

The

Blueprint:

Six Conditions

for

AI Acceleration



Visibility

A common mantra among CISOs is that they can't protect what they can't see. Visibility is a non-negotiable for effective security. Yet, according to Netskope data, an overwhelming 94% of enterprises report visibility gaps in their AI deployments, and only 9% can prevent a risky AI-driven action before it executes. Security leaders need to find ways to remedy this issue, tackling their shadow AI problem and improving their insight into vendor tools and supply chains.

Action 1

Start by removing the incentive to hide. Employees reaching for unsanctioned tools are usually trying to do their jobs, and treating them as adversaries only encourages concealment rather than compliance. The practical answer is to enable a authorized path that is genuinely usable, ideally consolidated onto a small number of platforms, with enforcement placed at the data layer. That way personal use remains possible, while corporate data cannot leave.

Action 2

Make the resulting visibility useful to the business, not just security teams. One organization issues monthly AI usage reports to a nominated ambassador in every team, helping them to understand what their own people are doing. Visibility becomes a service, and compliance follows.

Action 3

Accept that human review cannot keep pace. The volume of issues now being surfaced is far beyond what any team can triage manually, so automated detection is needed to help identify corrective actions at scale. As one CISO advised: "maybe it's actually AI that can help tackle the AI security problem."

"If you haven't provided a safe ecosystem or a contained environment for your employees to play with AI, it is highly likely they're off using it on the side with their own personal accounts."

– CISO, software, Australia

"Instead of treating employees as adversaries, provide coaching and guidance so that people know what the right decisions are."

– Steve Riley, Field CTO, Netskope

Governance

The governance framework and its related policies are where the security function sets out its intent. But the expectation that colleagues will read the governance documents and follow them carefully is under strain today, when AI adoption is distributed across the business and occurring at speed.

Action 1

Get policy off paper and embedded in products. Guardrails and harnesses can now have policies built in, to ensure security by design and reduce reliance on human workers to follow governance standards. As one CISO puts it, much of what sits in a policy document "...can be turned into machine language and actually embedded in the ecosystem". Security teams can also create a route for exceptions, so that an engineer who needs to vary a rule for a specific workload can request it.

Action 2

Establish a decision-making body between the business and the CISO. A cross-functional council that spans legal, privacy, vendor management, IT and the C-suite ensures all requests can find an answer, with a documented owner. That can be bolstered with named executive ownership for material use cases and quarterly board reporting on inventory, approved usage, exceptions and blocked actions.

Action 3

Make the governed route the fastest route. By pre-approving a small set of enterprise platforms, so anything inside them needs acknowledgment rather than assessment, security teams can focus their review effort on what is genuinely new. CISOs can also standardize what a review consists of, whether that's a fixed AI assessment questionnaire, independent penetration testing of vendor claims, or an external benchmark such as ISO 42001. They can do this by retaining evidence of the risk acceptance decision.

"We've been terrible in security, for forever and a day, around defining a security framework with a bunch of policies and standards, and expecting everyone to read them and know how to follow them."

– CISO, software, Australia

"We've formed a steering group with people from legal, ops, security and IT to review AI initiatives. That means we get diverse opinions at a time when the regulatory and security landscape is changing. So we get to hear from everyone and make informed decisions."

– VP Global Security, IT services, India

Controls

Until recently, controls were designed for humans. Now, AI agents create new vulnerabilities at machine speed. To be effective, modern controls must intervene inline, rather than simply logging what happened after the fact.

Action 1

Enforce at the data layer. Placing the control where data moves is what makes enforcement both inline and permissive at the same time. Security teams no longer need to block applications, so an employee can keep using their preferred service, but crucially corporate data cannot escape. This removes the main reason people route around security in the first place.

Action 2

Set and enforce boundaries for agents. Agents' actions must be evaluated before they execute, with a trust boundary set so that their remits are tightly bounded. As with human workers, it needs to be clear which action agents can perform, and on what data. Secure access service edge (SASE) or security service edge (SSE) frameworks should also help bring MCP traffic within existing security policies.

Action 3

Assume your controls will drift, and test them like an attacker. Currently most AI-related incidents can be traced back to a control that was set once and never checked. So each service needs to be monitored continuously, with controls adapted as it changes. One CISO has added what she calls a shift right to the more familiar shift left approach, pushing her team to "...act like a threat actor when it comes to AI and really try and break stuff," with a standing rule that anything found is fixed before an initiative goes live.

"AI is here and it's going to stay. It's not an external threat that CISOs need to chase. It's a constant variable they need to manage over time."

– CTO, IT services, Israel



Data protection

Part of AI's challenge to security teams is that it overturns the traditional approach to handling data. The most sensitive corporate information is now loaded into AI models deliberately, and comes back reshaped (and potentially polluted with hallucinations or poisoning). Security leaders must enforce modern data protection more rigorously.

Action 1

Approve the data, not the tool. Categorize your data first, then authorize each AI service against named data categories. That shifts the decision from whether a tool is permitted to what it's allowed to receive. Done well, this speeds up approvals, because a new use case for an approved service becomes a data question rather than a fresh review.

Action 2

Map data lineage before you trust output. CISOs should map data flows feeding each service, so they know where that data comes from and that it can be relied upon. This gives you greater confidence in AI outputs and the decisions made on the strength of a model's answer.

Action 3

Put retention and reuse in the contract; then verify it. Specify what a provider may retain, for how long, and whether your inputs may be used for training. Require independent testing rather than accepting self verification, and hold subcontracted fourth parties to identical obligations. These will need checking on a firm schedule, given how fast provider terms are changing. One security leader said he's seeing privacy policies at major providers change on a monthly basis.

"AI models require current, real data and struggle with synthetic data. They can create synthetic data sets for you, but it still means putting in your original crown jewels, so far as data is concerned."

– CISO, Australia

"Too many CISOs still frame their work around preventing intrusion when the real question for them today is preventing leakage through legit use. Because AI is legit. So it requires a conceptual shift, not just better tooling."

– CTO, IT services, Israel

Agent oversight

Security systems have been built on the assumption that every action has an identity behind it. From access rights to leaver processes, everything was attributed to a named human. But with the spread of AI agents, this approach breaks down. By the estimate of one CISO, in today's leading enterprises there can be 10 non-human identities for every human. This breaks down as AI agents gain greater access to collaboration tools, email, code repositories and identity systems.

Action 1

Give every agent its own identity, tied to the human who invoked it. Agents' credentials need to be tightly scoped, and ideally short-lived. CISOs should bind the agent identity to the person invoking it, so authorization can be evaluated as a single question about a specific human, agent, action and data. That blended identity combination helps bring agents inside the existing access model.

Action 2

Put agents through the joiner and leaver lifecycle. Agents are now being provisioned constantly but they are rarely decommissioned. Security teams must apply least privilege to agents, regularly review their entitlements, and terminate their access on the owner's final day, exactly as would happen with a normal user account.

Action 3

Supervise agents with agents, and record what they did. Human review cannot keep pace with autonomous activity. One option is to create security agents to monitor your other agents, acting as guardians over the wider environment. Each agent action should be logged so that incidents can be tracked and explained.

"The biggest thing many organizations are missing right now is identity for non-human actors."

– Steve Riley, Field CTO, Netskope

"It's a game of AI versus AI, with humans playing a critical role in the loop."

– VP Global Security, IT services, India

Confidence

If AI use is visible, governance is enforced, controls intervene inline, data is protected by category and agents are accountable, then approving a project becomes an evidence-based decision that CISOs can feel confident in. That's not the same as a risk-free approval, of course. But it ensures today's CISO can make recommendations to their CEO and board that increase business velocity and ultimately enable growth.

Action 1

Set minimum limits now and plan for continuous improvement in the future. AI is still a new and fast-evolving technology, so it's simply not possible to cover every eventuality right now. But CISOs can be clear about their baseline requirements for sensible security, while mapping out a plan to improve capabilities over time. As one CISO advises, it's important to get "really comfortable with being uncomfortable," yet commit to constant learning as this technology develops.

Action 2

Get the business to own the risk and put it in writing. CISOs should not be taking on the burden of risk acceptance for every tool and access request. Instead, they should present the risks plainly to the business stakeholder involved and ensure he or she understands the consequences. Putting the decision in writing provides confidence in the current process and future accountability.

Action 3

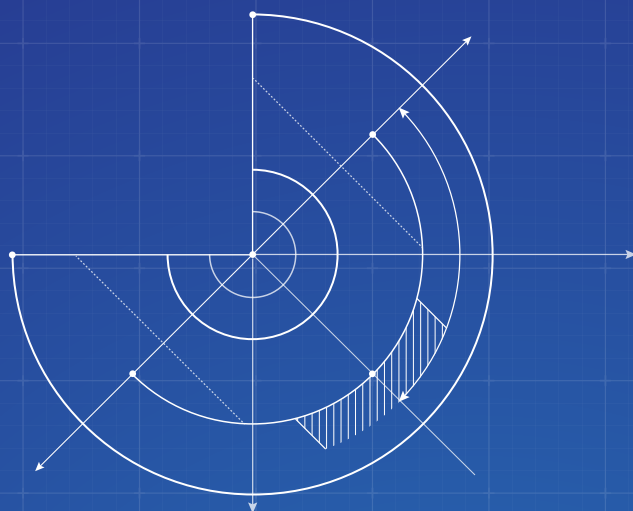
Report in business language. One of the best ways for the CISO to instill confidence in security decision-making is to give the board a small set of figures it can understand, framed within a compelling story and aligned to business goals. This could cover what has been approved, what has been blocked, what risk has been formally accepted and reduced, and what value that has enabled, perhaps on a quarterly rhythm. One experienced CISO urged his peers to "expand the skill set into softer skills like communication and storytelling."

"I can say yes to this project because I know that I've got visibility and control and governance in place."

– Steve Riley,
Field CTO, Netskope

About Netskope

Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for the AI ecosystem inclusive of agents, applications, tools, LLMs, people, devices, and data. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications, providing security and accelerating performance without trade-offs. Learn more at netskope.com, Netskope.ai, on [LinkedIn](#), and [Instagram](#).



©2026 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized "N" logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 09/26 RS-1026-1