TÜRKİYE AI SECURITY CISO SURVEY 2026

CRITICAL STEPS TO AI SECURITY

CISO CONNECT
An Exclusive CISO Platform

Methodology & How to use

Survey Scope & Participants

- The survey was conducted with **63 CISOs** from **CISO Connect**, an exclusive CISO platform built by **CISOs from Türkiye's largest enterprises**.
- Participants represent a broad and strategically critical cross-section of the Turkish economy, including **automotive, aviation, banking, energy, finance, fintech, FMCG, health, holding groups, insurance, logistics, online trade/e-commerce, retail, service providers, telecom and textile/apparel** sectors.

Survey Format

- Based on a **structured questionnaire** covering:
  - AI adoption & readiness
  - AI-related risks & threat landscape
  - Benefits and use cases of AI in security
  - Barriers, compliance challenges, and workforce impact
  - Strategic expectations for AI-augmented Security

Why This Survey Matters

- Provides the **most up-to-date view of AI adoption and AI risk perception** among Türkiye's largest enterprises
- Reflects the cybersecurity priorities of organizations representing **a major part of the country's enterprise-scale digital footprint**
- Highlights how Türkiye's largest companies are preparing for **AI-driven threats, compliance pressures, and SOC modernization**

How to Use These Insights

- Benchmark your organization's progress against the **largest CISO sample in the country**
- Guide **AI strategy, investment decisions, and risk management planning** for 2025–2026
- Inform board-level conversations on **AI governance, SOC transformation, and workforce readiness**

A Personal Thank You Note to Participating CISOs

A heartfelt thank you to all CISOs who generously contributed to this survey. Your contributions are invaluable — your insights and experiences form the foundation of this report, reflect the collective intelligence of Türkiye's leading CISOs and not only help us understand the current AI security landscape, but also shape the roadmap for our entire community.

CISO Connect is built by all of you, and this survey is yet another example of the strength of our collaboration.

I am truly grateful for your time, expertise, and ongoing support.

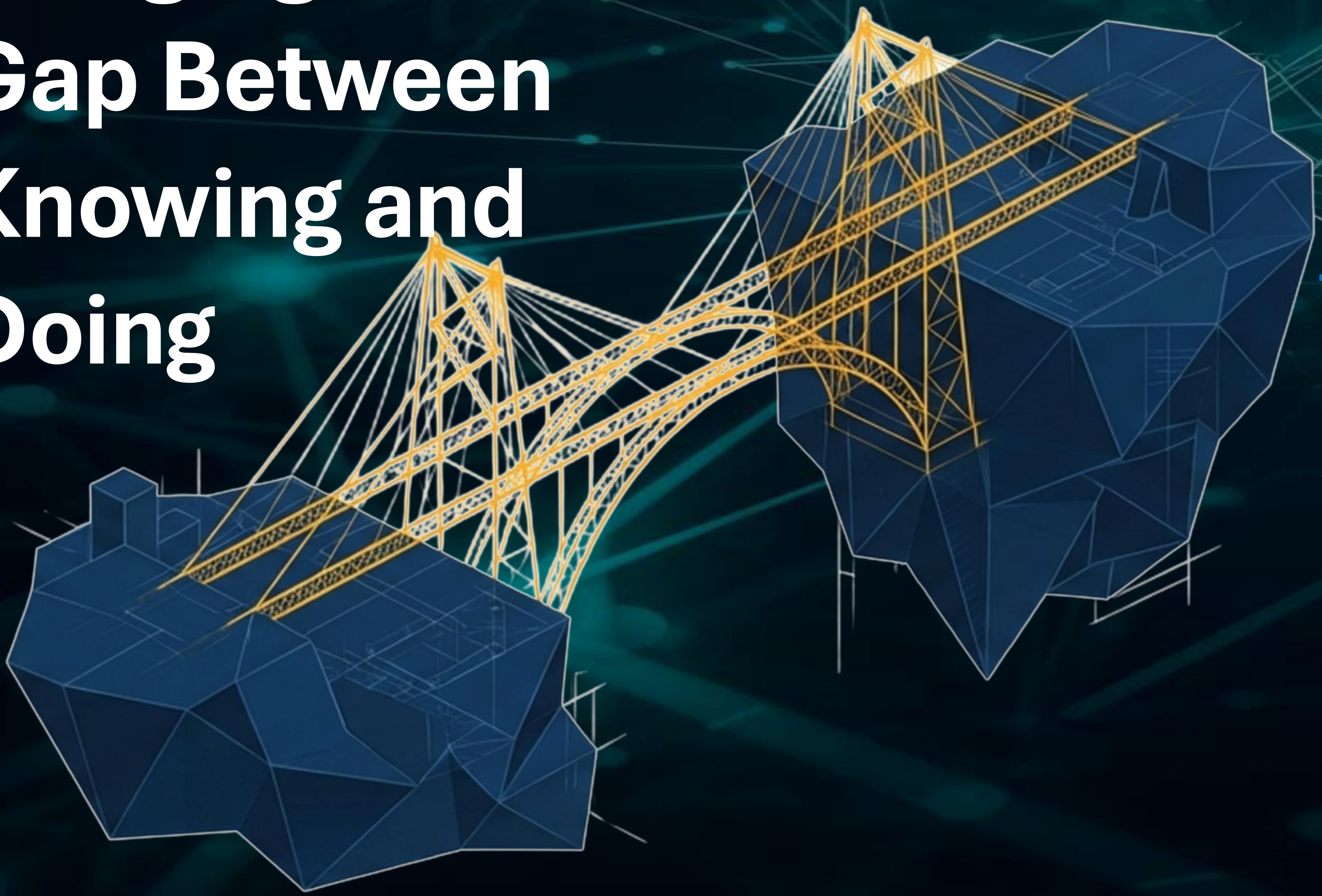
Gökhan Say
CEO
Cybridge Ventures

Critical Steps to AI Security

CISO
CONNECT
An Exclusive CISO Platform

An Analysis of CISO AI Priorities and Implementation Roadblocks

Bridging the Gap Between Knowing and Doing



The GenAI Security Consensus:

This study focuses on the survey questions related to recommended actions and implementation challenges in the CISO Connect AI Survey. It only includes the answers that were rated as critically or moderately important by more than 94% of CISOs.

CISOS Are Aligned on What to Do. The Real Challenge is How.

Survey data reveals a striking consensus among security leaders on the critical priorities across AI governance, security team readiness, project management, and tooling.

