WLAN Bericht Deutschland 2026

Den Multiplikatoreffekt freisetzen: Wie strategische WLAN-Investitionen das Unternehmenswachstum im KI-Zeitalter vorantreiben

Deutschland

Zusammenfassung

Im Jahr 2026 hat sich WLAN von einer bloßen Komfortfunktion zu einem strategischen Wachstumsmotor entwickelt. Weltweit sind Unternehmen, die ganzheitlich in WLAN investieren, viermal wahrscheinlicher, einen starken ROI und messbare Verbesserungen in allen Geschäftsbereichen zu erzielen – von der betrieblichen Effizienz bis hin zum Umsatzwachstum. Dieser Multiplikatoreffekt unterscheidet WLAN von anderen IT-Investitionen und liefert zusammengesetzte Renditen im gesamten Unternehmen.

Dennoch berichten fast alle (98 %), dass die Komplexität zunimmt, Sicherheitsbedrohungen sich vervielfältigen und die zur Bewältigung dieser Herausforderungen benötigten Fachkräfte immer knapper werden. Unternehmen müssen sich an unterschiedliche Konnektivitätsanforderungen anpassen und eine wachsende Vielfalt von Nutzern und Geräten unterstützen – von Mitarbeitern und Auftragnehmern bis hin zu autonomen Robotern, intelligenten Sensoren und KI-gestützten Anwendungen.

Globale Unternehmen, die ganzheitlich in KI, Automatisierung, moderne Sicherheit und zertifiziertes Fachwissen investieren, haben einen Vorsprung gegenüber jenen, die dies nicht tun:

+4x

wahrscheinlicher, starke Renditen bei WLAN-Investitionen zu erzielen

höherer durchschnittlicher ROI bei WLAN-Investitionen

Dieser erste Bericht offenbart ein WLAN-KI-Paradoxon: KI ist gleichzeitig der führende Treiber des WLAN-ROI und die größte Quelle eskalierender Risiken. Während KI-gestützte Betriebsabläufe Hunderte von Stunden pro IT-Fachkraft jährlich freisetzen können, verstärken sie auch den Infrastrukturbedarf, Sicherheitsbedrohungen und den Fachkräftemangel. Der Bericht stützt sich auf Wi-Fi als primäre Konnektivitätsebene im Unternehmensumfeld und analysiert zugleich das übergreifende drahtlose Ökosystem, das dadurch ermöglicht wird – einschließlich KI-gestützter Anwendungen, IoT- und OT-Infrastrukturen sowie aufkommender Nutzungsszenarien in der Unternehmenspraxis.

Unsere Forschung identifiziert veraltete Infrastruktur sowie drei miteinander verknüpfte Hindernisse, die Unternehmen daran hindern, den WLAN-ROI voll auszuschöpfen: betriebliche Komplexität, sich verschärfende Sicherheitsbedrohungen und Talentlücken. Diese Herausforderungen verstärken sich gegenseitig und führen zu eskalierenden Risiken.

Unternehmen, die diese betrieblichen, sicherheitsbezogenen und personellen Hindernisse ganzheitlich angehen, erzielen einen um 63 % höheren ROI als jene, die dies nicht tun. Dies zeigt, dass strategische WLAN-Investitionen messbare, zusammengesetzte Renditen in mehreren Dimensionen liefern.

Die Ergebnisse zeigen durchgehend, dass Unternehmen in Deutschland, die WLAN strategisch priorisieren, messbare Renditen in mehreren Dimensionen erzielen. Mehr als 76 % berichten über Verbesserungen bei der betrieblichen Effizienz, der Mitarbeiterproduktivität (73 %) und dem Kundenerlebnis (64 %), während 61 % positive Umsatzauswirkungen melden. Dies belegt, dass moderne WLAN-Infrastruktur sich direkt in Unternehmenswachstum übersetzt.

Das Fenster für Wettbewerbsvorteile ist jetzt geöffnet. Unternehmen in Deutschland, die 2026 entschlossen handeln – Abläufe vereinfachen, WLAN-Sicherheit modernisieren und zertifiziertes Fachwissen aufbauen – werden WLAN als strategischen Wachstumsmotor für das nächste Jahrzehnt positionieren.

