EINPRESSWIRE

# TuxCare Releases 2025 Enterprise Linux and Open Source Landscape Report

PALO ALTO, CA, UNITED STATES, February 25, 2025 /EINPresswire.com/ -- TuxCare, a global innovator in cybersecurity, today announced the release of its 2025 Enterprise Linux and Open Source Landscape Report. The second annual report aims to capture the preferences, behaviors, opinions and predictions of those who work with Enterprise Linux every day.

TuxCare

Throughout Q4 2024, TuxCare researchers gathered data from 293 participants that use Enterprise Linux in their organization. More than two thirds of respondents, most of which held technical roles, had more than 101 employees in their organization and operated between 10 and 500 Linux servers. The majority of respondents represented the industrial/manufacturing, IT/technology, and public sector fields. Full survey demographics are available within the report.

To explore the insights generated from this research, download the complete 2025 Enterprise Linux and Open Source Landscape Report here: https://tuxcare.com/downloadables/enterprise-linux-opensource-landscape-report/.

TuxCare’s researchers highlight the following three significant trends this year:

Unaligned Perceptions Surrounding Vulnerabilities
Security professionals’ perceptions do not align with the real-world threat landscape: When asked about vulnerability volumes compared to 2023, the responses followed an almost perfect normal distribution: approximately 24% believed vulnerabilities increased compared to last year, 50% said they remained stable, and 25% perceived a decrease in vulnerabilities. However, reality tells a drastically different story. Data from Mitre shows approximately 25% more vulnerabilities in 2024 compared to 2023. Even more alarming, Linux-specific vulnerabilities saw a staggering twelve-fold increase, jumping from 290 to 3,559, largely due to kernel CNA developments.

Reason for AI Adoption

Organizations are looking to AI increasingly for cost reduction, and less so for innovation. What organizations are using AI for is changing. A significant shift in primary objectives is noted, with cost-reduction goals increasing from 35% to 53%, while innovation-focused implementations have declined. The transition mirrors the historical evolution of cloud computing, suggesting AI is moving from a transformative technology to a practical business tool. The shift doesn't necessarily indicate diminishing AI effectiveness. Rather, it suggests organizations are developing more realistic expectations and measuring success through more concrete, business-oriented metrics.

Falling Confidence in Supply Chain Security

Confidence in supply chain security has plummeted from 23.81% to 12.31%. Paradoxically, 7% of organizations without formal security processes still report high confidence in their security posture – potentially a dangerous manifestation of the Dunning-Kruger effect in cybersecurity. Potentially most telling is the dramatic retreat from full automation in security processes, dropping from 14.48% to 2.56% – suggesting a growing recognition that, while automation is powerful, human oversight remains essential.

In addition to the most notable findings above, the report covers the following critical areas in detail:

- Trends in Enterprise Linux distribution and cloud services
- Linux patch and vulnerability management
- CrowdStrike incident impacts
- XZ incident causes of exposure
- Open source supply chain security
- Plans and status of AI adoption

"This year's 62-page Enterprise Linux and Open Source Landscape Report once again provides uniquely detailed insights surrounding Enterprise Linux users, highlighting among numerous other findings that a clear discrepancy exists between the perception of vulnerability levels compared to actual threats that are out there," said Michael Canavan, Chief Revenue Officer at TuxCare. "The report's numerous other findings also paint a picture of an open source and Enterprise Linux space that's experiencing ongoing innovation and disruption alongside ongoing security challenges."

About TuxCare

As organizations grapple with rising vulnerabilities and increasingly complex security challenges, TuxCare's rebootless patching, end-of-life security coverage, and enterprise support services provide a critical layer of protection by ensuring rapid remediation of vulnerabilities without downtime or disruptions.

TuxCare is on a mission to reduce the world's risk of cyber exploitation, enabling thousands of organizations to rapidly remediate vulnerabilities for increased security and compliance. The world’s largest enterprises, government agencies, service providers, universities, and research institutions are protected by TuxCare on over one million workloads and growing.  For more information, go to https://tuxcare.com.

DeShea Witcher
TuxCare
marketing@tuxcare.com