However, this universal agreement is met with a tough reality as these same leaders are facing severe obstacles making these critical tasks hard to implement.

This is the GenAI 'Implementation Gap'-the chasm between strategic clarity and operational reality.

94-100%

AGREEMENT on the
strategic priorities.

Up to 72%

DIFFICULTY
in implementation.

Four Systemic Challenges Driving the Execution Gap for Top AI Priorities

AI Governance

94-100% importance
53-88% Critically Important
vs. **46-64%** Hard to Implement

The challenge of creating enabling policies and cross-functional alignment.

Governance is about changing behavior, not just writing policy.

The challenge is operationalizing rules within workflows and across stakeholder groups with misaligned risk appetites.

Team Readiness

98-100% importance
42-67% Critically Important
vs. **41-49%** Hard to Implement

The challenge of upskilling security team and adapting talent strategy.

Team readiness is a continuous program, not a one-time training.

The challenge is building adaptive capacity for a rapidly evolving domain, focusing on reasoning over static credentials.

AI Projects

97-100% importance
36-81% Critically Important
vs. **42-61%** Hard to Implement

The challenge of balancing innovation with risk and measuring true impact.

Project success hinges on risky execution with scarce resources.

The challenge is in establishing clear metrics, securing high-risk areas, and resisting the pull of unmeasured transformation with scarce resources and ongoing other projects.

AI Tooling

94-100% importance
53-88% Critically Important
vs. **36-78%** Hard to Implement

The challenge of deploying a resilient, multi-layered defense with maturing technology.

Tooling requires architecting for opacity and immaturity.

The strategy must account for immature tools, a complex supply chain, and gaps between layers that demand a defense-in-depth approach.

Pillar 1: AI Governance

Cross-Functional Complexity

True AI governance requires deep, sustained alignment between Security, Legal, HR, Procurement, and Business Units. Unclear decision rights and differing risk tolerances create friction.

- ✓ Establishing clear rules of the road is the top priority for CISOs with 94-100% importance. But **46-64%** still say it's hard to implement.
- ✓ Because the implementation gap is driven by the difficulty of changing user behavior, aligning disparate stakeholders (Legal, HR, Business), and managing the fast-moving vendor ecosystem.
- ✓ The core challenge is making safe adoption the path of least resistance.

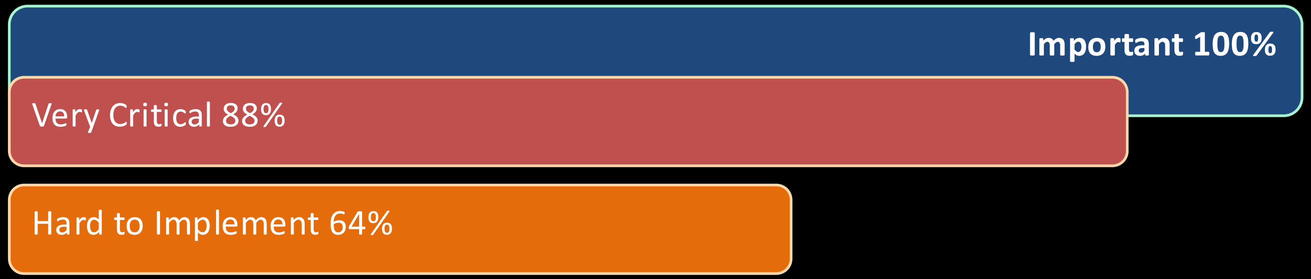
AI SECURITY STRATEGY: DEFENSE-IN-DEPTH & GOVERNANCE
DATA INTERRITY
MODEL ROBUSTRESS
SYSTEM MONITONING
CROSS-FUNCTIONAL ALIGNMENT (Security, Legal. Business)
AUTOMATED POTENTIAL vs. NOMAN CONTROL
ARCHITECTING FOR A NEW ATTACK SURFACE
AI SECURITY STRATEGY

Establishing the Foundations: Policies, Use Cases and Inventories

User policies + training for unsanctioned GenAI

Formulate user policies, training and guidance to minimize unsanctioned uses of GenAI, privacy and copyright infringement risks.

Rated by CISOs as:



Strategic Move

Make the safe path the default—clear policy, micro-training, and approved tools so "shadow AI" becomes unnecessary.

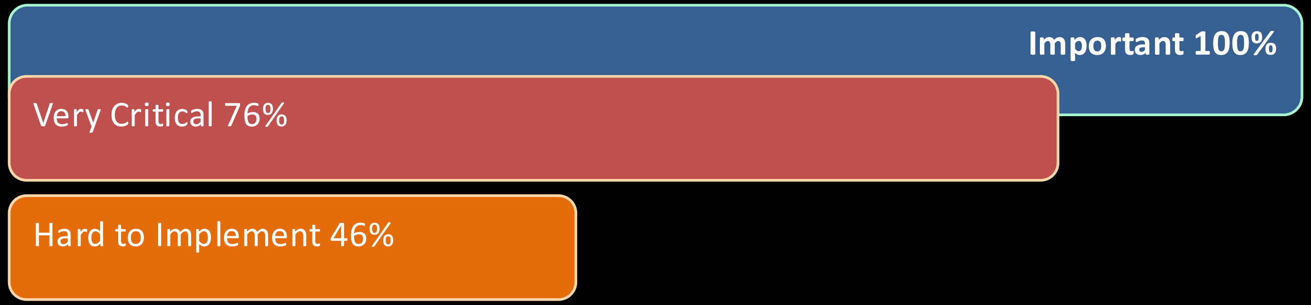
Underlying Challenge

Changing day-to-day behavior, aligning HR/legal/security wording, and embedding guidance into workflows takes time and sustained reinforcement.

Classify GenAI use cases

Classify use cases with the highest potential business impacts.

Rated by CISOs as:



Strategic Move

Build a value-vs-risk heatmap and prioritize use cases that drive measurable outcomes while protecting sensitive data.

Underlying Challenge

Impact scoring is subjective across business units and often requires data classification + agreement on what "material impact" means.