WLAN-Strategie in einem perfekten Sturm: Das KI-Paradoxon und die Hindernisse bei der ROI-Realisierung

Das WLAN-KI-Paradoxon und seine Bedeutung

Das WLAN-KI-Paradoxon stellt die zentrale strategische Herausforderung für Deutschlands Unternehmensführer im Jahr 2026 dar – und die Chance für First Mover. KI ist gleichzeitig der führende Treiber des WLAN-ROI und die Quelle der größten Herausforderungen. Weltweit sind Unternehmen, die KI einsetzen, eher geneigt, WLAN als strategisch kritisch anzusehen, und erzielen wesentlich stärkere Renditen, wenn sie die WLAN-Optimierung in ihre KI-Einsatzstrategien integrieren. Gleichzeitig schafft dieselbe KI noch nie dagewesene betriebliche Komplexität, trägt zu neuen Sicherheitsbedrohungen bei und verstärkt den Wettbewerb um Talente.

Das WLAN-KI-Paradoxon
KI ist sowohl die Lösung als auch die Herausforderung

Lösung
- KI-gestützte Betriebsabläufe vereinfachen die WLAN-Komplexität
- Automatisierung befreit IT-Teams, um sich auf die Strategie zu konzentrieren
- Optimierte Ticket-Bearbeitung und schnellere Workflows

Herausforderung
- KI-generierte Cyberangriffe sind die größte Sicherheitsbedrohung
- Talentmangel bei fortgeschrittenen WLAN-/KI-Fähigkeiten
- IT-Talente werden von WLAN in Richtung KI abgezogen

KI ist der führende Weg zum ROI im WLAN – aber auch die größte Risikoquelle.

KI stellt Wireless-Teams vor vielschichtige Herausforderungen

Wichtigste Ursachen von Sicherheitsbedrohungen	Top-Bereiche, die IT-Fachkräfte vom Wireless-Bereich abziehen	Größte Hürden bei der Gewinnung von Wireless-Fachkräften
#1 KI-generierte oder automatisierte Cyberangriffe / automatisierte Angriffstools	**#1** Cybersicherheit	**#1** Mangel an Kandidaten mit fortgeschrittenen Wireless- oder KI-integrierten Kompetenzen
#2 Remote- und Hybridarbeitsmodelle erweitern die Angriffsfläche / nicht verwaltete Endgeräte	**#2** KI / Machine Learning	**#2** Interne Budgetbeschränkungen oder Einstellungsstopps
#3 Zunehmende Nutzung von IoT und vernetzten Geräten	**#3** Softwareentwicklung / App-Entwicklung	**#3** Geografische Einschränkungen oder Herausforderungen bei Remote-Arbeit

Unternehmen in Deutschland, die KI-Workloads einsetzen, nehmen die Kritikalität von WLAN anders wahr als andere. Unter globalen WLAN-Spitzenreitern in Unternehmen mit KI-Workloads betrachten 56 % WLAN als strategisch kritisch, verglichen mit 46 % der Nicht-Einsetzer.

Der Grund für diese erhöhte strategische Bedeutung ist einfach: KI-Workloads erfordern leistungsfähigere und widerstandsfähigere drahtlose Netzwerke. Jene, die die WLAN-Optimierung in ihre KI-Einsatzstrategien integrieren, erzielen wesentlich größere Renditen. In Deutschland berichten fast sieben von zehn Unternehmen von positiven Auswirkungen ihrer WLAN-Investitionen in den Bereichen betriebliche Effizienz, Kundenbindung, Mitarbeiterproduktivität und Umsatzsteigerung.

Hindernis 1: Betriebliche Komplexität überfordert aktuelle Fähigkeiten

Das erste Hindernis, das Unternehmen daran hindert, das KI-Paradoxon aufzulösen, ist die zunehmende betriebliche Komplexität. Fast jeder WLAN-Verantwortliche (98%) in Deutschland berichtet, dass der WLAN-Betrieb komplexer wird, was zu einer reaktiven Haltung führt, die Ressourcen bindet, strategische Arbeit verhindert und die AIOps- und Automatisierungsinitiativen direkt unterhöhlt, die zur Reduzierung der Komplexität beitragen sollen. Dies führt zu einem Teufelskreis: Komplexität treibt reaktive Arbeit an, reaktive Arbeit begrenzt die Modernisierung, und fehlende Modernisierung perpetuiert die Komplexität.

