Securing **AI** at the endpoint

Why 5G belongs in your enterprise AI discussions.

This Omdia eBook and the research contained therein were commissioned by Verizon Business.

verizon

Table of contents

Securing AI at the edge

Enterprise AI is no longer a pilot project: 89% of organizations now have active AI initiatives, and the majority often access those tools over networks that IT does not control.

Network connectivity is a functional prerequisite for most enterprise AI activity. As AI tools become embedded in daily operations, accessed predominantly through browsers, productivity suites, and cloud-integrated workflows, the network carrying that traffic has become even more important.

For employees working outside managed environments, that network–public Wi-Fi, shared access points, hotel connections, or client sites–is frequently uncontrolled and typically underperforms. The question facing enterprise IT is no longer whether AI is being used but whether the network supporting that use is adequate and whether it is secure.

87%

agree that reliable, high-speed connectivity is critical to maximizing AI investments

97%

say that employee access to AI tools while they are mobile is important; 41% say it is critical

95%

are concerned about security risks posed by network access from outside the office

The connectivity dependency

Enterprise AI access is predominantly network dependent: 51% of organizations access AI via browser-based applications. Integrated productivity suites account for most of the rest. Each requires a live, secure network connection. For the majority of workloads, network quality is a direct determinant of both performance and security posture: 87% of IT leaders agree high-speed connectivity is essential to maximize AI investments.

The network-layer risk

When employees access cloud AI tools over public or semi-managed networks, data traverses infrastructure that is neither owned nor controlled by the IT department. IT leaders identified data exposure over unsecured networks as their greatest AI security concern, ahead of model reliability and compliance. However, 5G addresses this by relocating network security to the carrier layer: managed in fleet, auditable through logs, and enforced by policy.

Work beyond the perimeter

Enterprise AI has made network quality urgent, and 74% of IT leaders say mobile AI access is important to their strategy, yet mobile workers routinely operate under connectivity that the IT department does not control, whether at client sites, transit locations, or temporary workspaces with shared, bandwidth-capped, or absent guest networks.

1

The enterprise AI landscape creates security challenges

AI is operational, cloud dependent and exposed

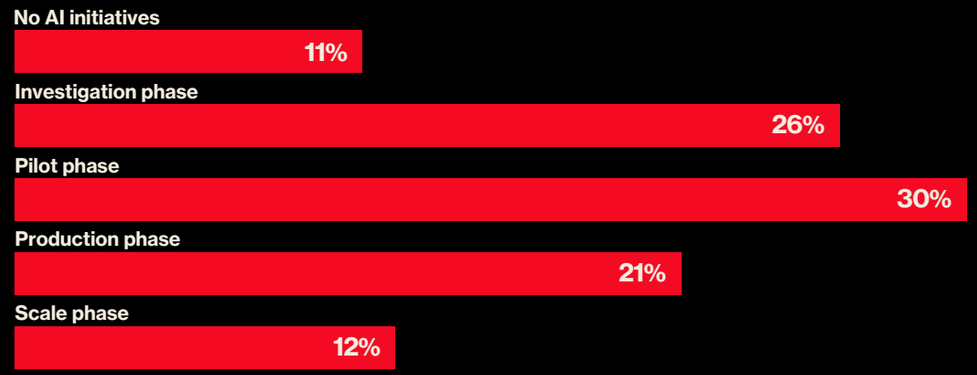
Eighty-nine percent have active AI initiatives, and 65% of workloads are cloud or hybrid, meaning the majority require a live, secure network connection at all times.

Omdia's survey reveals organizations selecting a variety of AI workload types across data analysis, security, productivity, and more. The majority are cloud or hybrid, and even on-premises deployments rely on cloud services for model updates, training data synchronization, and API calls to external AI platforms.

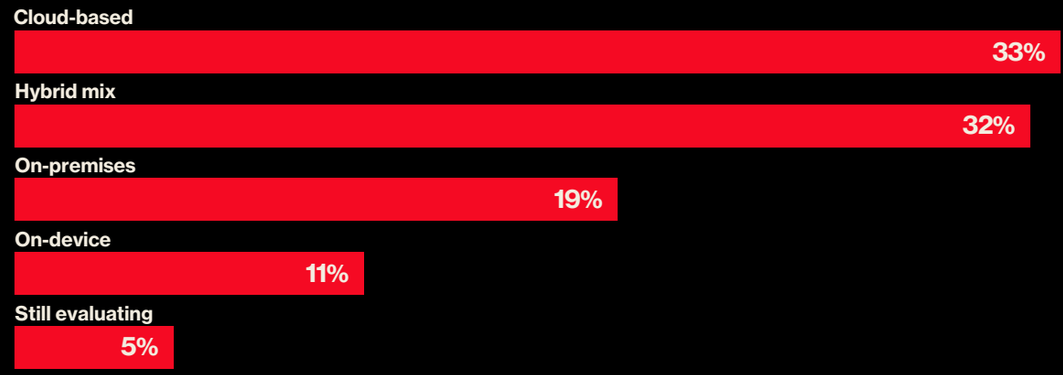
The connectivity dependency runs deeper than the workload infrastructure chart suggests: Nearly every deployment model involves live network traffic carrying sensitive organizational data. AI is no longer confined to specific teams. It is ambient, woven into productivity suites, collaboration platforms, and the operating system itself. When AI is everywhere, the network carrying AI traffic is everywhere too.

