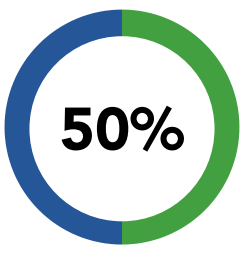
AI Security Benchmark 2026

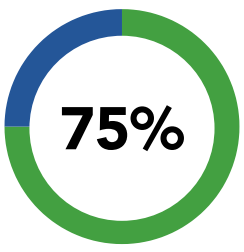
The **2026 AI Security and Exposure Benchmark** highlights crucial insights from 300 surveyed U.S. Chief Information Security Officers. Many organizations face significant barriers, **especially limited visibility** into their AI environments and reliance on outdated security tools.

67%

Limited visibility into AI ecosystems remains a major challenge for organizations, complicating effective security measures and risk management.



Cite **lack of expertise** as a barrier



Are relying on **legacy security tools**

75%

of US enterprises experienced **an attacker** inside their environment

$2.48M

Average yearly spend on cybersecurity

A staggering number of businesses report experiencing cyberattacks, with a notable average spending of **$2.48 million** annually on cybersecurity measures. By focusing on enhancing expertise and adopting innovative solutions, organizations can better secure their AI assets and thrive.

100%

While 100% of enterprises have **some** AI adoption, only 18% have managed to implement it on an enterprise-wide basis, reflecting significant gaps in deployment.

11%

Enterprises with dedicated AI security tools

18%

Percentage of enterprise-wide AI deployment

The **disparity between AI adoption and implementation** underscores the need for organizations to strategize effectively. A concerted focus on enterprise-wide deployment can enhance visibility and security, ensuring that AI functionalities are both robust and secure, ultimately reinforcing the overall cybersecurity posture.

corsica technologies

corsicatech.com | 855-411-3387

Source: https://corsicatech.com/blog/what-the-ai-security-exposure-benchmark-2026-reveals-about-your-risk-%F0%9F%92%A1/