Unternehmen in Deutschland nennen drei primäre Treiber dieser wachsenden Komplexität: die Notwendigkeit, neue Sicherheitsrisiken zu mindern (45%); unternehmenskritische IT-, IoT- und OT-Workloads – zunehmend einschließlich KI-gestützter Anwendungen (42%); und Unvorhersehbarkeit bei Clients (40%).

Diese Komplexität hat konkrete betriebliche Auswirkungen: 46 % berichten, dass ihr Team mindestens 50 WLAN-Support-Tickets pro Woche erhält, was bedeutet, dass

IT-Teams Hunderte von Stunden pro Monat mit der Verwaltung von WLAN-Tickets verbringen können.

Ein Bereich, der besorgniserregend ist, ist die reaktive Haltung, die typischerweise aus dieser Komplexität entsteht. 59% verbringen den Großteil ihrer Zeit mit reaktiver Fehlerbehebung und Incident Management. Das bedeutet, dass proaktive Arbeit, einschließlich strategischer Projekte, Schulungen, Zertifizierungen und Netzwerkoptimierung, in den Hintergrund tritt.

Ein kritischer Faktor, der diese betriebliche Herausforderung verschärft, ist ein Mangel an Transparenz. 89% der Unternehmen berichten von Transparenzlücken, die ihre Fähigkeit zur effektiven Fehlerbehebung bei WLAN-Problemen beeinträchtigen. Die am häufigsten gemeldeten Herausforderungen betreffen schlechte Anwendungs- und Cloud-Transparenz, Client-Transparenz und Pakettransparenz.

Ohne lückenlose Transparenz können Teams Probleme nicht schnell isolieren. Dies trägt zu einer besonders gefährlichen Dynamik bei: WLAN-Netzwerke werden zum Sündenbock für Probleme, die anderswo entstehen, wobei 64% der Befragten berichten, dass mehr als 10% der Vorfälle fälschlicherweise dem WLAN zugeschrieben werden.

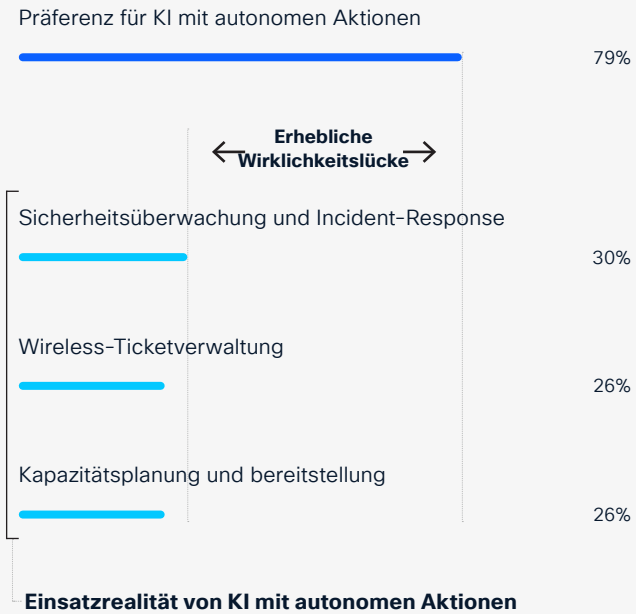
Angesichts der zunehmenden KI-gestützten Unternehmenstransformation glauben WLAN-Verantwortliche überwiegend, dass KI die vielversprechendste Lösung ist, um diese immer komplexeren Herausforderungen zu überwinden. Die Vorteile sind erheblich und messbar, einschließlich bedeutender Zeiteinsparungen, Vereinfachung des Netzwerkbetriebs und schnellerer Ticket-Bearbeitungszeiten.

Allerdings besteht in Deutschland eine erhebliche Lücke zwischen dem gewünschten und dem tatsächlichen Einsatz von KI-Fähigkeiten für WLAN. Die Präferenz für KI mit autonomen Aktionen liegt bei 79%, während die Einsatzrealitate deutlich darunter liegt.