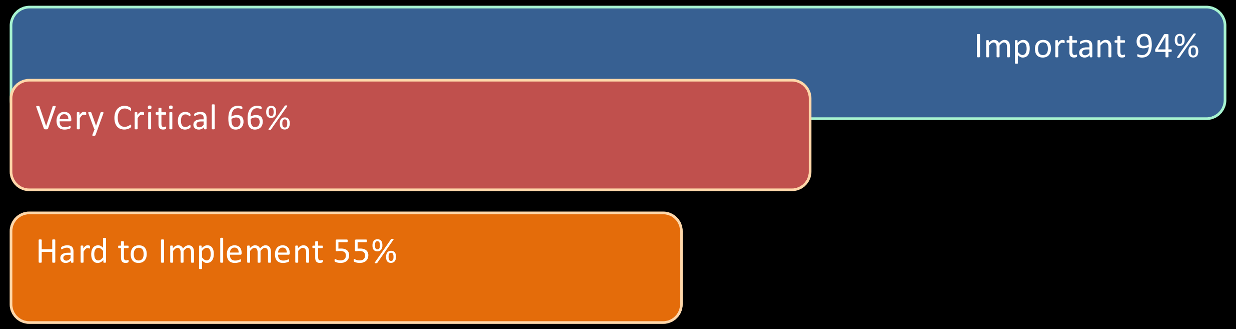
CISO CONNECT
An Exclusive CISO Platform

Foundational Governance: Where Policy Meets People and Process

Workflows for GenAI consumption

Define workflows to inventory, approve and manage consumptions of GenAI.

Rated by CISOs as:



Strategic Move

Treat GenAI like SaaS + data flow—who uses what model, with which data, for what purpose, under which approvals.

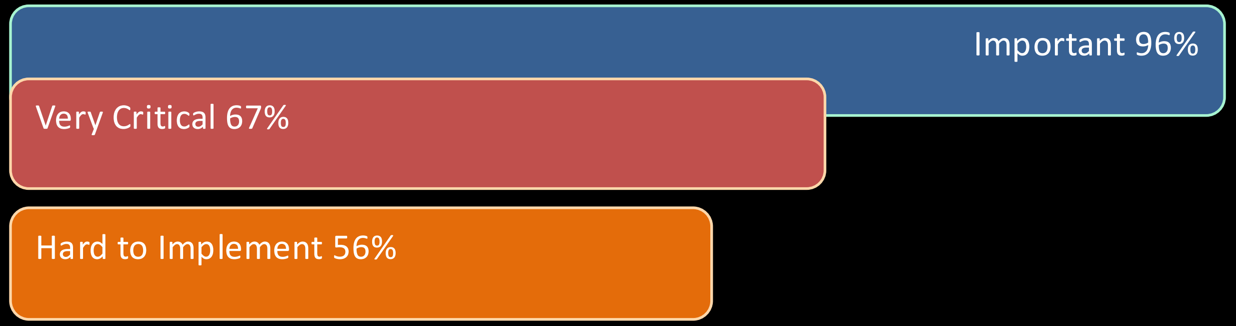
Underlying Challenge

Usage is fragmented across teams/tools, and you need process + tooling + ownership to keep inventories current.

Partner to set guardrails

Work with organizational counterparts who have active interests in GenAI (e.g., legal, compliance, lines of business) to formulate user policies, training and guidance—minimizing unsanctioned uses of GenAI and reducing privacy/copyright risks.

Rated by CISOs as:



Strategic Move

Create a cross-functional “fast lane” so governance enables adoption instead of blocking it.

Underlying Challenge

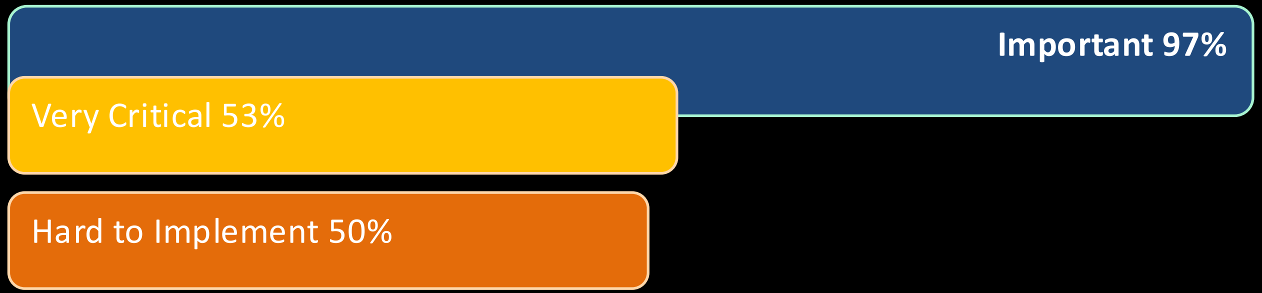
Stakeholders have different risk tolerances, and decision rights (who approves what) are often unclear.

The Ecosystem Challenge: Managing the Third Party & Vendor Risk

Transparency on data processing + supply chain dependencies

Identify changes in data processing and supply chain dependencies and require transparency about data usage by your security providers.

Rated by CISOs as:



Strategic Move

Ask every provider where data goes, which sub-processors/LLMs are used, and how data reuse is prevented.

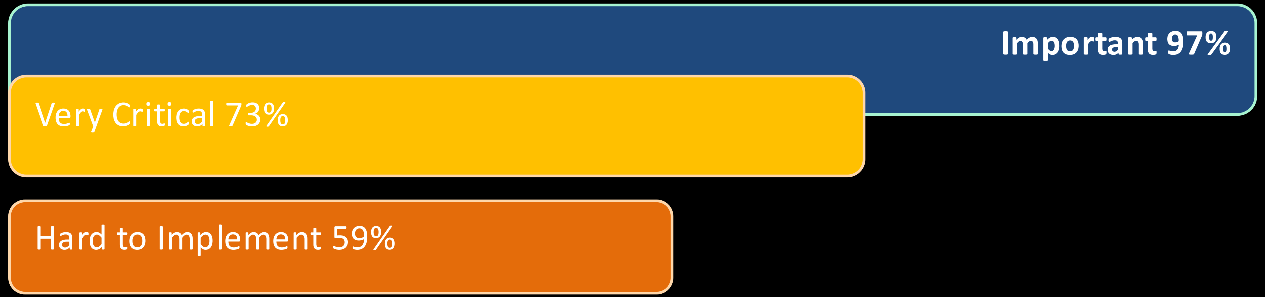
Underlying Challenge

Modern security stacks are multi-vendor and dependencies change fast, making continuous validation difficult.

New vendor risk requirements

Define new vendor risk management requirements for providers leveraging GenAI.

Rated by CISOs as:



Strategic Move

Update VRM for GenAI—model/provider disclosure, security testing evidence, change notifications, and incident clauses.

