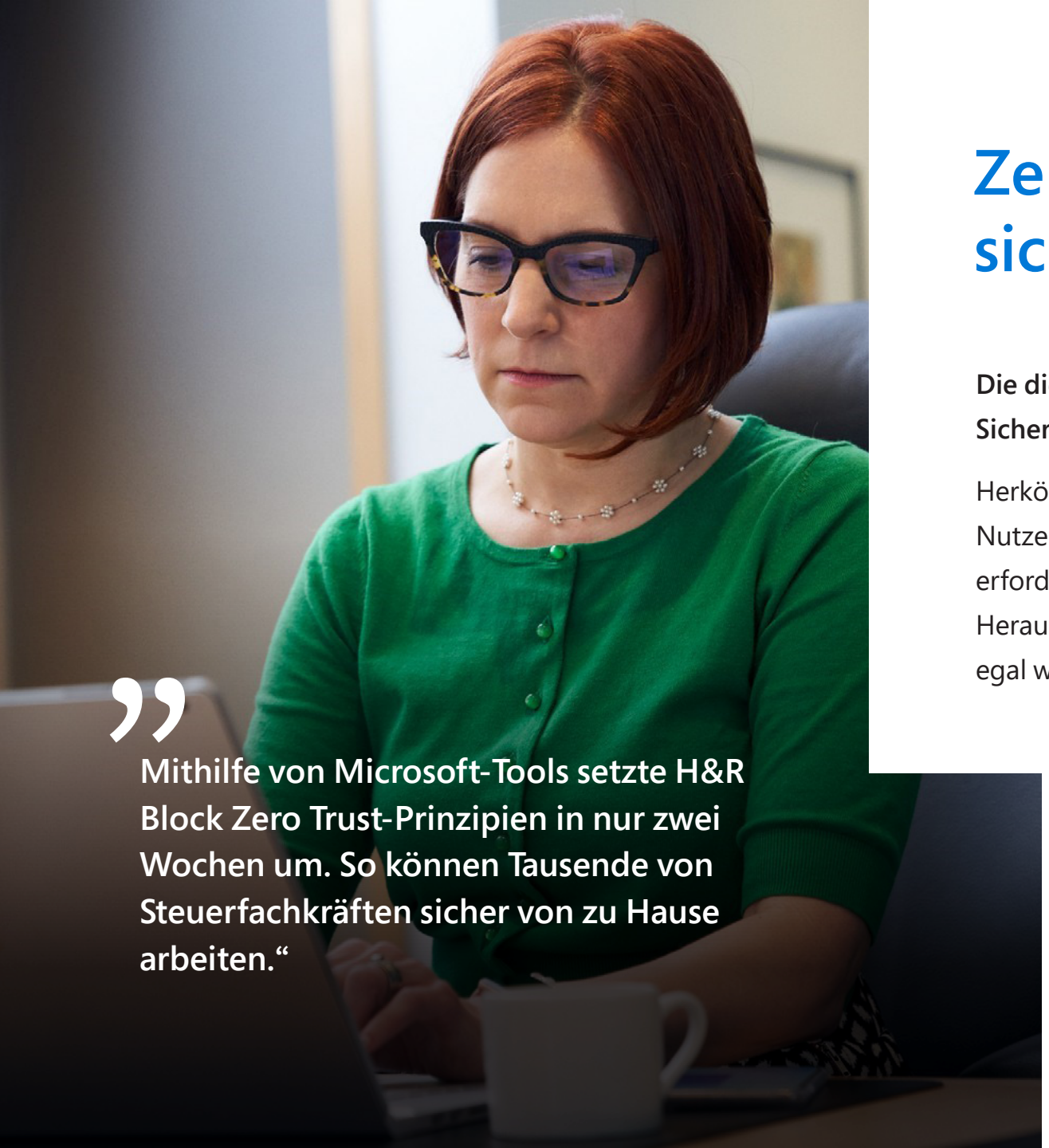
Unternehmen setzen auf die digitale Transformation, um die ständigen Veränderungen in ihrem Geschäftsumfeld zu bewältigen:

- → Wechselnde Geschäftsmodelle und Partnerschaften
- → Technologietrends
- → Regulatorische, geopolitische und kulturelle Kräfte

Die Fernarbeit im Zuge der COVID-19-Pandemie hat die Transformation vorangebracht. Häufig entwickelt sich die Sicherheit dabei von einer Kostenstelle zu einem strategischen Wachstumstreiber.