94% haben Transparenzlücken, darunter:

Schlechte Anwendungs-/ Cloud-Transparenz	43%
Schlechte Client-Transparenz	41%
Schlechte Pakettransparenz	41%

Die KI-Lücke: Wunsch versus Wirklichkeit



Hindernis 2: WLAN-Sicherheit unter Beschuss – IoT-Ausbreitung trifft auf KI-gestützte Bedrohungen

Die WLAN-Sicherheit stellt das zweite kritische Hindernis dar, das Unternehmen in Deutschland daran hindert, das KI-Paradoxon aufzulösen und einen starken WLAN-ROI zu erzielen. Unternehmen können WLAN nicht zuversichtlich als Plattform für unternehmenskritische Workloads einsetzen, wenn sie mit eskalierenden Sicherheitsbedrohungen und steigenden finanziellen Verlusten konfrontiert sind.

79 % der Unternehmen in Deutschland haben in den letzten 12 Monaten mindestens einen WLAN-Sicherheitsvorfall erlebt. 39% berichten von einer Eskalation der WLAN-Bedrohungen in den letzten zwei Jahren und sagen, dass diese häufiger, schädlicher und schwieriger zu erkennen und zu bewältigen geworden sind.

WLAN-Verantwortliche nennen KI-generierte oder automatisierte Cyberangriffe am häufigsten unter den Top-3-Treibern erhöhter Cybersicherheitsbedrohungen im WLAN-Bereich. Diese Bedrohungen können Netzwerkschwachstellen identifizieren, Angriffstrategien basierend auf Abwehrmaßnahmen anpassen und in einem Maßstab und mit einer Geschwindigkeit operieren, die die Fähigkeiten menschlicher Angreifer bei Weitem übertreffen.

Die Angriffsfläche für Unternehmen in Deutschland nimmt weiter zu. 32% der von Vorfällen Betroffenen berichten von Unterstörungen durch kompromittierte IoT- oder OT-Geräte, was eine erhebliche Bedrohung für WLAN darstellt, da dies die häufigste Konnektivitätstechnologie für IoT ist.

Die finanziellen Auswirkungen dieser Sicherheitsvorfälle sind erheblich. 49% der Unternehmen in Deutschland haben finanzielle Verluste durch WLAN-Sicherheitsvorfälle erlitten. 57% berichten von Verlusten, die im vergangenen Jahr 1 Million US-Dollar übersteigen.

Wichtigste Faktoren für ein erhöhtes Bedrohungsniveau für WLAN-Netzwerke

KI-generierte oder automatisierte Cyberangriffe / automatisierte Eindringungstools	33%
Remote- und hybride Arbeitsmodelle, die die Angriffsfläche / nicht verwaltete Endpunkte erweitern	25%
Zunehmendem Einsatz von IoT und vernetzten Geräten (rasantes Gerätewachstum)	25%
Mangel an qualifiziertem Personal oder Kapazität zur Überwachung und Reaktion auf Bedrohungen	25%
Begrenzte Netzwerk- und Anwendungstransparenz	23%

Unternehmen in Deutschland verlieren aufgrund von WLAN-Sicherheitsvorfällen mehr als Geld. 37 % haben einen Verlust des Kundenvertrauens erlebt, während 29% mit regulatorischen Sanktionen oder Compliance-Konsequenzen konfrontiert waren, was zeigt, dass die Auswirkungen weit über direkte Vorfallskosten hinausgehen.

Dennoch hat die Mehrheit der Unternehmen bisher Vertrauen in ihre WLAN-Sicherheit behalten. 80 % berichten, dass ihr Unternehmen ausreichend zum Schutz der WLAN-Netzwerke unternimmt, obwohl auch 77 % erwarten, dass WLAN-Sicherheitsversagen in den nächsten zwei Jahren zunehmen werden.

Hindernis 3: WLAN verliert den Wettbewerb um KI-Fachkräfte

Talente stellen das dritte Hindernis dar und schaffen zusammen mit betrieblicher Komplexität und zunehmenden Sicherheitsbedrohungen einen Katalysator, der Unternehmen daran hindert, den WLAN-ROI zu skalieren.