The majority of enterprise AI workloads run in cloud or hybrid environments, meaning nearly every deployment requires a live, reliable, and secure network connection to function.

Which best describes your organization's AI maturity?



AI workload infrastructure



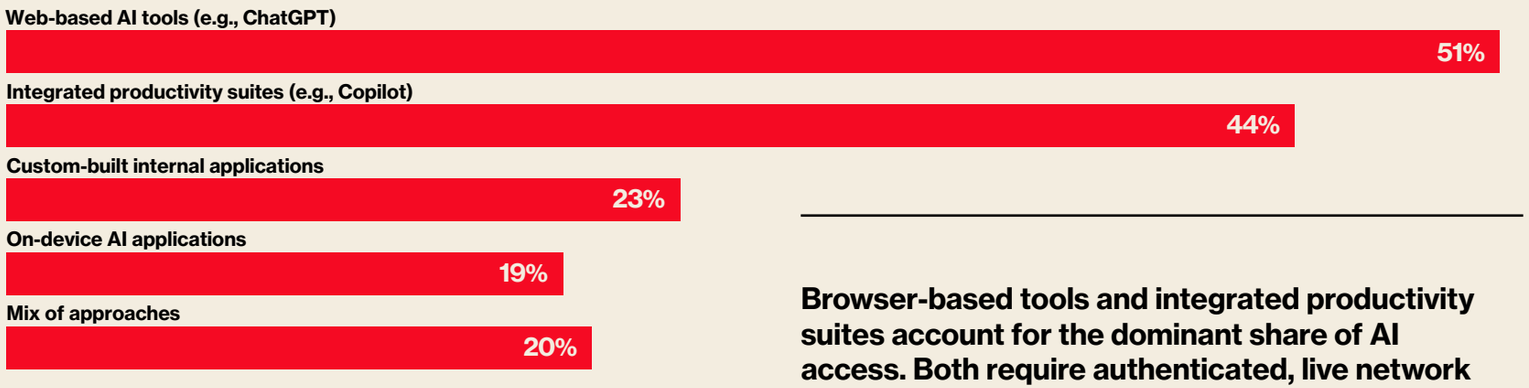
Where AI workloads live

Understanding where AI workloads execute is essential for infrastructure planning because the deployment model determines the connectivity requirement.

The two most common ways employees interact with AI–browser-based tools and integrated productivity suites–are both inherently cloud connected. When an employee uses a web-based chatbot or an AI feature in their productivity suite, that request traverses a network. The proprietary data it contains travels from the device to a cloud endpoint and back across whatever network the device happens to be connected to.

The top always-on use cases–analytics dashboards and real-time collaboration tools–are bandwidth intensive and latency sensitive. As AI usage scales from occasional to persistent, the frequency with which sensitive data travels across networks grows proportionally.

How do employees typically access AI tools at your organization?
(Select all that apply)



Browser-based tools and integrated productivity suites account for the dominant share of AI access. Both require authenticated, live network connections, making the quality and security of that connection a direct factor in AI performance.

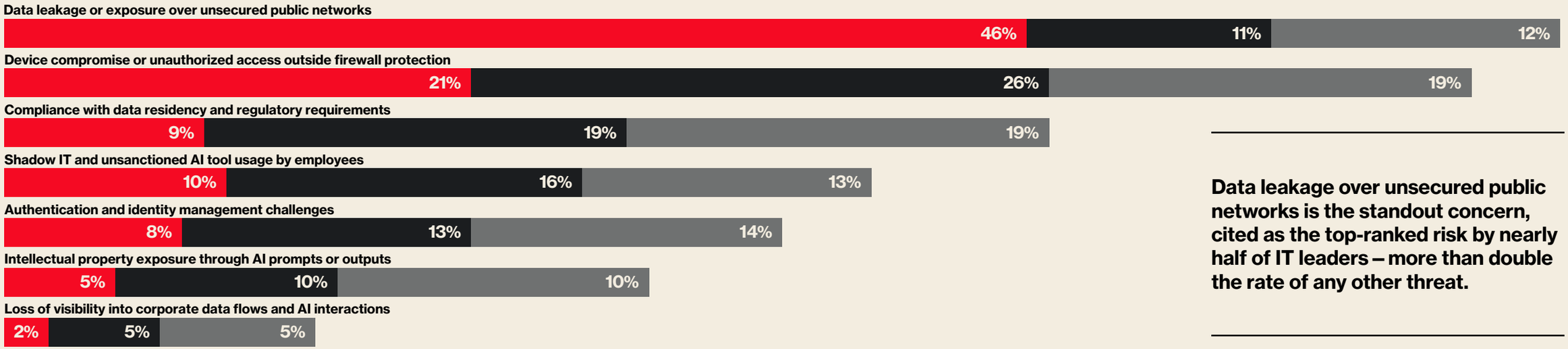
The security gap: Data leakage over public networks is the No. 1 concern

Sixty-one percent are satisfied with remote connectivity performance, but 95% are concerned about security outside the office. Current solutions meet the functional bar but not the security bar.