„COVID hat uns alle gelehrt, dass die Realität nicht immer perfekt ist und dass wir uns auch in Zukunft sehr schnell an neue Situationen anpassen müssen. Je näher wir einem Zero Trust-Modell kommen, desto weniger sollte es eine Rolle spielen, ob wir von zu Hause, der Cloud oder einem Rechenzentrum heraus arbeiten.“

– Führungskraft für Identity & Access Solutions bei einem Finanzdienstleister



”Mithilfe von Microsoft-Tools setzte H&R Block Zero Trust-Prinzipien in nur zwei Wochen um. So können Tausende von Steuerfachkräften sicher von zu Hause arbeiten.“

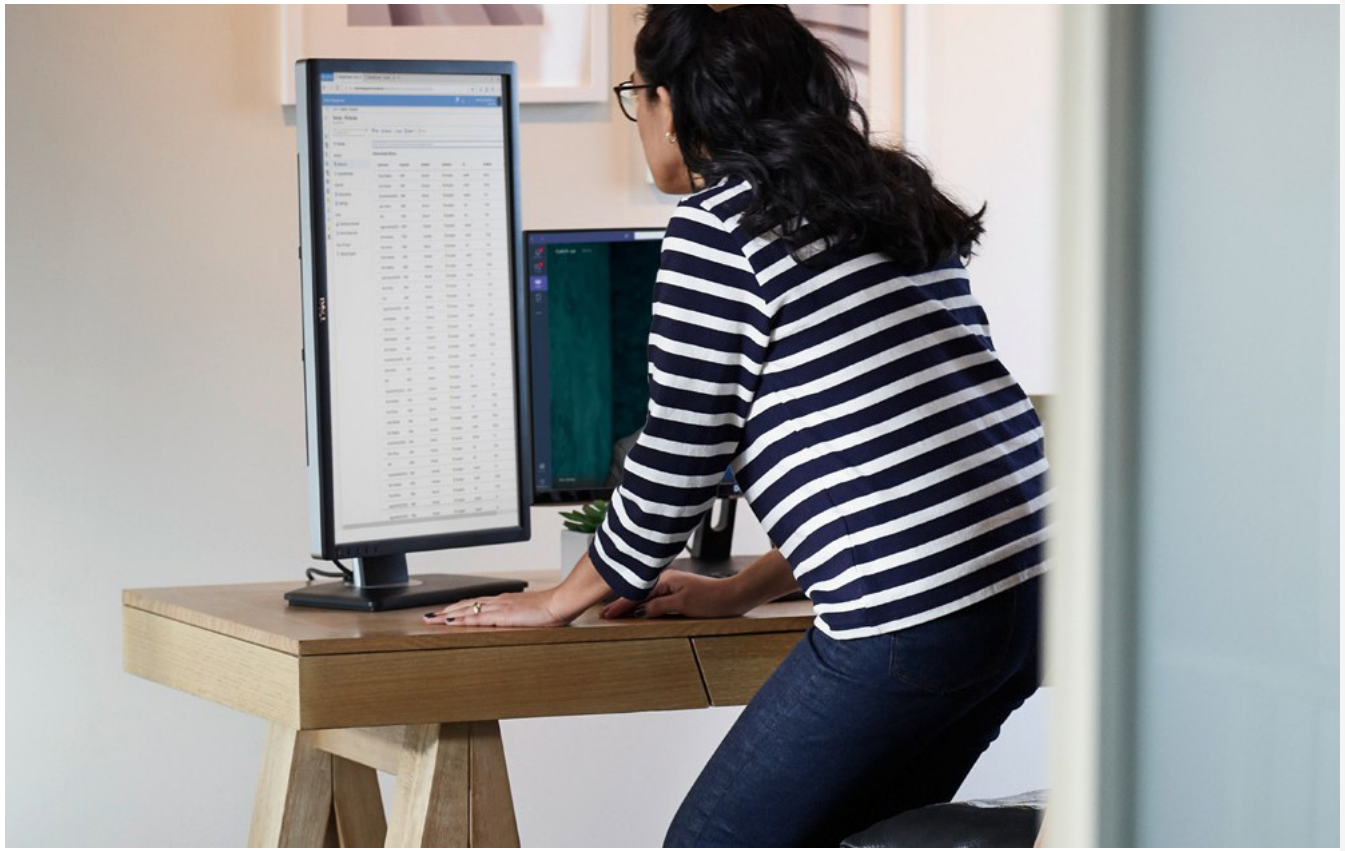
Zero Trust – der Schlüssel zu einer sicheren digitalen Transformation

