Infographic

Securing **AI** at the endpoint

Why 5G belongs in your enterprise AI discussions.

Network connectivity is a functional prerequisite for by far the greatest part of enterprise AI activity. The 2026 Omdia Securing AI at the Endpoint Report is based on a survey of 438 companies that gauges how they are deploying AI, securing it, and connecting to it and what the growing gap between AI adoption and network security means for enterprise IT strategy.

Check out these highlights from the report.

52%

of enterprises already have 5G-capable laptops

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%

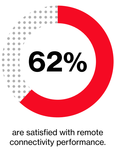
are concerned about security risks posed by network access from outside the office.

70%

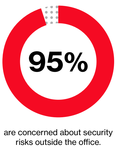
access AI via browser-based tools or integrated into productivity suites.

Satisfied with speed, terrified about security

Connectivity is critical for AI, yet the networks supporting it are often unmanaged and insecure.



are satisfied with remote connectivity performance.



are concerned about security risks outside the office.

Current solutions meet the functional bar but not the security bar

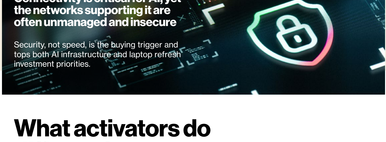
Top security concerns when employees use AI outside the corporate network

46%

Data leakage or exposure over unsecured public networks is the greatest concern organizations have when employees use AI tools outside the corporate network.

21%

A device being compromised through unauthorized access (e.g., lost or stolen) is the second-greatest concern of organizations.



Connectivity is critical for AI, yet the networks supporting it are often unmanaged and insecure

Security, not speed, is the buying trigger and tops both AI infrastructure and laptop refresh investment priorities.

What activators do differently

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, including the operational savings from consolidating hotspots and external modems, as well as tethering into a single carrier-managed connection. TCO's top ranking signals confidence that the return offsets the cost, not a willingness to spend more.

Satisfaction

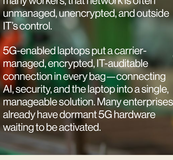
Enterprises with no 5G laptops report dissatisfaction with connectivity at nearly double the rate.

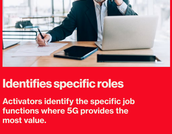
Poor connectivity is a real operational problem for organizations with Wi-Fi-only fleets. Satisfaction with their connectivity is nine percentage points higher among those that have activated 5G laptops.

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.



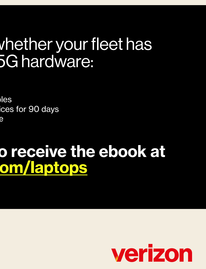


Identifies specific roles

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.

Summary



The connectivity layer AI depends on Enterprise AI runs on the cloud. The cloud runs on the network. For many workers, that network is often unmanaged, unencrypted, and outside IT's control.

5G-enabled laptops put a carrier-managed, encrypted, IT-auditable connection in every bag—connecting AI, security, and the laptop into a single, manageable solution. Many enterprises already have dormant 5G hardware waiting to be activated.

Find out whether your fleet has dormant 5G hardware:

- Audit your fleet
- Identify high-fit roles
- Pilot 30 – 50 devices for 90 days
- Scale on evidence

Sign up to receive the ebook at verizon.com/laptops

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

verizon