Underlying Challenge

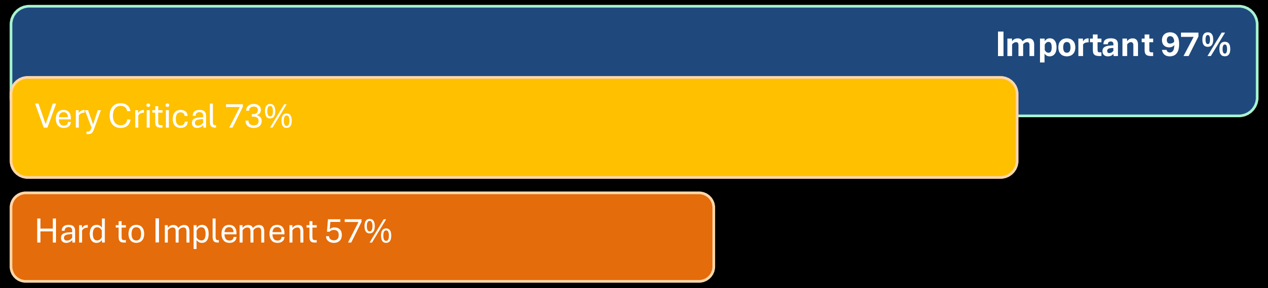
It forces new standards across procurement/legal/security and can slow buying unless you redesign the intake process.

Securing the Supply Chain Requires New Standards and Deep Vendor Scrutiny

Verify hosting/LLM vendors' governance & protection assurances

Obtain and verify hosting vendors' data governance and protection assurances that confidential enterprise information transmitted to its LLM.

Rated by CISOs as:



Strategic Move

Require specifics—data retention, training usage, tenant isolation, logging/redaction, auditability.

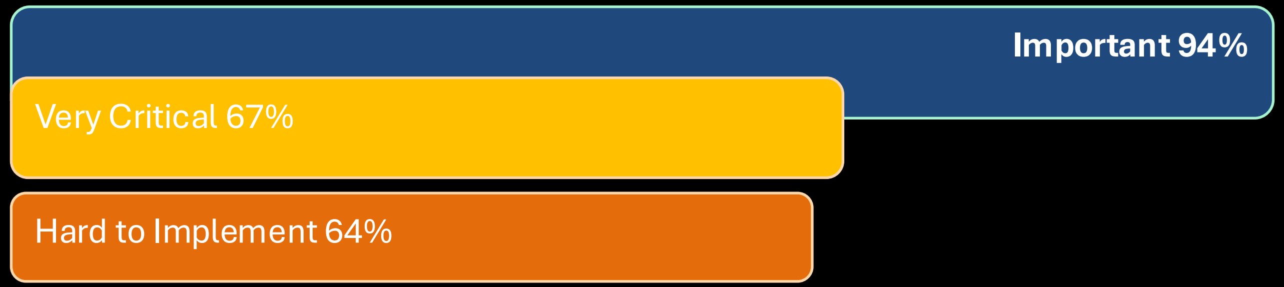
Underlying Challenge

Vendors vary widely in transparency, contracts take time to negotiate, and "LLM supply chain" details can be opaque.

Mandatory impact assessments (GDPR + EU AI Act, etc.)

Require from vendors the completion of the necessary impact assessments demanded by privacy and AI regulations (e.g., GDPR and the upcoming EU AI Act).

Rated by CISOs as:



Strategic Move

Standardize DPIA/AI impact assessment gates so vendors can move fast without compliance debt.

Underlying Challenge

Regulations are evolving, interpretation differs by region, and most vendors lack a scalable assessment workflow and accountable owners.

Pillar 2: Security Team Readiness

Evolving the Human Element for an AI-Native World

Preparing the Team and ensuring human oversight for AI is Critical, But requires a New Approach to Talent.

- ✓ CISOs agree on the need to prepare their teams as the effectiveness of any AI security strategy depends on the people who execute it.
- ✓ While they are focused on upskilling, addressing talent gaps, the implementation gap here is about the difficulty of continuous training, re-evaluating core competencies and fighting talent scarcity.
- ✓ The success lies in cultivating AI literacy, re-evaluating hiring to focus on reasoning skills and keeping humans in the loop without slowing down operations.

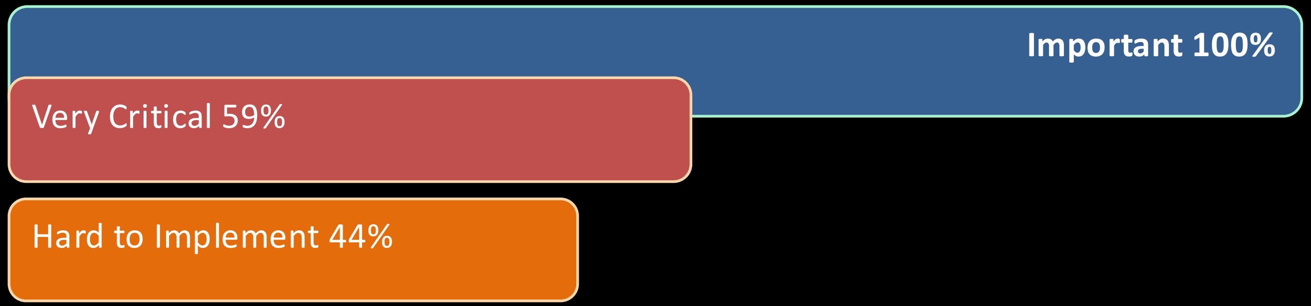
PILLAR 2: AI SECURITY TEAM READINESS -
HUMAN-AI COLLABORATION MODEL
UPSKILLING
REASONING SKILLS
HUMAN-IN-THE-LOOP OVERSIGHT

From AI Literacy to Talent Strategy: Building a Resilient Team

Build AI literacy

Continue to build AI literacy within your teams to set realistic expectations and develop a robust evaluation framework for AI.

Rated by CISOs as:



Strategic Move

Upgrade security judgment—teams need shared literacy to evaluate agents (reliability, permissions, data access, failure modes) before production.