Die digitale Transformation erfordert die Neuausrichtung traditioneller Sicherheitsmodelle

Herkömmliche Sicherheitskonzepte bieten nicht die geschäftliche Agilität, das Nutzererlebnis und den Schutz, die für eine dynamische digitale Umgebung erforderlich sind. Viele Unternehmen implementieren Zero Trust, um diese Herausforderungen zu meistern und die neue Normalität zu unterstützen – egal wann, wo und mit sie zusammenarbeiten.

Diese Erkenntnisse und Best Practices stammen aus Gesprächen mit Kunden und den Erfahrungen, die Microsoft bei der Implementierung von Zero Trust im eigenen Unternehmen gemacht hat.

Pragmatische Zero Trust-Einführung: Groß denken, klein anfangen, schnell handeln



Entwickeln Sie einen mehrjährigen Businessplan:

Quick-Wins priorisieren

und Einzelinitiativen schrittweise verfolgen

Vorhandene Technologien einbeziehen

nach vorheriger Bereitstellung oder Lizenzierung

Kohärente Initiativen strukturieren

mit klaren Ergebnissen, Vorteilen
und Zuständigkeiten

Die Einführung von Zero Trust

Wir haben ein handlungsorientiertes Best Practices-Framework entwickelt, das Sie durch Ihre eigene Zero Trust-Journey führt. In jeder Phase erhalten Sie Anleitungen, Best Practices, Ressourcen und Tools für eine reibungslose Implementierung.

1 Planen

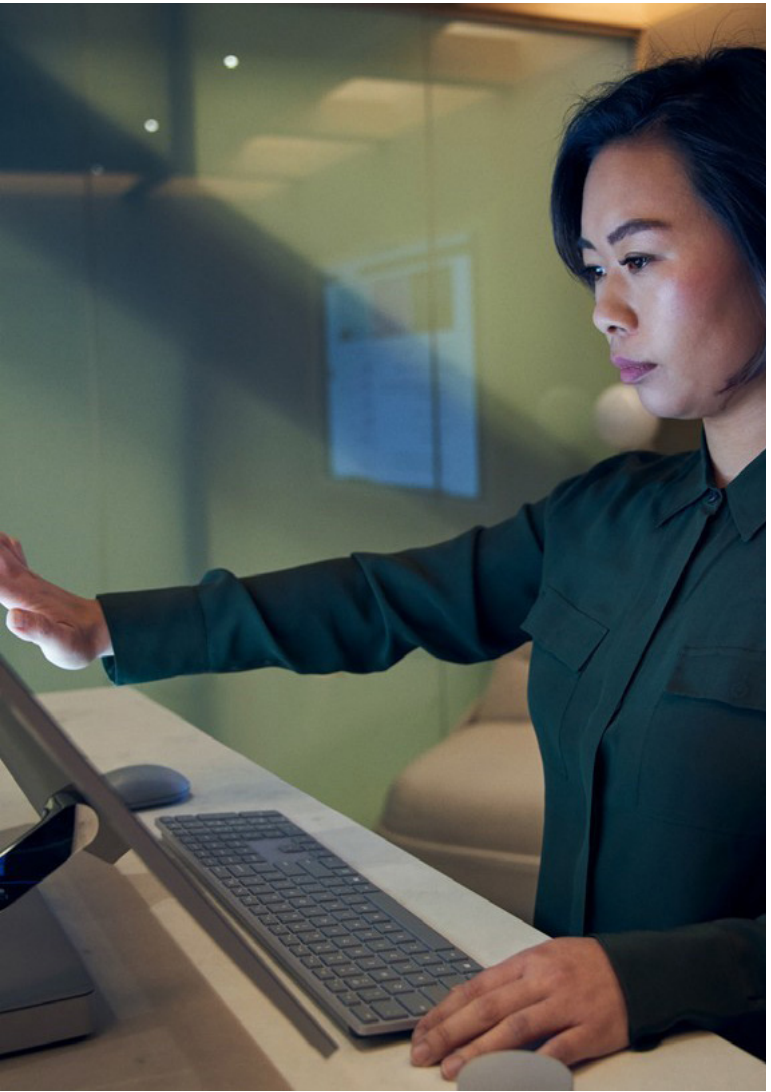
Erstellen Sie einen Business Case, der sich auf die Ergebnisse konzentriert, die die Risiken und strategischen Ziele Ihres Unternehmens am besten abbilden.