IT leaders point to two dominant fears: data leakage over unsecured public networks and device compromise or unauthorized access outside the corporate firewall. These priorities are reflected in spending: Security and compliance rank as the top criteria for both AI infrastructure budgets and laptop refresh decisions.

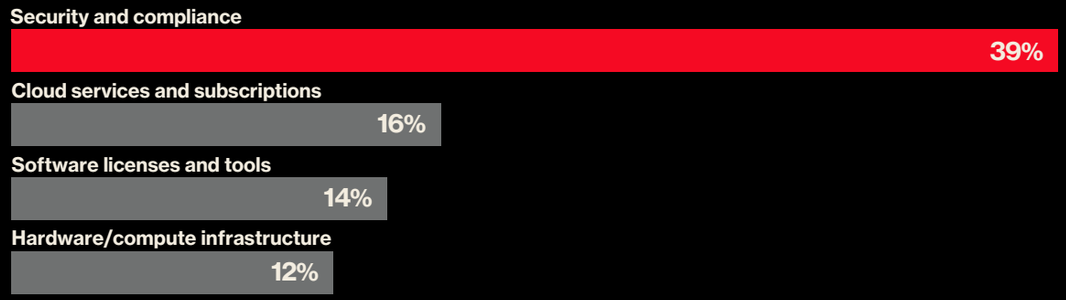
Both threat vectors are directly addressed by 5G-enabled laptops. Embedded cellular connectivity bypasses risky public networks entirely, significantly reducing data leakage risk at the source. Persistent cellular management allows IT to remotely monitor, manage, or wipe devices anywhere, closing the device compromise gap that exists beyond the corporate firewall.

Rank your top three security concerns when employees use AI-powered tools outside the corporate network

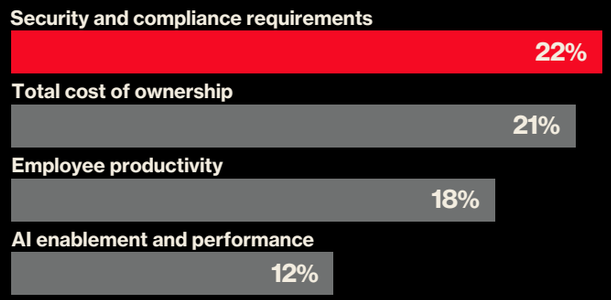


Data leakage over unsecured public networks is the standout concern, cited as the top-ranked risk by nearly half of IT leaders – more than double the rate of any other threat.

AI infrastructure priorities



Laptop refresh priorities



Security and compliance lead investment priorities for both AI infrastructure and laptop refresh decisions. Organizations are making a single, integrated decision guided by strategic priorities.

Security tops every investment priority

Thirty-nine percent rank security and compliance as the No. 1 priority for AI infrastructure investment. Half cite regulatory compliance as “very important” in evaluating connectivity solutions.

Concern about data leakage translates directly into budget allocation. Security and compliance dominate both AI infrastructure investment and laptop refresh priorities, ranking first in both conversations. Organizations are not making two separate purchasing decisions; they are making a single set of investment decisions in which security and AI are inextricably linked. A laptop refresh that addresses both security posture and AI capability is responding to the same underlying concern from two angles.

Enterprises evaluate connectivity through a governance and compliance lens. Performance metrics matter, but compliance comes first.

The unmanaged network problem

AI workloads do not stop at the office door and neither should your connectivity.

Client site
Guest Wi-Fi with bandwidth caps and shared access

Hotel or Conference
Throttled connections, port restrictions, no enterprise encryption