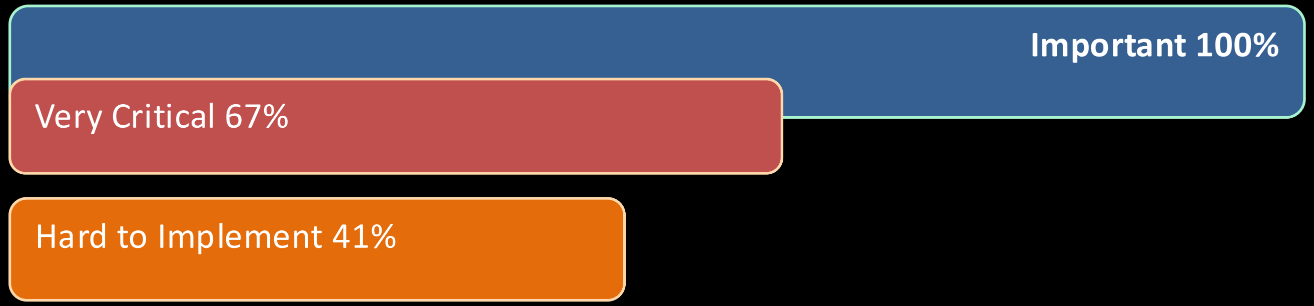
Underlying Challenge

Evaluation is hard without repeatable benchmarks, model behavior drifts with updates, and teams lack time and tooling for continuous testing.

Prepare your team for GenAI impacts

Prepare and train your team for dealing with direct (privacy, IP, AI application security) and indirect impacts (other teams using GenAI across HR, finance, procurement, etc.) coming from generative AI uses in the enterprise.

Rated by CISOs as:



Strategic Move

Treat AI readiness like an incident-prep program - role-based training, clear escalation paths, and shared playbooks across security, legal, and the business.

Underlying Challenge

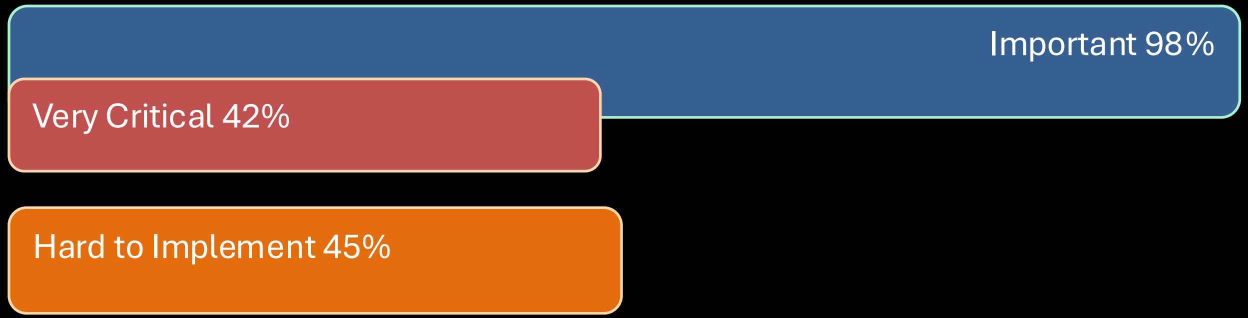
Training must cover many functions and scenarios, content becomes outdated quickly, and changing behavior requires sustained reinforcement.

Hiring Differently and Safeguarding critical skills Are Parallel Imperatives

Address talent gaps

Address talent gaps by reevaluating hiring requirements and recruiting new sources of talent—prioritizing critical thinking and logical reasoning over out-of-date experience or certifications.

Rated by CISOs as:



Strategic Move

Hire for fundamentals and adaptability - reasoning, systems thinking, and curiosity - then upskill on AI security specifics internally.

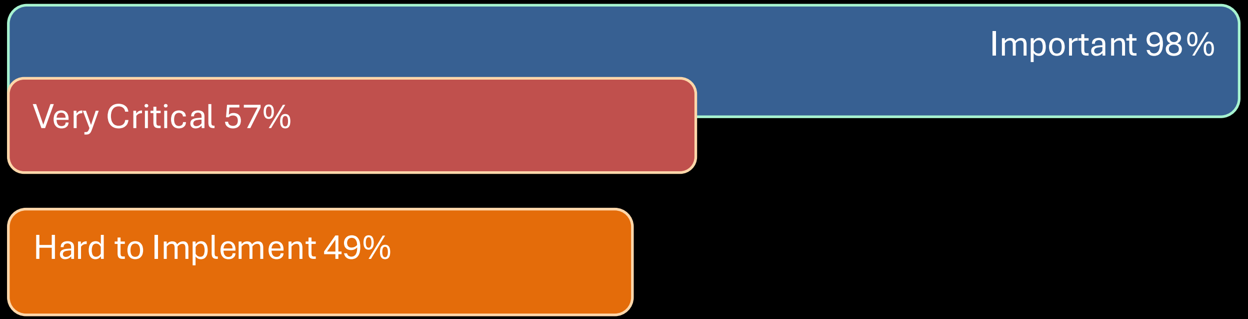
Underlying Challenge

The market is tight, hiring processes are slow to change, and mapping 'AI security' roles to clear competencies is still evolving.

Safeguard critical skills

Safeguard critical skills by integrating regular manual verification as part of semi-automated workflows—sample verification during testing and ongoing checks in production.

Rated by CISOs as:



Strategic Move

Keep humans in the loop where it matters - sample-check AI outputs to prevent silent failure and to avoid deskilling the team.

Underlying Challenge

Manual review adds cost and latency, it's hard to choose the right sampling rate, and ownership for verification is often unclear.

Pillar 3: AI Security Projects

From Measured Experiments to High-Stakes Deployment

Success Lies in Measurable Experiments, Not Vague Transformations

- ✓ For AI projects, the gap is defined by the pressure to deliver transformative results versus the practical need for rigorous, metrics-driven experimentation.
- ✓ The hardest part is embedding security into high-risk, high-reward use cases without stifling the pace of innovation.
- ✓ To deliver real value, AI initiatives must be ruthlessly prioritized, meticulously measured, and carefully balanced between automated potential and human control.

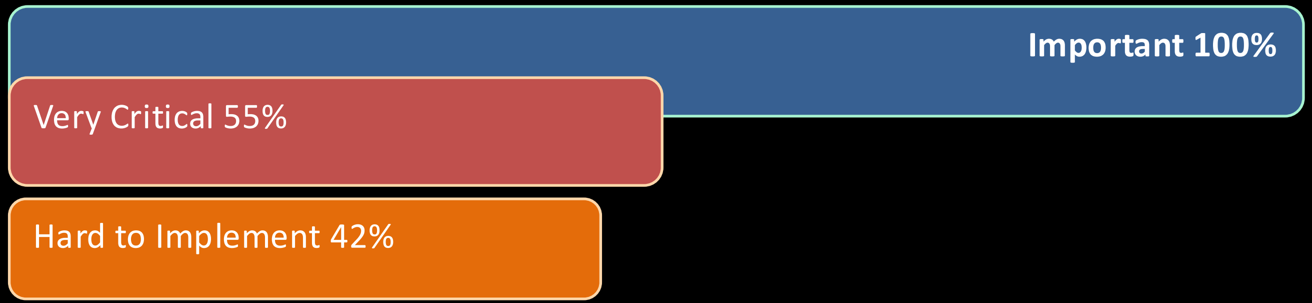
CISO CONNECT
An Exclusive CISO Platform

From Ambitious Transformation to Measurable Wins

Prioritize outcome-driven AI initiatives

Prioritize outcome-driven AI initiatives rather than unclear, difficult-to-measure transformation programs—combine smaller experiments with continuous evaluation of AI augmentation benefits for security teams.

