Executive Summary

verizon

Securing **AI** at the endpoint

Why 5G belongs in your enterprise AI discussions.

Enterprise AI is operational, cloud dependent, and increasingly accessed over networks that IT does not control

Organizations have invested heavily in cloud platforms, endpoint security, and zero-trust architectures, yet **nearly half of IT decision makers rank data leakage over unsecured public networks as their primary AI security concern**, more than double the rate of any other threat. With 89% of enterprises having active AI initiatives, a majority of AI workloads operate in cloud or hybrid environments, and the two dominant access methods–browser-based AI tools, used by 51% of organizations, and cloud productivity suites, used by 44% require live, authenticated connections to function. The question is no longer whether connectivity matters to AI security but whether enterprises have made connectivity a deliberate part of their security posture.

89% **of enterprises have active AI initiatives**

The risk is largely unacknowledged. Connectivity is rarely flagged as a barrier to AI adoption, yet 87% of IT leaders describe it as critical to AI success, and 97% say access to AI tools while mobile is important or critical. This gap suggests connectivity has been treated as a background utility rather than a deliberate security variable, even as the risks of unmanaged networks have grown. This gap reflects how **connectivity has been treated as a background utility rather than a security variable.** The enterprise security stack has hardened at the endpoint and application layers through data loss prevention (DLP), endpoint detection and response (EDR), and identity controls, but the network layer between device and cloud remains a shared medium in most deployment models. **When employees access AI tools over public Wi-Fi, guest networks, or home broadband, that traffic operates outside enterprise visibility and encryption standards.**

87% **of enterprises say connectivity is critical to AI**

This gap is addressed directly by 5G-enabled laptops. **Carrier-grade encryption operates at the network layer, reducing dependency on individual user behavior** or application-level configuration for transport-layer security. IT-managed connectivity provides centralized provisioning, policy enforcement, and auditable session logs, significantly reducing reliance on public Wi-Fi, hotel networks, and home broadband as default access points. This is not a replacement for endpoint or application security: It is an additive control that operates below those layers. When a clinician accesses an AI diagnostic tool from a patient's home, or a financial analyst queries a cloud model from a client office, **5G is designed to encrypt, authenticate, and log the network connection before data reaches the endpoint security stack.** The relationship is complementary: Zero-trust validates identity and device posture; DLP monitors data movement at the application layer; 5G secures the pipe.

Security concerns dominate every related investment decision. When asked specifically about AI infrastructure investment priorities, 39% rank security and compliance

73% **of enterprises rate regulatory compliance as important when evaluating laptop connectivity solutions**

as their top consideration, and 72% place it in their top three, higher than performance, cost, or scalability. The same pattern holds for what criteria are considered most when refreshing laptops: **56% identify security and compliance requirements as a top criterion for laptop refresh.** Regulatory compliance ranks first among the factors considered when connectivity solutions for laptop fleets are being evaluated: 73% rated it important. In regulated industries, this pressure is tangible and growing. PCI DSS 4.0 has extended compliance obligations to home Wi-Fi environments. In the US, the Health Insurance Portability and Accountability Act (HIPAA) requires documented security controls over patient data regardless of where it is accessed. Legal and financial services firms face increasing scrutiny over data transmitted outside managed networks. **Security has shifted from a defensive posture to a design requirement for enterprise AI**, and connectivity is the variable that most organizations have not yet addressed.

The dormant hardware gap and the activation decision

52% **of enterprises already have 5G-capable laptops**

52% of surveyed enterprises already deploy 5G-capable laptops, but only 30% have activated carrier plans. The 22 percentage point gap represents capability sitting dormant: hardware purchased, provisioned, and distributed without the connectivity service that makes it functional. This is not a procurement failure but reflects the structural separation between hardware refresh cycles and service activation decisions. Laptops are replaced every three to four years in fixed budget cycles. Cellular activation is a monthly operating expense, deployed role by role, with pricing that varies by plan and deployment scale and is fully reversible without hardware replacement. The current refresh cycle makes this decision time sensitive. **Organizations specifying 5G capability now preserve optionality for the next three to four years.** Those that do not specify it will be locked out of the option until the next hardware cycle.

Activated and nonactivated organizations are demographically identical: same size distribution, same industry mix, same AI adoption rates. The difference is operational, not strategic. Activators are:

21% more likely to rank total cost of ownership as a top evaluation criterion.

49% more likely to cite security monitoring as a postactivation use case.

9 percentage points more likely to report connectivity satisfaction than nonactivators (67.4% versus 58.3%).

Deployment patterns are targeted, not universal. Half of activators prioritize frequent travelers, and 42% focus on executive roles. Only 9% pursue fleetwide rollout. Security has shifted from barrier to use case: Activators treat 5G as a monitoring and compliance tool, not just a backup connection. One of the most commonly cited causes of friction is IT management complexity (27% of respondents), and that share rises with deployment experience, making upfront MDM integration and zero-touch provisioning essential to a smooth rollout. In practice, **embedded 5G simplifies the connectivity picture rather than complicating it**: It consolidates external hotspots, tethering arrangements, and ad hoc Wi-Fi dependencies into a single carrier-managed connection, provisioned via the same MDM profiles IT teams already use.

The activation pathway is structured in decision gates, not commitments. A fleet audit (two to three weeks) identifies existing 5G-capable hardware and maps it to user roles and mobility patterns. Role identification (two to three weeks) prioritizes high-exposure roles: frequent travelers, remote executives, field staff, and regulatory-sensitive functions. A 90-day pilot deploys 30 – 50 devices, representing 10 – 15% of the eligible fleet, with defined success metrics: connection uptime, security incident reduction, user satisfaction, and help desk volume. Phased scaling follows only if pilot metrics justify expansion, and quarterly decision gates are tied to cost per secured connection and measurable risk reduction. This is a controlled connectivity layer added to the existing security stack, activated where risk and mobility intersect and scaled only where the economics and operational evidence support it.

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

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

verizon