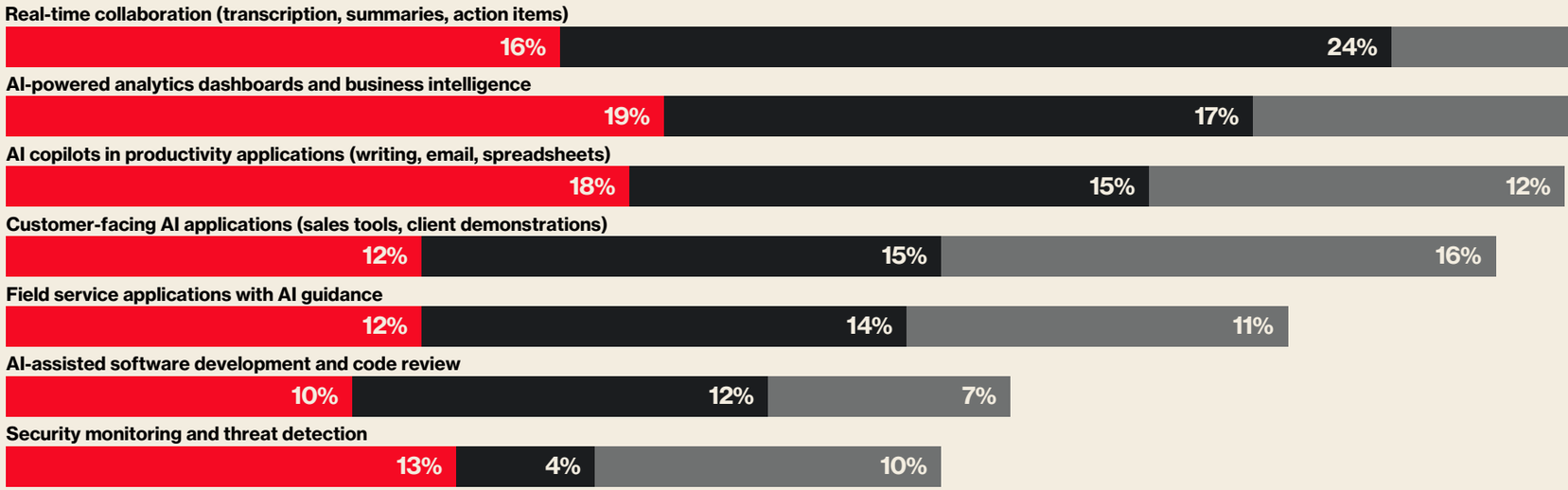
Airport or in-transit
Open public network shared with thousands of unknown devices

Coffee shop or coworking
Unsecured, unmanaged, and shared with the public

Industrial site
No Wi-Fi or sparse connections

Outpatient visits
Guest Wi-Fi, no enterprise encryption

Which AI-powered applications in your organization would benefit most from always-available connectivity?



Real-time collaboration and AI-powered analytics dashboards are the top two use cases requiring always-available connectivity, together accounting for the largest combined share of rankings.

Rank 1 Rank 2 Rank 3

5G solves some security concerns and complements others

Using 5G connectivity consolidates hotspot management, VPN overlays, and ad hoc Wi-Fi dependencies into a single, IT-managed connection.

Network layer

What 5G handles

Capability	Detail
Carrier-grade encryption	Data never traverses an unmanaged access point
Fleetwide IT-managed connectivity	MDM policies extend to cellular connections regardless of location
Auditable connection logs	Every connection is documented, which is critical for regulated industries
Always-on failover	Automatic switch from Wi-Fi to cellular when connectivity drops or degrades
Mobile device management extensions	Remotely monitor, manage, or wipe capability anywhere with a cellular signal

Application layer

What works better alongside 5G

Capability	Detail
Endpoint security	Device-level protection, threat detection, and response
Data loss prevention	Monitoring and controlling data movement across applications
Zero-trust network access	Identity-based access policies regardless of location
AI governance and policy enforcement	Controlling which AI tools employees can use and how
Identity and access management	Authentication, authorization, and session controls

2

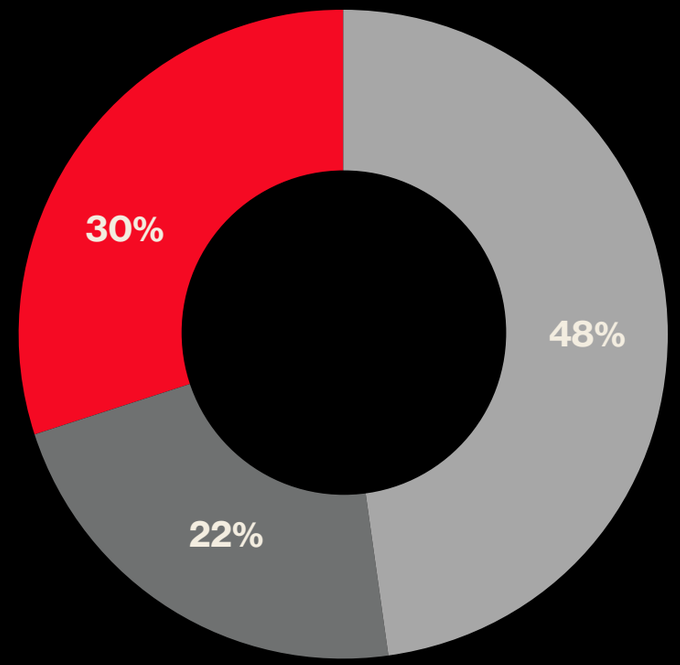
Unlocking the device you already own

52% of enterprises are already equipped to make use of 5G

Though 52% of enterprises already have 5G-capable laptops in their fleet, only 30% have activated them with a carrier plan. The other 22% have the technology sitting dormant.

The conversation about 5G laptops often defaults to a procurement question. For many organizations, that question has already been answered, but no follow-up action has been taken to activate the 5G capability. Cellular-enabled laptops are a growing share of enterprise PC shipments, and OEMs are accelerating the shift. If your organization has refreshed any portion of its laptop fleet in the past two to three years, some of those devices likely already have 5G hardware built in.

The hardware decision and the activation decision should be treated as fundamentally separate strategic choices. One is a capital investment in optionality. The other is an operational expense tied to demonstrated value.



What distinguishes organizations that are getting value from 5G

Activated and nonactivated organizations look almost identical on paper. Company size is virtually the same; industry distribution differs only modestly. What separates activators is how they approached the decision, not who they are.

Pragmatism is the strongest signal. Activators are 21% more likely to rank cost-effectiveness among their top evaluation criteria–focused on measurable outcomes, not theoretical benefits. Satisfaction follows activation. This is not a selection effect: They have better connectivity because they activated.

Most importantly, activators have undergone a conceptual shift around security from “worried about security” to “using connectivity for security.” The question is not “Are we the right type of organization?” but “Are we willing to pilot, measure, and decide based on evidence?”

Pragmatism

Activators are 35% more likely to rank total cost of ownership as a top laptop evaluation criterion.

Activators consider the comprehensive cost and ROI implications. TCO’s top ranking signals confidence that the return offsets the cost, not a willingness to spend more.

Satisfaction

Enterprises with no 5G laptops report dissatisfaction with connectivity at nearly double the rate.

Poor connectivity is a real operational problem for organizations with Wi-Fi-only fleets. Satisfaction with their connectivity is nine percentage points higher among those that have activated 5G laptops.

Security as capability

Activators are 49% more likely to identify security monitoring as something connectivity should enable.

Both groups worry about security equally, but activators have moved further. Instead of treating connectivity as the thing to be secured, they treat it as the thing that does the securing.

Identifies specific roles

Activators identify the specific job functions where 5G provides the most value.

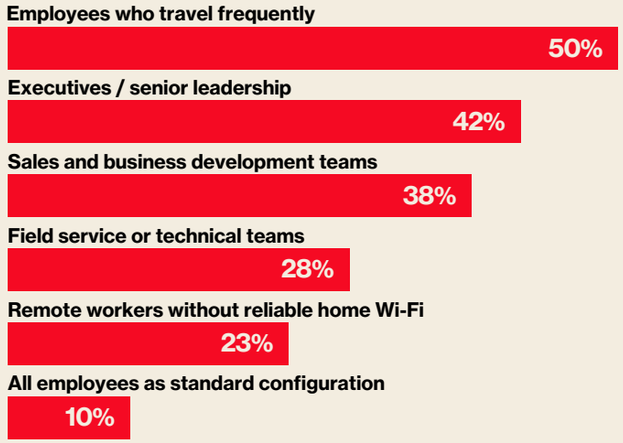
Activators are 47% more likely to see executive leadership as a 5G use case.

5G drives the most value in key job roles

Only 10% believe 5G should be standard for all employees. Value concentrates in roles combining mobility, cloud AI dependency, and sensitive data exposure.

Dimension	What it means	High-fit signal
Connectivity necessity	Constant access to cloud applications and collaboration tools throughout the day	Uses browser-based AI, cloud analytics, or SaaS productivity tools as primary work method
Physical mobility	Regular movement to locations without managed Wi-Fi	Spends two or more days per week at client sites, branches, field locations, or patient homes
Sensitive data exposure	Handles regulated data, client IP, or confidential information where public Wi-Fi creates compliance risk	Works with PII, PHI, financial data, legal documents, or proprietary client information
Cloud AI tool utilization	Active use of cloud-based analytics, CRM, AI decision support, or generative AI	Relies on AI-powered dashboards, copilots, diagnostic tools, or research platforms

Where 5G-active organizations are targeting deployment



Deployment is targeted, not universal: Frequent travelers and executives together account for the majority of activated use cases, reflecting a role-by-role approach focused on where mobility and data sensitivity intersect.

3

Industry perspectives

Healthcare: scale, mobility and high-stakes data

Healthcare presents one of the clearest cases for 5G-enabled connectivity, not because of any single statistic but because mobility, data sensitivity, and AI adoption uniquely intersect in this vertical.

The healthcare workforce operates across a wide spectrum of mobility patterns. At one end, administrative staff work from fixed locations. At the other, home health workers and community health workers spend their days in locations where enterprise networks do not exist. The CDC reports approximately 4.5 million home health visits annually in the US, each representing a clinical interaction where patient data must be accessed and transmitted from wherever the clinician happens to be.

Our survey data shows 52% of healthcare organizations are in a pilot phase or beyond for AI. However, healthcare's barriers to 5G activation differ from those of other verticals: The cost of data plans (41%) and unclear ROI (35%) rank highest.

5G connectivity can support these compliance efforts by providing encrypted transport for data in transit, but it does not by itself satisfy the full scope of obligations under HIPAA or applicable state privacy regulations. Clinical and operational teams should work with qualified legal and compliance professionals to assess how connectivity solutions interact with their specific regulatory requirements.