2 Implementieren

Entwickeln Sie eine mehrjährige Strategie für Ihre Zero Trust-Bereitstellung, und priorisieren Sie frühe Maßnahmen auf der Grundlage Ihrer Geschäftsanforderungen.

3 Messen

Überwachen Sie den Erfolg Ihrer Zero Trust-Bereitstellung, um sicherzustellen, dass die Zero Trust-Implementierung messbare Fortschritte bringt.



Zero Trust-Plan: Ihre Schritte zum Erfolg

Empfohlene Priorisierung:

→ **Vision festlegen** – Zero Trust ist eine komplexe Journey, die sich über mehrere Jahre erstrecken kann. Wenn Unternehmen ihre Ziele, Ergebnisse und Architekturen klar **definieren**, ist der Erfolg größer als bei einem reaktiven Ansatz.

Hinweis: Der Nutzen und die Implementierung können je nach Rolle und Verantwortungsbereich stark abweichen.

→ **Unterstützung von Vorgesetzten sichern** – Erfolgreiche Zero-Trust-Implementierungen sind auf Geschäftsergebnisse ausgerichtet, um mit Unterstützung der Führungsebene ambitionierte Ziele, Budgetzuweisungen und interne Abstimmungen zu erreichen.

→ **Endnutzer stärken** – Dank Zero Trust können Technologieteams direkt mit den Endnutzern in Kontakt treten, um Sicherheit als Motor für ein positives Nutzererlebnis und hohe Produktivität zu nutzen.

PLANEN 〉 IMPLEMENTIEREN 〉 MESSEN

Eine Vision festlegen und Unterstützung von Vorgesetzten sichern

Um sich die Unterstützung von Führungskräften zu sichern, müssen Sie zuerst die geschäftlichen Prioritäten ermitteln und verstehen. Entwickeln Sie dann eine Vision, die auf die Geschäftsergebnisse ausgerichtet ist.

Obwohl diese Vision immer auf die geschäftlichen Prioritäten und die Unternehmenskultur zugeschnitten werden muss, haben wir in unterschiedlichen Unternehmen mehrere gemeinsame Ansätze gefunden:

- → **Geschäftliche Agilität**, um schnell neue Chancen zu erkennen und zu nutzen – bei gleichzeitiger Risikoeindämmung, Unterstützung von Fernarbeit und Migration in die Cloud
- → **Eindämmen der Komplexität**, die durch ständig neue Geschäftspartnerschaften, den Wettbewerb und das dynamische technische Umfeld entsteht
- → **Messbare Prozesse**, um die Verantwortlichkeit für Geschäftsergebnisse und Risiken sicherzustellen

”Einer der wichtigsten Faktoren unserer Zero Trust-Bereitstellung ist die Top-down-Unterstützung. Unser CEO weiß, wie riskant der Verzicht auf eine Zero Trust-Strategie sein kann – dafür sind wir verantwortlich.“

– Führungskraft, Identity & Access Solutions, Finanzdienstleistungen

Einen überzeugenden Business Case für Zero Trust erstellen

Ein überzeugender Business Case trägt dazu bei, sich die Unterstützung von Vorgesetzten zu sichern und alle Geschäftsbereiche einzubinden. Obwohl ein Zero Trust-Sicherheitsmodell viele Vorteile mit sich bringt, erzielen Unternehmen den größten Erfolg mit diesen vier Business Cases:

- → Orts- und zeitunabhängiges Arbeiten unterstützen
- → Sichere und schnelle Cloudmigration fördern
- → Kostenvorteile durch ein vereinfachtes Sicherheitskonzept erzielen

Konzentrieren Sie sich auf die Vorteile für Ihr Unternehmen wie:

- → **Proaktive Risikovermeidung** und -kontrolle
- → **Risikomanagement für Partner**, die über schwache Sicherheitsprogramme verfügen
- → **Agile Sicherheit und Compliance**, um schnelle Statusänderungen in Bezug auf Rollen und Unternehmen zu berücksichtigen