Talentmangel verlangsamt nicht nur die Modernisierung; er verstärkt direkt den betrieblichen Druck und die Sicherheitsrisiken, während er die Implementierung von AIOps erschwert. Dies trägt zu einem Teufelskreis bei: Unternehmen, denen Talente fehlen, sind langsamer bei der Modernisierung, Komplexität und Sicherheitsrisiken eskalieren, Kosten steigen, und die besten Talente verlassen das Unternehmen zugunsten modernerer Organisationen.

89% der Unternehmen in Deutschland berichten von Schwierigkeiten bei der Einstellung, wobei IT-Talente andere, sichtbarere Technologiebereiche wie KI und Cybersicherheit priorisieren. Dies führt zu einer Qualifikationslücke, die sich in höheren Betriebskosten (34%), niedrigerer Moral (29 %) und reduzierter Innovation (26%) niederschlägt.

Die Talentekrise offenbart die miteinander verbundene Natur des WLAN-KI-Paradoxons. Ohne KI in den Kern des WLAN-Betriebs zu integrieren, werden Unternehmen weiterhin Talente verlieren. Ohne die Talente wird es schwieriger, strategische Projekte wie die Sicherheitsmodernisierung umzusetzen. Ohne moderne Sicherheit steigen die Kosten für Vorfälle, was es schwieriger macht, sowohl in Talente als auch in Technologie zu investieren.

Diese zusammengesetzte Dynamik erklärt, warum Unternehmen alle drei Hindernisse gleichzeitig angehen müssen, um dem Paradoxon zu entkommen.

KI verknüpft mit WLAN-Talent-Abwanderung und Qualifikationsmängeln

Rangierung unter den Top-3-Bereichen, die Talente vom WLAN abziehen

Cybersicherheit	50%
KI / Maschinelles Lernen	46%
Software-Engineering / App-Entwicklung	36%

Primäre Gründe für Einstellungsschwierigkeiten bei WLAN-Talenten

Mangel an Kandidaten mit fortgeschrittenen WLAN- oder KI-integrierten Fähigkeiten	40%
Interne Budget-Einschränkungen oder Einstellungsstopp	32%
Geografische Einschränkungen oder Herausforderungen durch Remote-Arbeit	31%

Methodik

Diese Forschung umfasste Interviews mit 6,098 Organisationen in 30 Märkten, darunter 302 Organisationen in Deutschland. Die Forschung wurde im November 2025 von Sandpiper Research and Insights durchgeführt.

Forschungsumfang

Profil der Befragten: Interviews wurden mit 6.098 WLAN-Entscheidungsträgern und technischen Spezialisten in Organisationen mit mindestens 250 Mitarbeitern durchgeführt. Sechs von zehn (61 %) Befragten arbeiten in Organisationen mit einem Jahresumsatz von mindestens 100 Millionen US-Dollar.

Amerika — 22%

Europa, Naher Osten und Afrika — 28%

Asien-Pazifik — 50%

Geografische Abdeckung: Die Forschung umfasste 30 Märkte, darunter Australien, Brasilien, Kanada, Festland-China, Frankreich, Deutschland, Hongkong, Indien, Indonesien, Italien, Japan, Malaysia, Mexiko, Niederlande, Neuseeland, Philippinen, Polen, Saudi-Arabien, Singapur, Südafrika, Südkorea, Spanien, Schweden, Schweiz, Taiwan, Thailand, Vereinigte Arabische Emirate, Vereinigtes Königreich, Vereinigte Staaten von Amerika und Vietnam.

Branchenvertretung: Die Befragten arbeiteten in verschiedenen Branchen, darunter Unternehmensdienstleistungen, Bauwesen, Bildung, Ingenieurwesen, Design und Architektur, Finanzdienstleistungen, öffentliche Verwaltung und öffentliche Dienste, Gesundheitswesen, Fertigung, Medien und Kommunikation, Naturressourcen, Immobilien, Gaststättengewerbe, Einzelhandel, Technologiedienstleistungen, Transport, Reisedienstleistungen und Großhandel.

Zeitpunkt: Die Forschung wurde im November 2025 durchgeführt.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices