

WHITEPAPER

Zero Trust in der Praxis: Wie moderne Unternehmen ihre Netzwerke *vereinfachen* *und absichern*

Hybrides Arbeiten, Multi-Cloud, verteilte Standorte und wachsende Security-Risiken stellen Unternehmen heute vor große Herausforderungen. Klassische VPN-Lösungen sind schwer skalierbar, komplex zu managen und sicherheitstechnisch überholt.

NetBird bietet einen modernen Zero Trust Ansatz auf Basis von WireGuard® – einfach auszurollen, hoch performant, identitätsbasiert und ideal für moderne IT Infrastrukturen. Dieses Whitepaper zeigt anhand realer Use Cases, wie Unternehmen NetBird erfolgreich einsetzen.



USE CASE 1: Sichere Remote-Arbeit ohne VPN Komplexität

| | |
|---------------------------|--|
| Herausforderung | Große Remote-Teams erzeugen VPN-Bottlenecks, unsichere breite Netzfreigaben und hohen Supportaufwand. |
| Lösung mit NetBird | <ul style="list-style-type: none">› NetBird-Agent auf jedem Endgerät – verbindet sich automatisch per WireGuard-Tunnel› Keine Firewall-Regeln oder komplexe Konfiguration nötig› Zugriff basiert auf Gruppen statt IP Adressen› Integriertes MFA & SSO |
| Vorteile | <ul style="list-style-type: none">✓ Schnellere Verbindungen ohne VPN-Engpässe✓ Benutzerfreundlich (kein VPN-Client-Chaos)✓ Least-Privilege-Zugriff für mehr Sicherheit |

USE CASE 2: Standortvernetzung über Routing Peers

| | |
|---------------------------|---|
| Herausforderung | Standorte, Rechenzentren und Cloud-VPCs müssen sicher angebunden werden – oft mit Ressourcen, die keinen Agent unterstützen (Drucker, Datenbanken, Legacy-Server). |
| Lösung mit NetBird | <ul style="list-style-type: none">› Routing Peers verbinden NetBird-Nutzer mit internen Netzwerken› Unterstützt Windows, Linux, VM, Docker, Kubernetes, Raspberry Pi etc.› Eingehende Ports können vollständig geschlossen bleiben |
| Vorteile | <ul style="list-style-type: none">✓ Keine Agent-Installation auf Zielsystemen✓ Hochverfügbarkeit mit mehreren Routing Peers✓ Sichere Verbindung zwischen On-Prem & Cloud |

USE CASE 3: Cloud-Access-Control für SaaS (z. B. Microsoft 365)

| | |
|---------------------------|---|
| Herausforderung | Zugriff auf sensible Cloud-Systeme soll nur aus sicheren Verbindungen erfolgen. |
| Lösung mit NetBird | <ul style="list-style-type: none">› Cloud-Domains als virtuelle Ressourcen verwalten (z. B. Office365)› Zugriff wird nur erlaubt, wenn der User im NetBird-Netz ist› Traffic kann über definierte Routing Peers laufen |
| Vorteile | <ul style="list-style-type: none">✓ Schutz vor Datenabfluss✓ Konsistente Compliance✓ Identity-basierte Cloud-Sicherheit |

USE CASE 4: Zero-Trust durch Geräte- und Sicherheitszustand

| | |
|---------------------------|---|
| Herausforderung | Nicht alle Geräte sind sicher: BYOD, ungepatchte Systeme oder Geräte ohne EDR erhöhen Risiken. |
| Lösung mit NetBird | <ul style="list-style-type: none">› Posture Checks: OS-Version, Prozesse, Client-Version prüfen› MDM/EDR-Integration: Zugriff nur von verwalteten, sauberen Geräten› CrowdStrike ZTA-Score kann als Sicherheitsfilter genutzt werden |
| Vorteile | <ul style="list-style-type: none">✓ Konsequente Zero-Trust-Durchsetzung✓ Reduzierte Angriffsfläche✓ Keine Schatten-IT mehr |

USE CASE 5: Automatisiertes Identity-basiertes On- & Offboarding

| | |
|---------------------------|--|
| Herausforderung | Manuelle Pflege von VPN-Usern und Firewalls kostet Zeit und produziert Fehler. |
| Lösung mit NetBird | <ul style="list-style-type: none">› Vollständige Integration in IdPs (Entra ID, Okta, Google Workspace)› Gruppenänderungen synchronisieren Zugriffsrechte automatisch› Sofortige Deaktivierung bei Offboarding |
| Vorteile | <ul style="list-style-type: none">✓ Weniger IT-Tickets✓ Hohe Sicherheit durch sofortigen Zugriffsentzug✓ Sauberes Rollen- & Berechtigungsmanagement |

USE CASE 6: Monitoring, Audit & Compliance

| | |
|---------------------------|---|
| Herausforderung | Unternehmen benötigen lückenlose Nachvollziehbarkeit für Audits & Incident Response. |
| Lösung mit NetBird | <ul style="list-style-type: none">› Audit-Logs dokumentieren alle Netzwerkänderungen› Traffic-Events analysieren Peer-Traffic, Site-to-Site & Ressourcenkommunikation› Export in SIEM/Monitoring-Tools wie Logsign, Data Lake von Bitdefender oder Enginsight |
| Vorteile | <ul style="list-style-type: none">✓ Transparent & revisionssicher✓ Einfache Audit-Vorbereitung✓ Schnellere Reaktion auf Sicherheitsvorfälle |



Integrierte Checkliste – „Bin ich bereit für Zero Trust mit NetBird?“

Diese Checkliste hilft dem User sofort zu erkennen, ob NetBird zur eigenen Umgebung passt.

1. Sicherheit & Identität

- › Wir nutzen einen Identity Provider (z. B. Entra ID, Okta, Google Workspace).
- › User Gruppen sind sauber aufgebaut (für Zugriffssteuerung).
- › Wir möchten On- / Offboarding automatisieren.
- › Wir haben MDM oder EDR im Einsatz (z. B. CrowdStrike)
- › Wir wollen Zugriffe basierend auf Gerätezustand steuern (Posture Checks).

2. Infrastruktur & Netzwerke

- › Wir kennen unsere internen Ressourcen (Server, Drucker, DBs etc.).
- › Wir müssen Geräte einbinden, die keinen Agent unterstützen. (→ Routing Peers)
- › Wir haben mehrere Standorte oder Cloud VPCs.

3. Cloud Zugriff

- › Bestimmte SaaS-Dienste sollen nur aus sicheren Verbindungen erreichbar sein.
- › Wir möchten Traffic über definierte IPs oder Peers leiten.
- › Wir wollen Cloud-Zugriff identitätsbasiert statt IP-basiert steuern.

4. IT Prozesse & Automatisierung

- › Wir möchten Zugriffsrechte automatisiert über Gruppen steuern.
- › Wir wollen Firewall- und VPN-Tickets reduzieren.
- › Wir nutzen Intune oder Kandji für Geräte-Rollouts. (→ MSI Deployment)

5. Monitoring & Compliance

- › Änderungen am Netzwerk müssen protokolliert werden. (→ Audit Logs)
- › Wir brauchen Traffic-Transparenz.
- › Logs müssen in Tools wie Datadog, S3 oder SIEM-Systeme exportierbar sein.

6. User Experience & Performance

- › VPN-Latenzen oder Ausfälle sind ein Problem.
- › Remote-Mitarbeiter sollen stabilere & schnellere Verbindungen bekommen.
- › Wir brauchen eine Lösung ohne komplexe Firewall-Konfiguration.