PLANEN 〉 **IMPLEMENTIEREN** 〉 MESSEN

Zero Trust-Implementierung: Ihre Schritte zum Erfolg

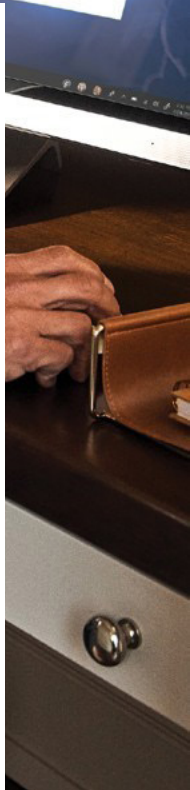
Unterteilen Sie das Programm in klare und kohärente Initiativen. Microsoft hat festgestellt, dass sich technische Strategien und Architekturen ganz natürlich in diese Sicherheitsinitiativen einfügen:

- → Produktivitätssicherung
- → Moderne Sicherheitsmaßnahmen
- → Operative Technologie (OT) und Internet der Dinge (IoT), *falls für das Unternehmen zutreffend*
- → Rechenzentrum, Dienste und API

Diese Initiativen beruhen auf den Erfahrungen von Microsoft und weiteren erfolgreichen Kundenimplementierungen.

Priorisieren und planen Sie Initiativen:

- → **Einzelne Initiativen auf die Geschäftsziele ausrichten** und potenzielle positive Auswirkungen auf das Geschäft, Reibungspunkte und Herausforderungen evaluieren
- → **Kurzfristigen Plan entwickeln.** Beginnen Sie mit Quick-Wins, und sichern Sie sich die Unterstützung der Führungsebene.
- → **Langfristige Roadmap entwickeln**



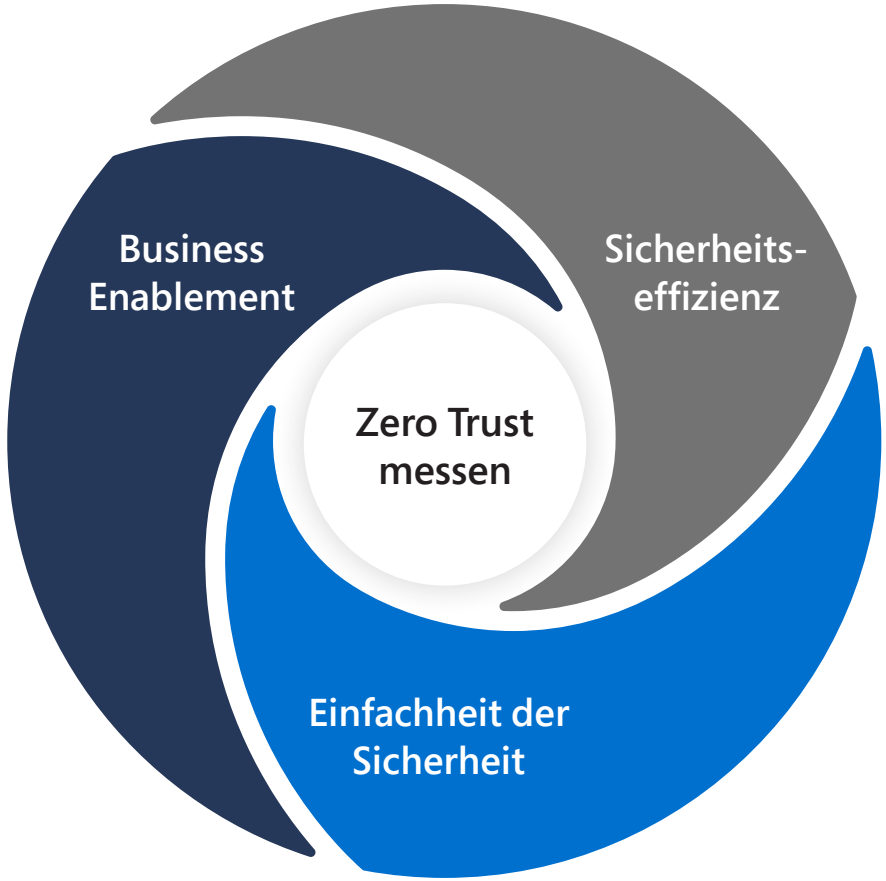
Fortschritt messen – Ihre Schritte zum Erfolg

Identifizieren Sie wichtige Meilensteine und Leistungsziele für Ihr Unternehmen. Messen Sie den Fortschritt, und erstellen Sie Berichte über Erfolge und Lerneffekte.