Rated by CISOs as:



Strategic Move

Optimize for measurable wins - pick specific use cases (MTTR, detection engineering throughput, review time) and iterate fast.

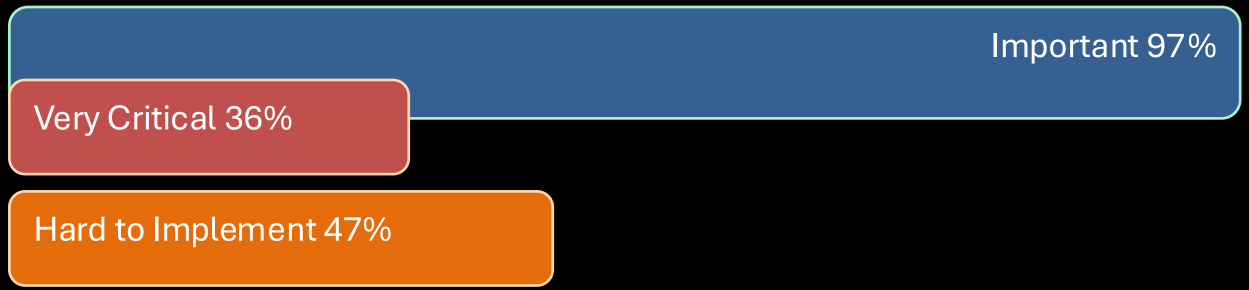
Underlying Challenge

Stakeholders want big transformation stories, but benefits are hard to isolate, and experimentation needs disciplined governance and metrics.

Establish metrics to benchmark

Establish or extend existing metrics to benchmark generative cybersecurity AI against other approaches, and to measure expected productivity improvements.

Rated by CISOs as:



Strategic Move

Make AI accountable - compare AI-assisted vs non-AI baselines and measure quality, not just speed.

Underlying Challenge

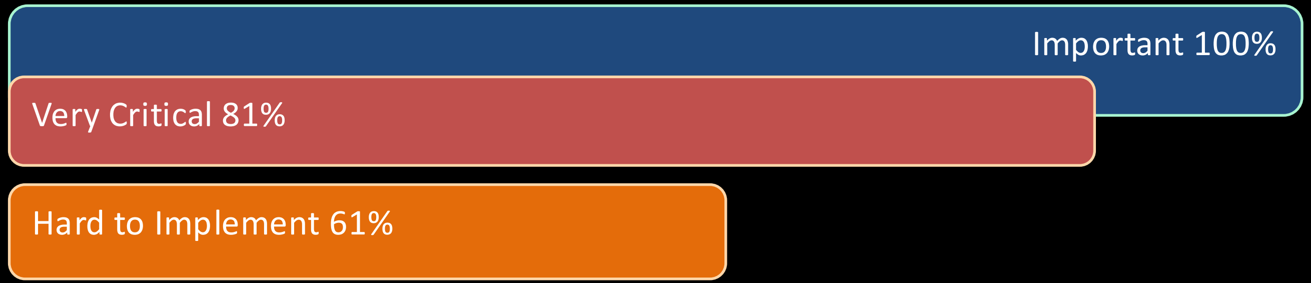
Metrics are inconsistent across teams, ground truth is scarce, and it takes time to instrument workflows end-to-end.

Prioritizing Security Where the Blast Radius is Highest

Prioritize security resource involvement

Prioritize security resource involvement for use cases with direct financial and brand impacts, such as code automation, customer-facing content generation and customer-facing teams, such as support centers.

Rated by CISOs as:



Strategic Move

Put security where the blast radius is highest - code, customer channels, and high-trust workflows should get the earliest guardrails.

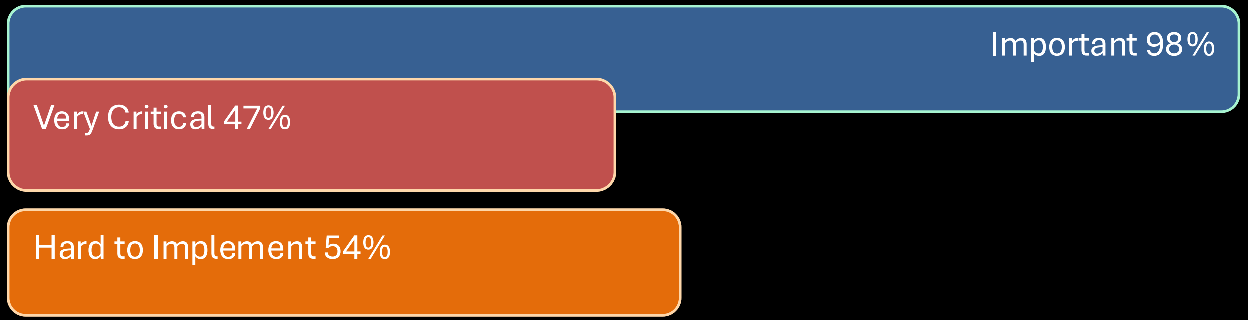
Underlying Challenge

Security teams are capacity-limited, business teams move fast, and avoiding political prioritization decisions without clear risk criteria is critical.

Determine the right balance

Determine the right balance between autonomy and control for each use case through extended pilots and rigorous agent monitoring. Train employees on agent interaction and debugging.

Rated by CISOs as:



Strategic Move

Scale autonomy gradually - start with assisted modes, add monitoring and rollback, and train users to debug and verify agent work.

Underlying Challenge

Agent behavior can be unpredictable, monitoring is immature, and failures can be high-impact without clear kill-switches.

Pillar 4: AI Controls & Tooling

Architecting a Defens-in-Depth for a New Attack Surface

Foundational Visibility and Defense-in-Depth Are Harder Than Testing New Tools

- ✓ The security stack is evolving to address a new attack surface. CISOS recognize the need to experiment with new tools and they are focused on adopting new controls, preparing for AI-native threats, and instrumenting a new technology ecosystem.
- ✓ But deploying such tools are rated as the hardest tasks due to
  - Technical and organizational complexity.
  - The immature AI Security tooling and the fragmented technology stack
  - The immense operational burden.

