QSC 24

Navigating Security Challenges of Large Language Models with AI Asset Visibility and Model Scanning

Nayeem Islam
Vice President, Product Management

Rijul Nirwal
Product Manager, TotalAI

Agenda

01 LLM Adoption

02 Current Challenges

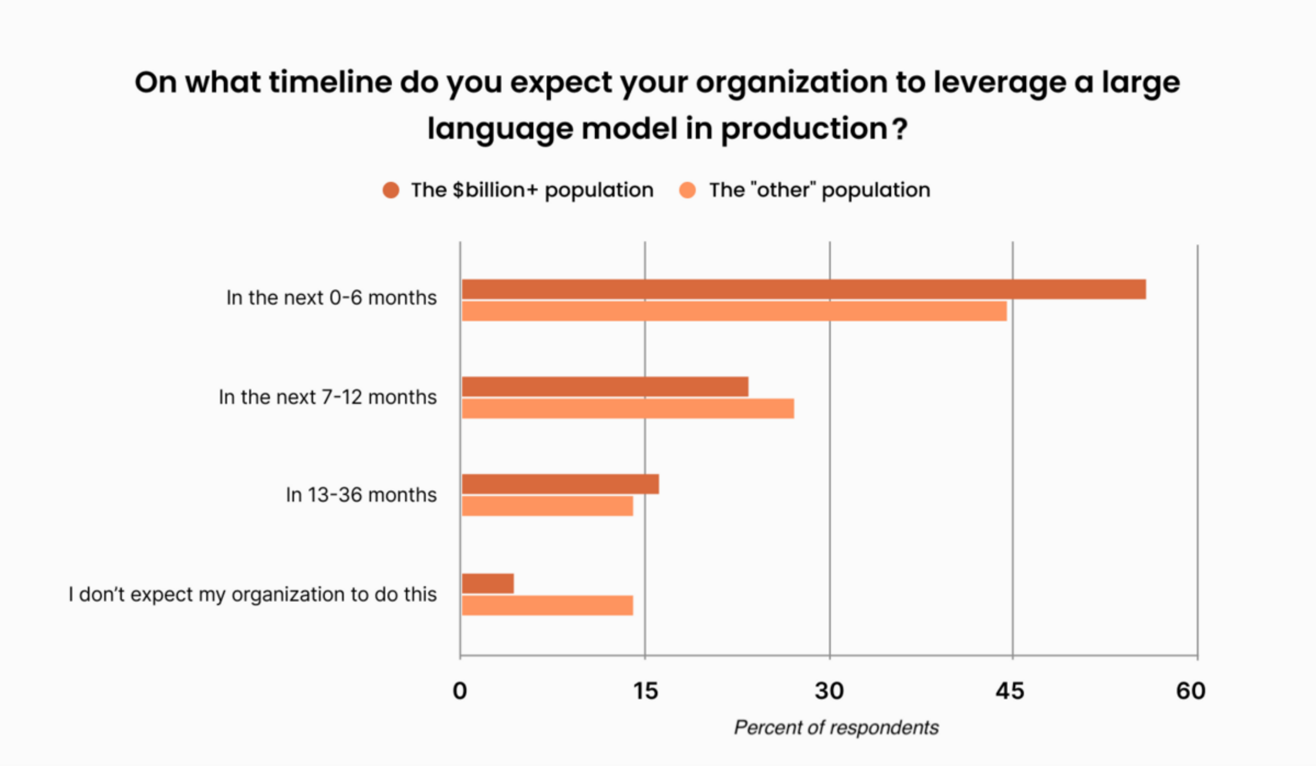
03 Introducing: Qualys LLM security

04 Benefits and Business Outcomes

05 Demo

LLM Rapid Deployments

70% of Enterprise want to deploy LLM in production in next 12 months



snorkel.ai

Respondents from $billion+ companies: 68
Other respondents: 169

Blindsided: Most security teams are unaware of LLMs in their environment.

Overlooked risk: security teams struggle to keep pace, skipping detailed security reviews.

Lack Prioritization: there is no good way to prioritize risk across security tools.

Enterprise Building and Leveraging AI and LLM

Used Internally by Enterprise

Employees using LLM tools like ChatGPT, etc. and other AI-enabled SaaS productivity tools

Developers using other coding products with embedded LLM

Consumer of LLMs

Created for End Customer

AI / LLM tools **embedded in product** for their end customers

E.g., Qualys creates a LLM chatbot to summarize risk or asset information

Area of Focus

Creator of LLMs

Challenges

AI and LLMs bring incremental risks to an Enterprise

Increased Attack Surface

Attackers are targeting LLMs and AI infrastructure
to steal model (crown jewel) and training data (PII)

How do I get ahead of attackers?

Model and Data Loss

AI packages and AI infrastructure related CVEs can lead to data and model theft:

How to I discover and fix critical vulnerabilities in AI Infrastructure?