- **Business Enablement –** Messen Sie negative Auswirkungen auf das Nutzererlebnis und die Dauer, bis interne Sicherheitsgenehmigungen für Initiativen vorliegen.

- **Sicherheitseffizienz –** Ermitteln Sie, inwieweit die Anzahl oder die Auswirkungen von Sicherheitsvorfällen zurückgehen, nachdem das Unternehmen eine Zero Trust-Strategie eingeführt hat.

- **Einfachheit der Sicherheit –** Verringern Sie die Anzahl von Sicherheitsanbietern, die Ihr Team integrieren muss, und senken Sie die Kosten, die durch manuelle Aufgaben entstehen (z. B. Anrufe zum Zurücksetzen von Kennwörtern).

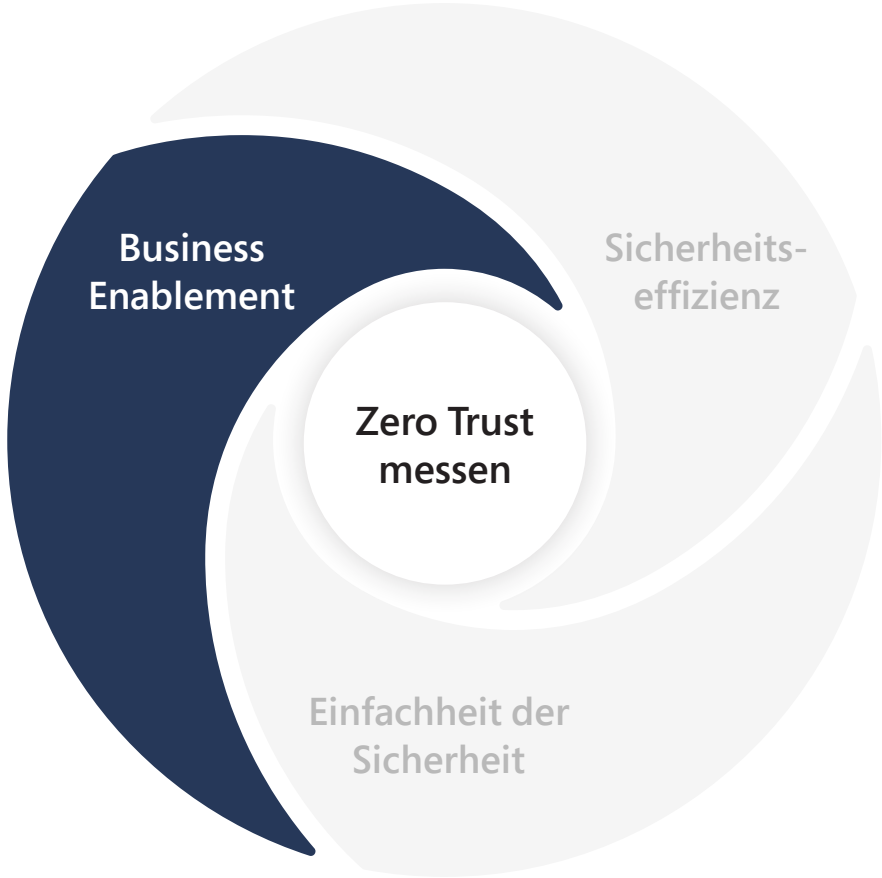


Fortschritte beim Business Enablement messen

Das Ziel von Zero Trust ist eine reibungslose Nutzer- und Entwicklererfahrung:

- → Anzahl der sicherheitsbedingten Unterbrechungen im Benutzerworkflow (z. B. Aufforderungen zur mehrstufigen Authentifizierung an einem Tag)
- → Meilensteine bei der Bereitstellung (z. B. Prozentsatz der Beschäftigten, die über Single Sign-On auf Apps zugreifen)
- → Sichtbarkeit von Meilensteinen (z. B. Rückgang der App-Nutzung aufgrund einer negativen Anmeldeerfahrung)
- → Durchschnittliche Startzeit verwalteter Geräte in Sekunden
- → Durchschnittliche Dauer für die Sicherheitsbewertung von Anwendungen in Tagen

Vergessen Sie nicht die Mechanismen zur Befragung der Endnutzer. Erkundigen Sie sich, wie benutzerfreundlich der Zugriff oder Prozess zum Zurücksetzen von Kennwörtern empfunden wird.

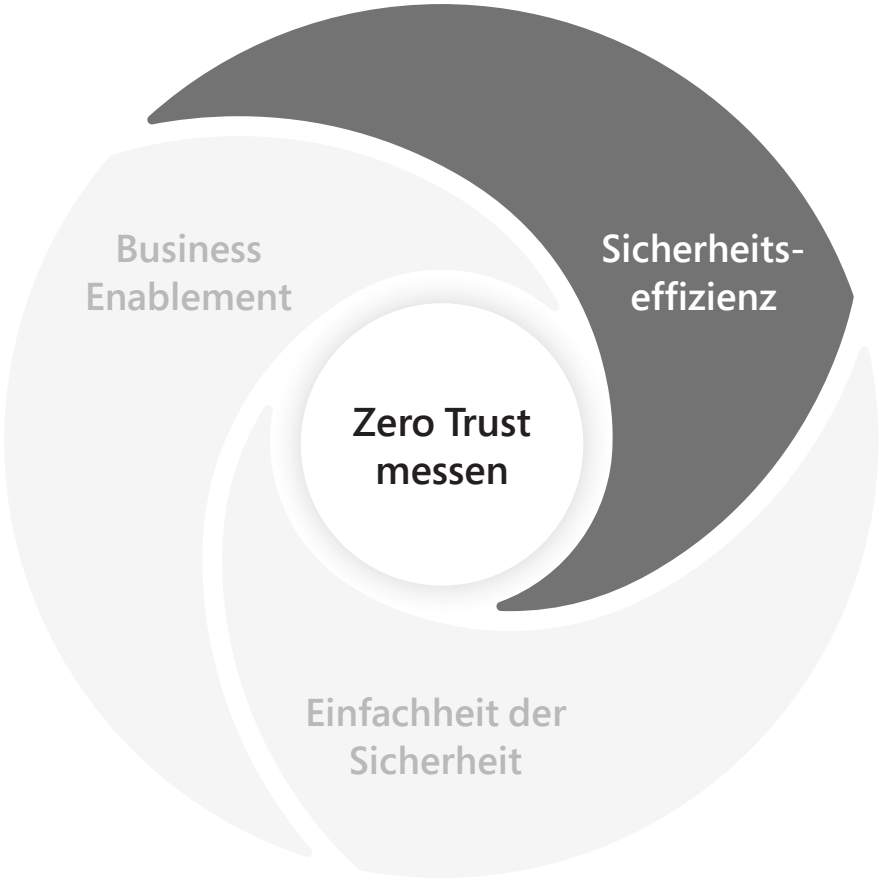


Sicherheitseffizienz messen

Messen Sie Ihren Sicherheitsstatus und die daraus resultierenden Auswirkungen von Sicherheitsvorfällen:

- Anzahl der Sicherheitsvorfälle (nach Schweregrad)
- Meilensteine bei der Bereitstellung (z. B. Prozentsatz der Beschäftigten, die MFA aktiv nutzen)
- Sichtbarkeit der Meilensteine (z. B. der Prozentsatz verwalteter Geräte/Apps)
- Sicherheitsstatus – Verfolgen Sie den Fortschritt mithilfe der Microsoft-Sicherheitsbewertung.

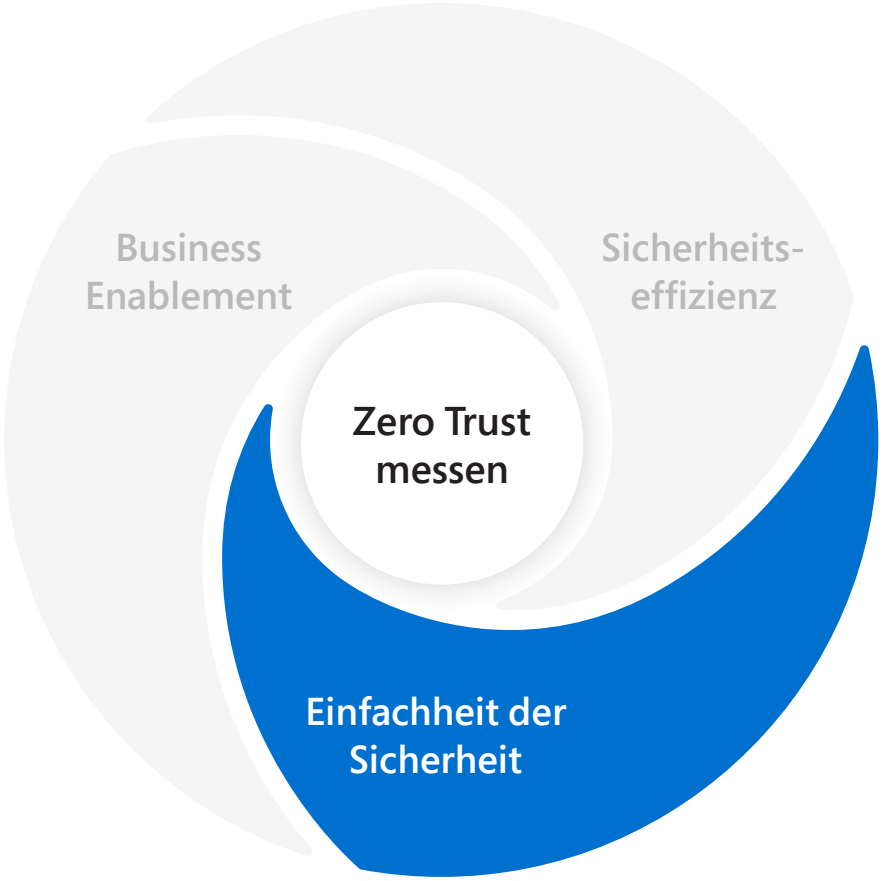
Im Kontext betrachtet: Zero Trust führt zu einer höheren Sichtbarkeit, sodass Sie möglicherweise Vorfälle entdecken, die früher übersehen wurden.



Einfachheit der Sicherheit messen

Zero Trust senkt häufig die Anforderungen, die zur Umsetzung des Sicherheitskonzepts nötig sind

- Anzahl der doppelten Sicherheitstools, die ähnliche oder identische Funktionen ausführen
- Anzahl der Sicherheitstools, die eine individuelle Integration erfordern
- Prozentualer Anteil der Zeit, die der IT-Helpdesk für geringwertige Aktivitäten wie das Zurücksetzen von Kennwörtern aufwendet
- Die Anzahl der manuellen Schritte in wiederkehrenden Workflows (z. B. die Untersuchung häufiger Warnungen/Vorfälle, die manuelle Nutzerbereitstellung und Aufgaben rund um Complianceberichte)
- Prozentualer Anteil der falsch-positiven Warnungen, die von Sicherheitsteams untersucht werden
- Verhältnis der Zeit, die für die Wartung von Tools statt zur tatsächlichen Reaktion auf Vorfälle aufgewendet wird



Zero Trust – eine Grundvoraussetzung für die digitale Transformation

Sie müssen nicht gleich die ganze Technologie austauschen, um loszulegen.

Beginnen Sie damit, Ihre Zero Trust-Investitionen auf Ihre aktuellen Geschäftsanforderungen abzustimmen, und konzentrieren Sie sich auf Quick-Wins. Jeder Erfolg bringt einen zusätzlichen Nutzen und trägt zu mehr Sicherheit in der ganzen digitalen Umgebung bei.

Es ist nie zu spät, mit Zero Trust anzufangen – auch mit einem kleinen Einstiegsprojekt.

> **Seit wir bei unserer Zero Trust-Strategie auf Microsoft 365-Technologien vertrauen, können wir unseren Mitarbeitern einen weltweiten Arbeitsplatz bieten, ohne auf die engmaschige Kontrolle der IT-Sicherheit zu verzichten.“**
>
> – Igor Tsyganskiy, Chief Technology Officer, Bridgewater Associates

Wie geht's weiter?

Vielen Dank für Ihr Interesse am Best Practices-Leitfaden zu Zero Trust. Lesen Sie bitte unser Microsoft Zero Trust Maturity Model Vision Paper (zum Herunterladen anklicken), falls Sie es noch nicht kennen. Darin werden die Grundprinzipien von Zero Trust und unser Reifegradmodell beschrieben, in dem die wichtigsten Anforderungen für jedes der sechs grundlegenden Elemente aufgeschlüsselt sind.

Wir haben außerdem nützliche Erkenntnisse, technische Anleitungen und weitere Ressourcen auf unserer externen Microsoft Zero Trust-Website zusammengestellt.


Microsoft