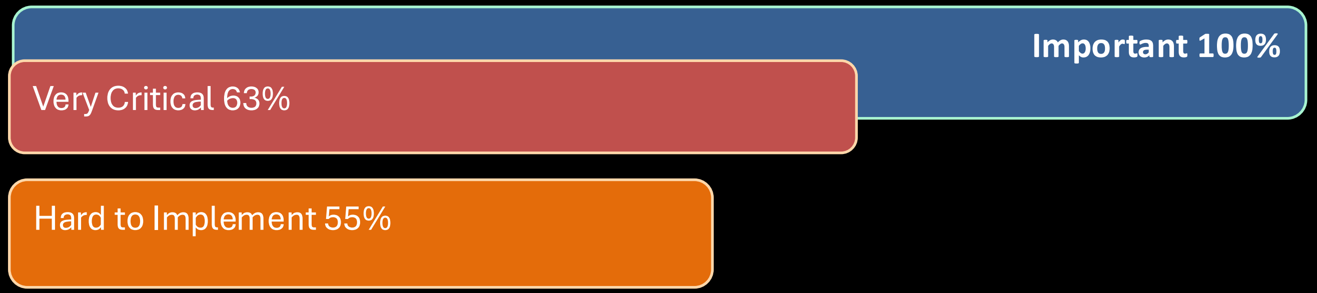
AI SECURITY STRATEGY: DEFENSE-IN-DEPTH & GOVERNANCE
Security, Legal
HR
Business Units
CROSS-FUNCTIONAL ALIGNENT
EXPERIMENTATION METRICS (Measured to High-Stakes)
150
100
50
0
HIGH-STAKES DEPLOYMENT: 78%
Security
Legal
HR
Business Units
CROSS-FUNCTIONAL ALIGNMENT
AI CONTROLS & TOOLING: NEW ATTACK SURFACE
AI TASKS
AI LITERACY TRAINING
AI LITERACY TRAINING
HUMAN-IN-THE-LOOP OVERSIGHT

AI Security Experimentation is Risky

Run experiments with new AI features

Run experiments with new features from existing security providers, starting with targeted and narrow use cases in the security operation and application security areas.

Rated by CISOs as:



Strategic Move

Pilot where you already have telemetry - test small, targeted workflows and scale only what works.

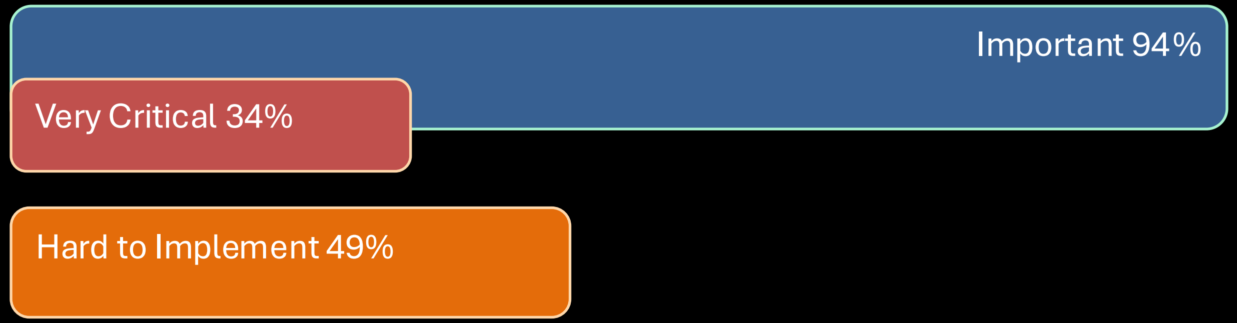
Underlying Challenge

Feature maturity is uneven, integrations can be complex, and it's hard to separate true gains from AI marketing.

Test emerging products

Test emerging products that inspect and review outputs for misinformation, hallucinations, factual errors, bias, copyright violations, and other unwanted content.

Rated by CISOs as:



Strategic Move

Trust, but verify - add output inspection so risky content is caught before it reaches employees or customers.

Underlying Challenge

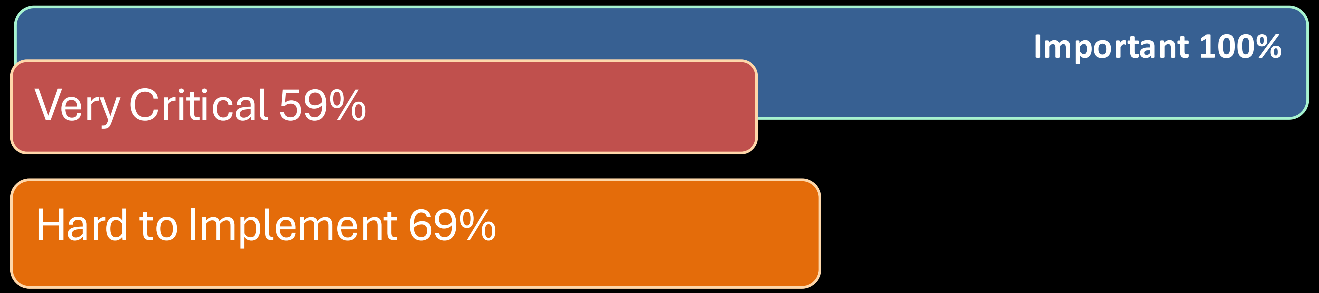
‘Ground truth' is context-dependent, false positives create friction, and maintaining review coverage at enterprise scale is operationally heavy.

Building the Foundational Stack: Visibility and Defense-in-Depth

Use a layered trust, risk and security stack

Use a layered approach comprising all layers of the trust, risk and security management stack to protect your AI interactions, and make sure your enterprise broadens its focus from runtime vectors to the software supply chain and infrastructure stack.

Rated by CISOs as:



Strategic Move

Defense-in-depth for AI - protect data and prompts, runtime behavior, and the supply chain AI depends on.

