digicert®

The Executive Guide to Trust in the Age of AI

AI changes everything. Trust must change, too.

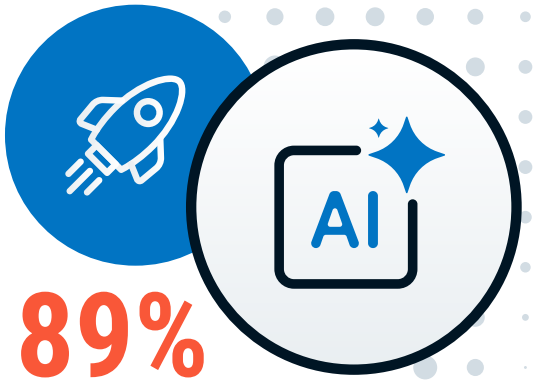
Artificial Intelligence is transforming the way organizations operate. But as AI systems proliferate, it is becoming clear that traditional security and governance frameworks were not created with AI in mind, and the enterprise attack surface is expanding at unprecedented speed.

AI agents operate at machine speed with limited oversight. AI models influence critical decisions. AI-generated content blurs reality. And most organizations are deploying AI faster than they can secure it.

Without trusted AI, organizations face growing risks to governance, compliance, operational resilience, and brand reputation. The AI trust problem has arrived.

To succeed in the AI era, leaders need confidence in the systems they deploy, the decisions those systems influence, and they content they create.

Today, trust cannot be assumed. It must be cryptographically verifiable.



89%

of C-level executives do not feel completely prepared for large-scale AI deployment[1]

Defining the new business risk

Without effective AI trust and governance, organizations face growing exposure across several critical areas: regulatory compliance, operational resilience, intellectual property protection, brand reputation, and financial performance.

These risks stem from a lack of visibility. **98% of organizations report some form of shadow AI[2]**—employees using unsanctioned AI in their work. The resulting breaches are more costly than traditional incidents and have a higher probability of exposing sensitive data. Yet many leaders lack a clear understanding of what AI systems are being used, what data is being shared, and what risks are being introduced.

Legal and liability risks are also growing. High-profile organizations have already faced lawsuits tied to AI-generated outputs, data usage practices, and algorithmic decision-making. As the risk landscape evolves, some insurers are even beginning to reevaluate or restrict coverage for AI-related claims.[3]

These risks share a common root cause: organizations often lack reliable ways to verify the identity, integrity, and provenance of the AI systems and content they depend on.

3
questions every executive should be asking about AI

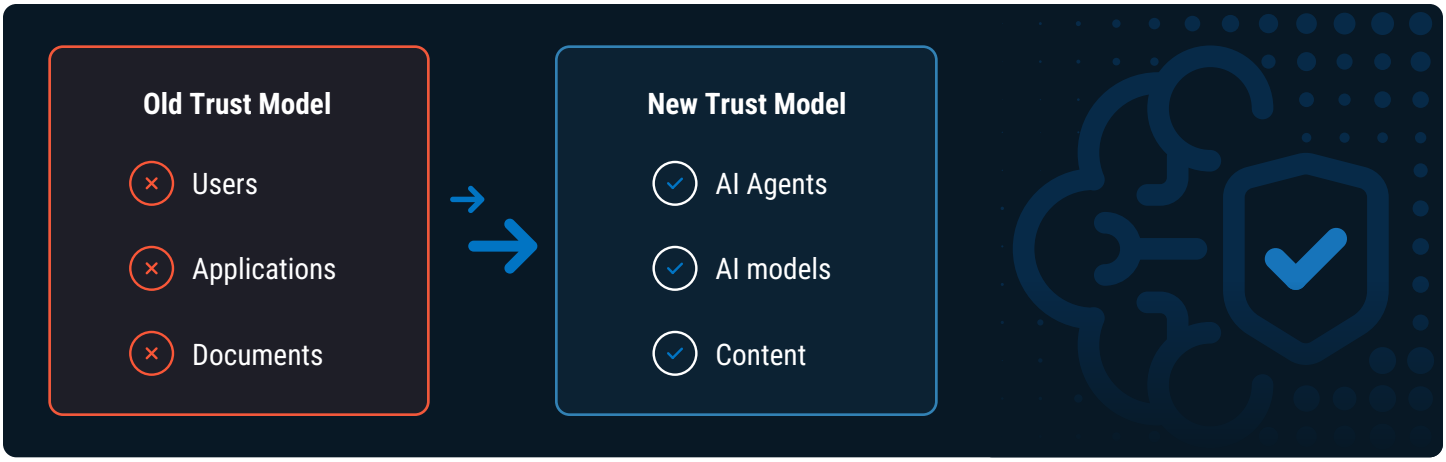
As leaders seek to manage these new risks, three key questions should guide every AI strategy:

- **Can we verify what our AI systems are doing?**
- **Can we trust the outputs AI creates?**
- **Can we prove governance and accountability when regulators ask?**

For many organizations, the answer to one or more of these questions is still no. Getting to yes requires a new approach to managing trust.

Managing AI risk with intelligent trust

Traditional security was built for human users, applications, and devices. As AI adoption accelerates, trust frameworks must extend to autonomous agents, AI models, and AI-generated content.



This new trust model must move from assumed trust to provable trust at scale.

This does not mean inventing new technologies but rather extending existing, proven trust principles to a new generation of AI systems. PKI, DNS, attestation, and cryptographic identity have secured the global internet at scale for decades.

This makes them the natural foundation to establish trust in AI systems and their outputs.

The key components of an AI trust strategy

To answer the three key questions outlined above, organizations need clear controls for identity, integrity, and provenance.

Identity	Integrity	Provenance
Identify the agents and systems that are acting, and provide authentication, authorization, governance, and lifecycle management for these new digital actors.	Ensure AI systems, models, and data remain trustworthy and unaltered, with controls that verify what is running, what has changed, and whether it can be trusted.	Establish a verifiable chain of custody for content, making it possible to understand where it originated, how it was created, and how it has changed over time.

AI Trust simplified

Identity verifies who or what is acting.

Integrity verifies that it can be trusted.

Provenance verifies where it came from.

Solving the AI trust problem

The organizations that will emerge as leaders in the age of AI will be those that can confidently solve the AI trust problem.

Success will be determined by an organization's ability to establish visibility, enforce policy, and demonstrate governance at scale.

The challenge is not whether organizations will adopt AI. It is whether they can do so in a way that is trustworthy, transparent, and verifiable. Building that foundation requires a trust architecture designed for AI systems, autonomous agents, and AI-generated content.

Dive deeper with DigiCert's full technical whitepaper:
The New Trust Architecture for AI

1. IBM https://www.ibm.com/thought-leadership/institute-business-value/en-us/c-suite-study/cxo
2. Varonis https://www.varonis.com/blog/shadow-ai
3. https://www.tomshardware.com/tech-industry/artificial-intelligence/insurers-move-to-limit-ai-liability-as-multi-billion-dollar-risks-emerge