Low Security Maturity

LLMs often lack robust security measures, which can lead to compliance violations and fines

How can I test the model to understand risk?

Low Visibility

Security teams blindsided by their AI workloads and model?

Do I have models in my Infrastructure? Where are they running?

Security Silos

Too many tools, yet a lack of visibility

How can I get better ROI from my security investments?

LLM Security Challenges

Consequences of Security Gaps

Teams are forced to take unnecessary risk leading to unintended consequences

Data and IP Breach

Brand Reputation

Financial Cost

Introducing Qualys TotalAI

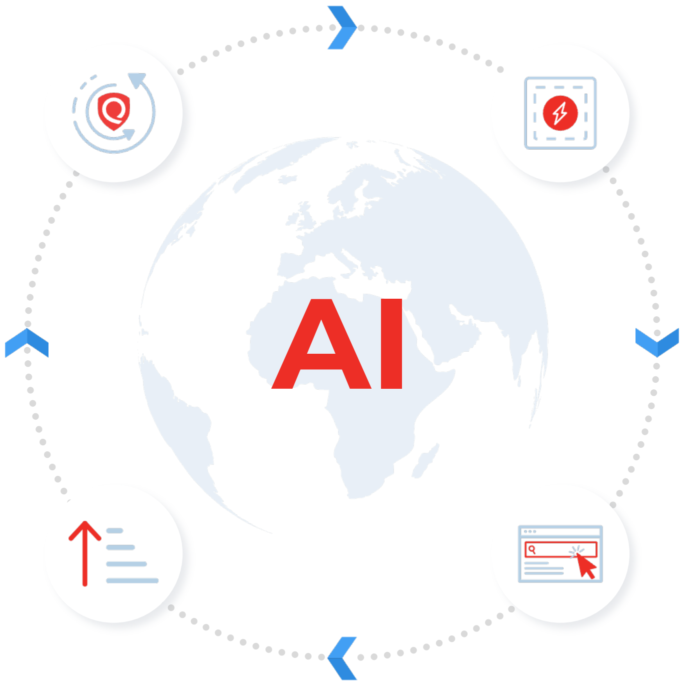
Single platform for a unified view of LLM risk, AI-Workloads, and AI-vulnerabilities

Complete Visibility Across Your Stack

- Discover all your AI-Workloads
- Get inventory of AI packages, AI-software and AI-hardware (GPUs)

Assess Your Models for Risk

- Scan LLM endpoints
- Prompt your LLMs for OWASP TOP 10 to ensure they are not leaking data, showing bias, or can be jailbreak



Vulnerability Assessment

- 1000+ AI-specific vuln detections correlated with threats for TruRisk
- Patch vuln risks to harden Infra from model and data theft

Reporting and Compliance

- Prevent fines due to compliance violations (e.g., GDPR, PCI)
- LLM security report for management

Leverages Existing Qualys Agent and Scanner

Qualys Risk Operations Center

Challenges with Status Quo

40%
Productivity increase is expected by application of Gen AI

71%
of IT leaders are concerned about vulnerabilities introduced by implementation of Gen AI

Top 3 privacy risks
are AI, brand reputation, and compliance

Measure and Prioritize Risk

Enterprise TruRisk™ Platform

- AI Asset Context
- AI Models
- Infrastructure
- AI Pipelines
- Cloud

500

Reassess Risk Score

Reduction of Risk

Drive Action

- Automated Patching of assets with AI fingerprint
- Host Isolation of vulnerable AI assets
- Mitigation Techniques for infrastructure & AI models
- Remediation Workflows

Customer Outcomes

Enterprise Visibility → Risk Prioritization → Risk Quantification → Reduction of Risk

Benefits

Discover, monitor, and reduce your LLM risks

Enhanced Visibility and Control

Complete visibility into your AI infrastructure. **Know where your AI models reside.**

Proactive Infrastructure Hardening

Continuously identify and prioritize real-time CVEs. **Prevent Model Theft and Data Loss.**

Prevent compliance fines

Regular model scans help ensure compliance with relevant data protection and privacy regulations. **Ensure your models are not leaking data.**

TruRisk

Risk Prioritization and Elimination

Prioritize risk across the AI-stack using TruRisk. **Remove security tool silos.**

Targeted LLM security

LLM-specific scans. **Focus on the most critical security risks specific to LLMs.**

Demo

Qualys®

Qualys TotalAI™

Secure Your AI

Discover AI Workloads, Prevent Theft, Data Leaks, and Compliance Risk!

01

Discover all AI and LLM

workloads, software, packages, GPUs.

02

Harden AI infrastructure

by detecting, prioritizing and remediating AI-specific vulnerabilities.

03

Assess LLMs

for model and data theft, prompt ingestion, and sensitive data exposure attacks.

qualys.com/totalai

Get Early Access to Qualys TotalAI and Your Custom AI Risk Report of Your Environment

DE-RISK YOUR **BUSINESS**

Qualys.

Thank You

Qualys®