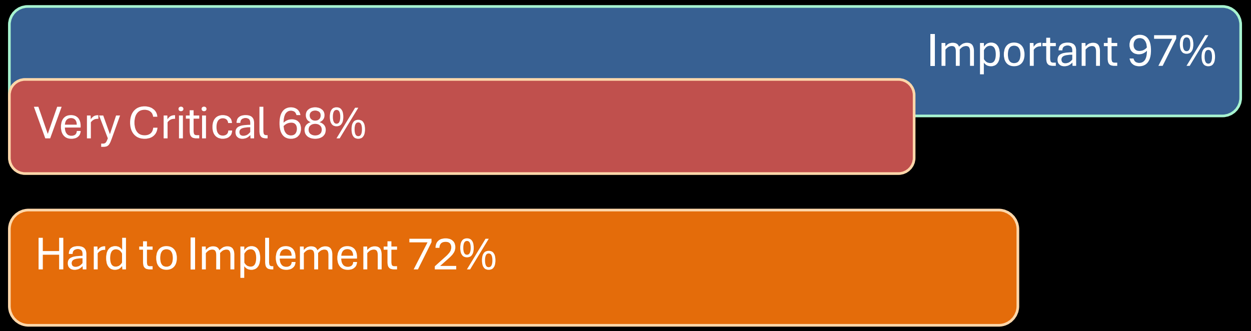
Underlying Challenge

Coverage spans many tools and teams, overlapping controls add complexity, and gaps often appear between layers.

Deploy AI governance tools

Deploy AI governance tools that continually evaluate and assure the security posture of all your AI assets, especially those from your software supply chain.

Rated by CISOs as:



Strategic Move

You can't secure what you can't see - continuously inventory and assess models, datasets, connectors, and third-party components.

Underlying Challenge

Inventories are incomplete, standards are forming, and posture assessment requires deep integration with procurement, ML platforms, and security operations.

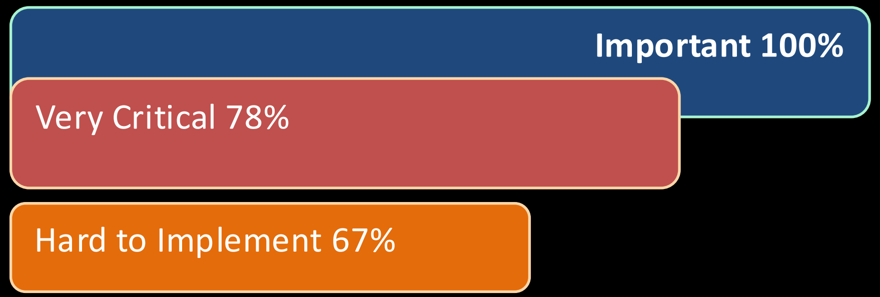
CISO CONNECT
An Exclusive CISO Platform

Defending a New and Evolving Attack Surface

Initiate SCA and vulnerability assessment programs

Initiate software composition analysis and vulnerability assessment programs for AI applications. Don't assume that existing infrastructure security and vulnerability scanning tools handle AI components properly.

Rated by CISOs as:



Strategic Move

Treat AI applications as a new attack surface - cover models, pipelines, dependencies, and exposed endpoints.

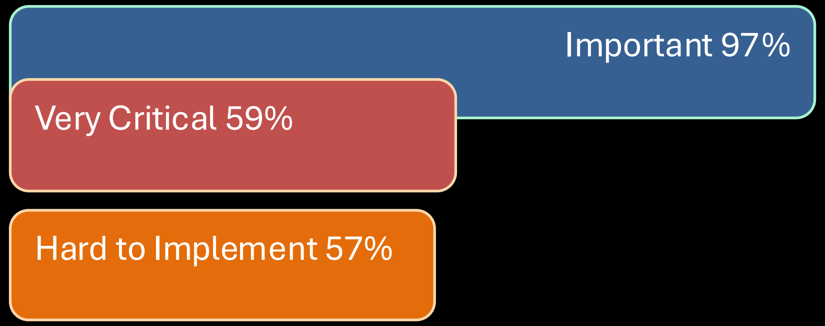
Underlying Challenge

Tooling is still maturing, AI stacks are diverse, and ownership spans data, ML, engineering, and security.

Anticipate new waves of account takeover

Anticipate new waves of account takeover attacks by reassessing communication channel and credential security, especially in semiautomated and upcoming AI agent architectures.

Rated by CISOs as:



Strategic Move

Identity becomes the control plane - harden phishing-resistant MFA, resets, session controls, and channel verification.

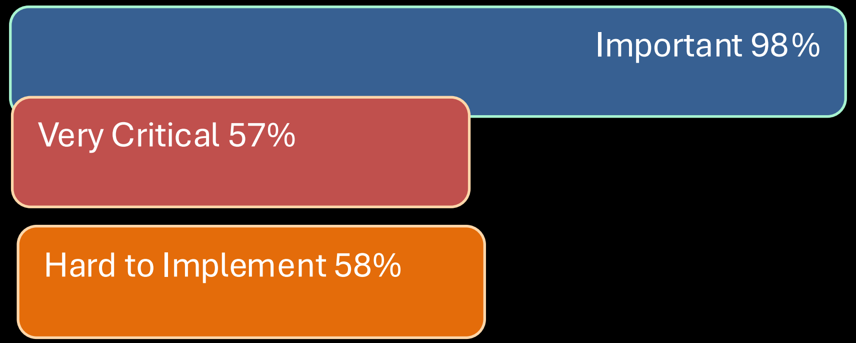
Underlying Challenge

Identity changes are disruptive, legacy auth paths persist, and stronger controls can hurt user experience if not managed carefully.

Keep an AI threat intelligence function

Prepare for potential new threats by keeping an AI threat intelligence function and tuning its defense to the observed and harmful deepfake attacks.

Rated by CISOs as:



Strategic Move

Extend threat intel to AI-native abuse - track deepfake-enabled fraud and tune detection and response as attack quality improves.

Underlying Challenge

The landscape evolves rapidly, validation is difficult, and response spans security, identity, comms, and fraud teams.

The Path Forward:

From Strategic Consensus to Operational Mastery

The Vision and the blueprint for what needs to be done is clear and The work ahead is to translate this universal consensus into durable, enterprise-wide practice .

The leaders are building the operational muscle to execute on that consensus at scale.
This survey highlights a critical need to invest in the operational capabilities required to bridge the gap for:

- ✓ Building cross-functional operating models for rapid decision-making.
- ✓ Investing in foundational visibility and control planes for AI assets.
- ✓ Redesigning talent and training programs for a new class of risk.

Success will be determined not by finding a single perfect tool, but by the deliberate, disciplined, and cross-functional strategy to close the implementation gap across your governance, your team, your your projects, and your controls.

CISO CONNECT
An Exclusive CISO Platform