More than 3 million Americans receive home health care each year.[1]

1: https://www.cdc.gov/nchs/fastats/home-health-care.htm

Financial services: compliance, client visits and regulatory urgency

Financial services arrives at the same 5G conclusion as healthcare via a different path. The workforce is overwhelmingly deskbound, and the 5G use case targets the mobile minority: client-facing advisors, traveling portfolio managers, claims adjusters, and relationship bankers whose roles take them outside managed Wi-Fi environments.

What distinguishes financial services is the severity of data sensitivity and the regulatory framework. PCI DSS, SOX, and SEC regulations require documented security controls over data in transit. A financial advisor reviewing a client's portfolio using AI-powered analytics at a coffee shop is not just creating a security risk: They are creating an audit exposure.

PCI DSS 4.0 is now enforced, extending compliance requirements to home and remote environments, including home Wi-Fi networks. Carrier-managed 5G provides a path to compliance that does not depend on an employee's home broadband infrastructure.

Carrier-managed connectivity can strengthen the documented security controls that PCI DSS 4.0, GLBA, and SEC frameworks require over data in transit, but it does not constitute full regulatory compliance in itself. Financial services organizations should engage qualified legal and compliance counsel to determine how cellular connectivity fits within their specific compliance architecture.

PCI DSS 4.0 is now enforced, extending compliance requirements to home and remote environments, including home Wi-Fi networks.

Professional services: client-site connectivity gaps and IP protection

Professional services is defined by a single structural reality: extended, deep engagement at client sites where the firm controls nothing about the network. The management consultant embedded Monday through Thursday, the auditor working onsite for weeks during busy season, and the IT consultant deploying systems at a client facility for months, every one of these engagements creates a dependency on whatever connectivity the client provides: guest Wi-Fi with bandwidth caps, restricted ports, limited or no VPN passthrough, and shared access with every other visitor in the building.

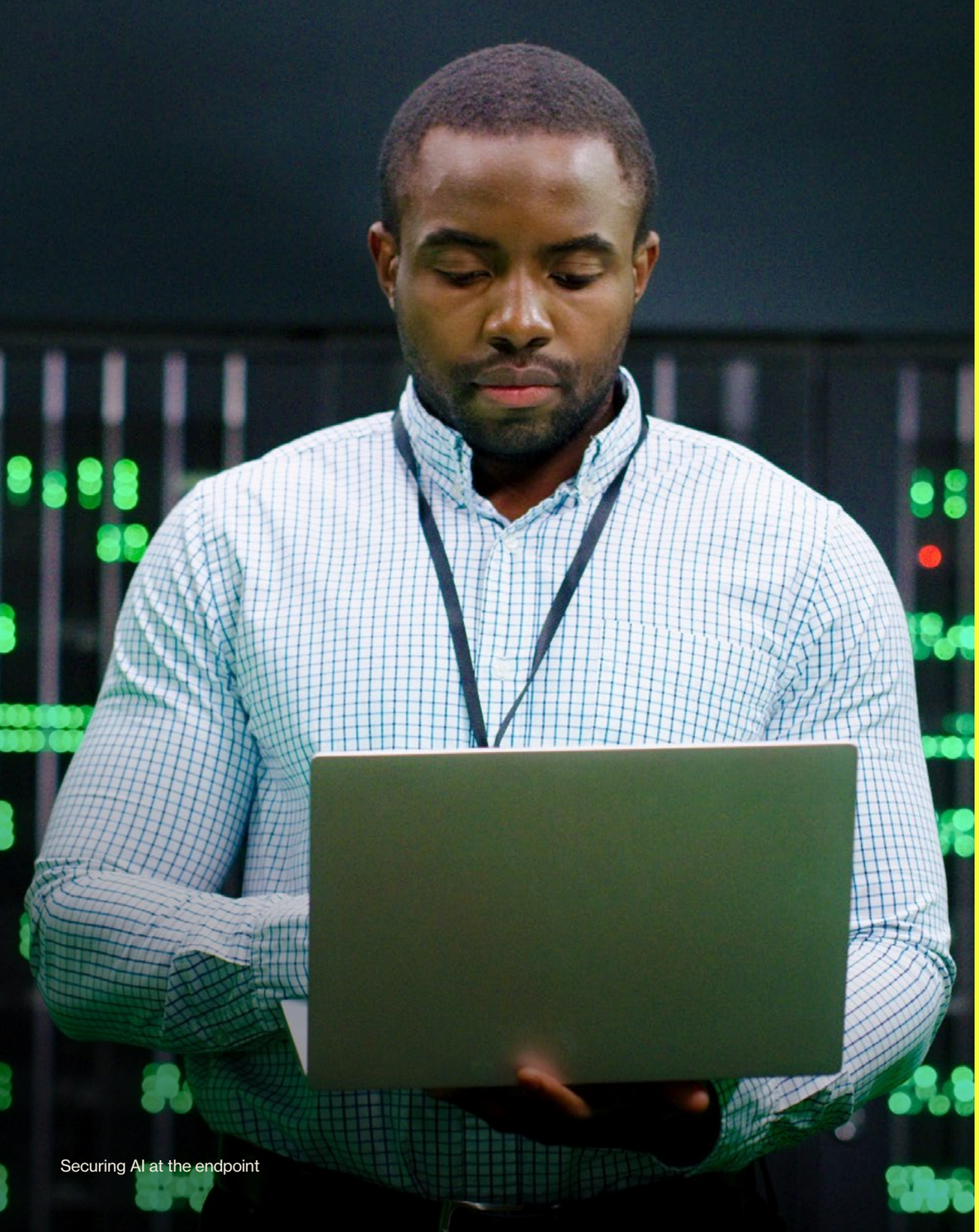
Professional services firms are also rapidly adopting generative AI for document analysis, research synthesis, and case analysis. When a consultant pastes a client's privileged information into a consumer AI tool, the firm creates not just a data breach but a potential breach of attorney-client privilege or professional confidentiality obligations. The architecture simplification argument is sharp: Handle network-layer security through the carrier, eliminate dependency on client infrastructure, and focus security resources on AI governance.

For professional services firms, 5G connectivity can reduce the network-layer exposure created by client-site and remote working, but connectivity alone does not resolve confidentiality obligations, privileged information considerations, or data protection requirements that vary by jurisdiction and engagement type. Firms should assess their specific obligations with qualified legal and compliance professionals.

A midsize consulting firm with 500 consultants, each averaging 150 client-site days per year, generates 75,000 days annually on which sensitive client data is accessed over networks the firm does not control.

4

Clearing the path to 5G: practical steps for enterprise IT



Simplifying IT deployment

Managing cellular connectivity adds provisioning, MDM integration, and cost-allocation workflows. But the share of enterprises citing this as a concern masks a clearer finding: Organizations that invested in zero-touch deployment, preconfigured MDM profiles, and carrier coordination before rollout report satisfaction levels comparable to those seen with Wi-Fi management.

These are provisioning and configuration challenges, exactly the kind of operational work that IT teams handle routinely when onboarding any new endpoint capability. The playbook is well established and mirrors what IT teams already do for any fleetwide capability rollout.

Zero-touch deployment
Carrier-coordinated provisioning; devices arrive preactivated

MDM integration
Preconfigured profiles via Intune or Workspace ONE, cellular policies alongside Wi-Fi/VPN

Cost visibility
Usage dashboards for departmental allocation and plan optimization

Enterprise support tier
Dedicated carrier support for cellular troubleshooting, not consumer helplines

76%

prioritize IP protection in their AI strategy. Because 5G handles your most automatable security problem, it simplifies this, freeing up your team for the problems that cannot be automated.

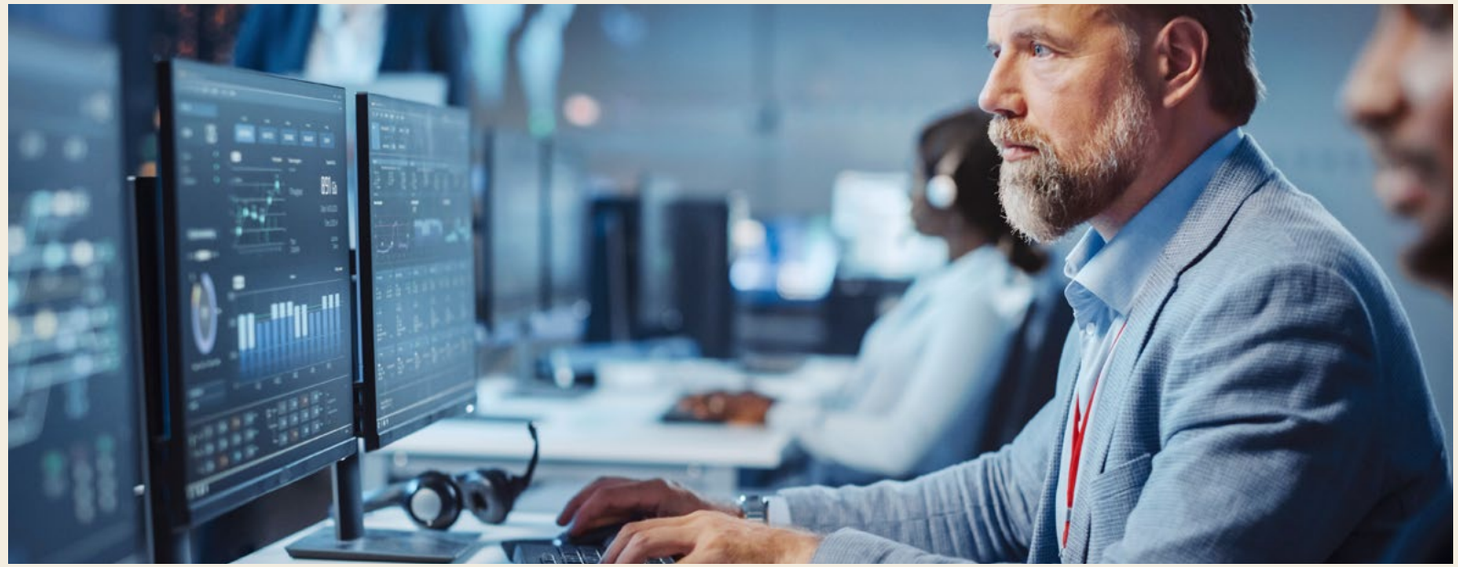
The security architecture advantage: Focus your team where it matters

Enterprise AI security has two layers: network and application. With 5G, the network layer is handled by design, freeing your security team to focus on the application-layer challenges that require human judgment.

The more consequential AI data leakage vector is the application layer, such as employees pasting sensitive data into consumer AI tools on personal accounts outside the purview of the IT department. A growing share of respondents already flag unsanctioned AI tool usage as a distinct risk, and the overwhelming majority prioritize IP protection in their AI strategy.

The gap between the scale of the behavior and the share of organizations tracking it suggests application-layer exfiltration is substantially undermeasured.

AI governance requires user awareness, policy enforcement, application-level controls, and comprehensive security policies. These are human challenges, not infrastructure challenges. Your security team should be spending its time on these, not worrying about whether the consultant at the client site is on a secure network.



Right-sizing the investment by matching connectivity to the workload

The most common hesitation around 5G activation is cost, but framing it as a fleet-level budget decision is what makes it feel expensive. Investments rarely start with a fleet-wide refresh; rather, the decision is typically made one role at a time.

Start with the roles where mobility, cloud AI dependency, and sensitive data exposure intersect. Frequent travelers, client-facing teams, and executives operating across locations without managed Wi-Fi are the natural first cohort. Among organizations with active 5G deployments, these are precisely the roles being prioritized, with universal fleet-wide rollout chosen by fewer than one in ten.

The Wi-Fi sufficiency argument deserves scrutiny before it closes the conversation. Among organizations that have activated 5G, a third still describe Wi-Fi as sufficient, yet they activated anyway. The reason is that “sufficient” only describes environments where Wi-Fi is available and well-managed. It says nothing about the 39% of working situations where it is not.

A phased approach resolves the cost question in practice. Activate for the highest-fit roles first, define success metrics upfront – connection uptime, security incidents, user satisfaction – and measure against a matched Wi-Fi-only control group over 90 days. That evidence base is more persuasive to a budget holder than any fleet-wide projection, and it lets the investment scale only where it is demonstrably earning its place.

Before concluding that Wi-Fi is sufficient, pressure-test these assumptions:

1

Do employees access AI or productivity tools from locations without managed Wi-Fi?

2

Have you received connectivity complaints from employees who travel or visit external sites?

3

Do mobile employees use public Wi-Fi for work, and is that acceptable under your security policy?

4

How much productive time is lost in the gaps between managed Wi-Fi environments?

5

Does your current VPN/ hotspot solution create compliance gaps or user friction for mobile/hybrid roles?

5

Evaluating 5G for your enterprise

Evaluating 5G for your enterprise

Audit

- Review device inventory for built-in cellular capability.
- Identify 5G-capable laptops not yet activated.
- Map dormant capability against active carrier plans.

Identify

- Score the workforce against four dimensions: connectivity dependency, physical mobility, sensitive data exposure, and cloud AI dependency.
- Prioritize roles where all four intersect.

Pilot

- Deploy activated 5G laptops to the highest-fit roles.
- Define success metrics upfront: security incidents, connectivity tickets, user satisfaction, and productivity benchmarks.
- Compare against a matched Wi-Fi-only control group.

Measure and scale

- Evaluate the pilot cohort versus the control group on measurable outcomes.
- Build the internal business case with real performance data.
- Expand role by role with quarterly review gates.
- This will be more persuasive to budget holders than enterprise-wide projections.

6

Summary

Why connectivity is the missing piece in enterprise AI security

Enterprise AI is operational and almost entirely network-dependent. 89% of organizations have active AI initiatives. The majority of workloads run in cloud or hybrid environments, and the two dominant access methods – browser-based tools and integrated productivity suites – both require a live, authenticated connection to function.

The enterprise security stack has hardened at the endpoint and application layers. Identity controls verify who is connecting. Endpoint detection monitors the device. DLP watches what moves through applications. But between the device and the cloud, the default for mobile and remote workers is often public Wi-Fi, guest networks, or home broadband – infrastructure IT neither owns nor controls.

95% of IT leaders are concerned about security risks from outside the office. Nearly half rank data leakage over unsecured public networks as their single greatest AI security concern – more than double the rate of any other threat. Security and compliance top the investment priority list for both AI infrastructure and laptop refresh decisions.

5G-enabled laptops address this at the architectural level. Carrier-grade encryption operates before any application-layer control comes into play. IT-managed connectivity travels with the device regardless of location. Every session is logged, auditable, and governed by the same MDM policies that cover the rest of the fleet.

Many enterprises already have some dormant 5G-capable laptops. The hardware decision has been made. The activation decision is what remains.

Learn about Verizon's 5G activation solutions.
verizon.com/laptops

This Omdia eBook and the research contained therein were commissioned by Verizon Business.

verizon