FRONTIERZERO SOLUTIONS

FrontierZero

AI Security Playbook: Managing Risks, Compliance, and Control

For Chief Security Officers (CSOs) and IT leaders, AI presents an entirely new attack surface—one that many organizations are failing to monitor or secure properly.

Artificial Intelligence (AI) is fundamentally reshaping industries across the world. From automating business processes to enhancing decision-making, AI tools are rapidly being integrated into daily operations.

However, as AI adoption accelerates, security and compliance challenges are mounting.

Employees sign up for AI tools with just an email, upload confidential business data, and move on—without considering where that data is stored, who has access to it, or how secure the platform really is.

This Guide Outlines:

- The biggest security risks of AI Adoption
- The rapidly evolving regulatory landscape for AI compliance
- How AI breaches lead to ransomware, fraud and financial loss
- Actionalbe steps to take control of AI usage in your organization

Security teams must get ahead of the AI security problem before it escalates into financial losses, regulatory fines, and reputational damage.

Key Benefits

We help you with the unknown

AI Tool Discovery
Automatically identify which AI applications employees are connecting to your environment—even unsanctioned ones.

Compliance Risk Monitoring
Spot AI tools that could expose your organization to regulatory penalties under GDPR, EU AI Act, and industry standards.

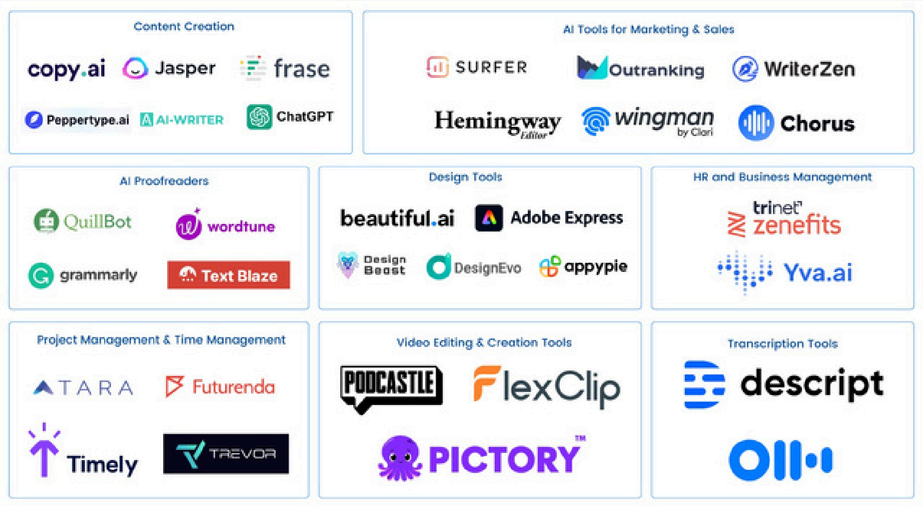
Access and Data Protection
Track who is using AI tools, what data they access, and whether MFA and secure configurations are in place.

Shadow AI Detection
Uncover hidden AI usage across departments before it becomes a security or compliance liability.

Audit-Ready Reporting
Easily generate reports to show auditors and leadership how AI risks are being monitored, mitigated, and controlled.

FrontierZero

1. The Hidden AI Security Risks: What you don't see can hurt you



The adoption of AI tools is outpacing security oversight. Employees across departments are using AI to improve productivity, often without IT approval.

Common AI-driven activities include:

- Sales teams summarizing calls with AI-powered transcription tools.
- Finance departments running budget forecasts through AI assistants.
- Legal teams reviewing contracts using AI-based document analysis.
- HR teams screening resumes with AI-powered recruitment platforms.

While these tools improve efficiency, they also introduce major security risks.

Key AI Security Risks Organizations Face:

- Shadow AI Usage – Employees use AI tools without IT knowledge, exposing sensitive data.
- Unmonitored Third-Party Integrations – AI apps connect to corporate platforms, expanding the attack surface.
- Data Leakage – AI platforms may store and process uploaded data indefinitely.
- Weak Authentication – Many AI tools lack robust security controls, making them vulnerable to breaches.
- Regulatory Compliance Risks – AI usage may violate emerging global regulations on data security and AI governance.
- Data Sovereignty Concerns – AI tools may store data in locations that conflict with regional data sovereignty laws, putting organizations at risk of legal violations and fines.

AI is reshaping cybersecurity—and security leaders must ensure their organizations do not fall behind.

2. The AI Regulatory Landscape: Global Compliance and Challenges for Businesses

The EU AI Act, which came into force in August 2024, is the world's first comprehensive law regulating artificial intelligence. Much like GDPR transformed data privacy, this legislation sets a new benchmark for AI security and compliance.

Its goal is to ensure AI development is both safe and ethical while minimizing security risks and regulatory violations. But compliance isn't optional—companies worldwide that develop or use AI affecting the EU market must comply or face severe penalties.

For security leaders, the biggest risk isn't just their official AI tools—it's shadow AI. If employees are using unapproved AI applications to process sensitive data, the company could unintentionally violate AI laws, triggering heavy fines and legal repercussions.

This risk is even more pronounced for companies outside the EU, like those in Australia, USA, UAE, and Singapore, that work with EU-based clients or handle EU citizen data, but aren't thinking about EU regulations.

Even indirect connections to European systems can bring your organization under the Act's jurisdiction, exposing you to substantial penalties if shadow AI use goes unchecked.

Key Provisions: Understanding the Regulatory Framework

The EU AI Act follows a risk-based approach, categorizing AI systems into different levels of risk.

Banned AI Practices (Unacceptable Risk)

These AI applications are considered too dangerous and are prohibited outright, with enforcement beginning in February 2025:

- Manipulative AI – AI that influences behavior in harmful ways, such as deceptive advertising targeting children.
- Social Scoring – Assigning individuals a score based on behavior, similar to China's social credit system.
- Untargeted Facial Recognition & Biometric Categorization – AI that identifies race, religion, or sexual orientation without consent.
- Real-Time AI Surveillance – AI-driven tracking in public spaces, except for national security purposes.

Risk of Shadow AI: Employees adopting AI tools with biometric screening, behavioral analysis, or AI-driven decision-making could unknowingly expose the company to compliance violations. Without proper oversight, security teams may be unaware of these risks until regulators step in.
How do you know your employees aren't using AI tools like this without your knowledge? Are you confident that unapproved apps aren't making their way into your tech stack?

High Risk AI systems

These are AI tools that directly impact human rights, safety, or financial stability. Companies deploying these systems must meet strict security, transparency, and oversight requirements by August 2026:

- AI in healthcare, such as automated diagnoses
- AI in finance, including credit scoring models
- AI in hiring and employment, such as AI-based resume screening
- AI in law enforcement, such as predictive policing algorithms

Risk of Shadow AI: Employees using unauthorized AI-driven hiring tools or financial models could create compliance risks. An AI-powered chatbot screening resumes may violate hiring bias laws under the EU AI Act if it lacks transparency.
To operate legally in the EU, high-risk AI systems must undergo:

- Regular audits to ensure compliance
- Human oversight of AI-driven decisions
- Strict risk assessments before deployment

If shadow AI bypasses these requirements, companies may be held accountable—even if the IT team isn't aware of the tool's use.

General Purpose AI (GPAI) and Transparency Rules

Starting August 2025, all general-purpose AI models (like ChatGPT, DeepSeek, Gemini) must meet strict transparency standards:

- Clearly label all AI-generated content
- Undergo bias and discrimination audits
- Prove models don't expose personal or sensitive data

AI tools deemed "systemically risky" will face even tougher controls.

Risk of Shadow AI: If employees use unapproved AI tools without understanding these new obligations, they could create AI-driven reports or decisions that violate EU laws—without even realizing it. Imagine marketing teams publishing AI content that triggers fines or reputational damage.

One unmonitored AI tool could cost millions.
Do you know which AI tools your teams are already using?

Global Reach: Extraterritorial Compliance

The EU AI Act applies beyond European borders. If a company develops, sells, or uses AI that impacts EU citizens, compliance is mandatory.
Examples of affected businesses:

- A U.S.-based AI-powered chatbot interacting with EU customers.
- A Chinese AI facial recognition company operating in the EU.
- A Singapore-based AI hiring tool screening EU candidates.

Ignoring these regulations can result in fines of up to €35 million or 7% of annual revenue, whichever is higher.

Risk of Shadow AI: Security teams may track approved AI vendors, but what about unapproved tools that employees use without oversight? Non-compliant AI tools hidden within an organization could trigger legal penalties, even if they were adopted without IT approval.

Countries and Agencies Banning DeepSeek AI:

DeepSeek AI Bans and Restrictions Around the World

Multiple governments have banned or restricted DeepSeek AI due to security and privacy concerns:

- Italy: Banned over data privacy issues
- Taiwan: Prohibited use in public sector and critical infrastructure
- Australia: Banned on all federal devices
- United States: Navy, Commerce, and other agencies restricted use
- South Korea: Blocked new downloads over personal data risks
- India: Finance Ministry warned against AI tools like DeepSeek

Risk of Shadow AI: When employees use unmonitored AI tools, you're not just facing internal risks—you're exposing the company to global regulatory scrutiny and penalties.

Are you confident you know which AI tools your teams are using right now?

The Compliance Challenge: Why Shadow AI Creates Hidden Risk

Companies must now rethink AI strategies—not just for official tools, but for identifying and eliminating Shadow AI before it creates liability.

The Cost of Compliance:

High-risk AI vendors must complete extensive documentation and security testing.

- Compliance costs for smaller firms estimated at €50,000–€300,000 per AI system
- Big tech (Google, Microsoft, OpenAI) can adapt—startups face serious hurdles

Risk of Shadow AI: Focusing compliance budgets only on approved tools leaves companies exposed to legal and financial fallout from unseen Shadow AI usage.

Sector-Specific Disruptions:

- Healthcare AI: Diagnoses must be validated by doctors
- Finance AI: Loan decisions must offer transparent explanations
- Retail & Advertising AI: AI-generated ads must be clearly labeled

Risk of Shadow AI: If employees use non-compliant AI for diagnoses, financial approvals, or marketing, they could unknowingly break industry-specific regulations.

Supply Chain & Third-Party Risks:

Companies must manage not only their AI, but also their vendors' tools.

- Audit third-party AI for compliance gaps
- Update contracts to address AI risks
- Ensure informal AI use still meets EU standards

Risk of Shadow AI: Unapproved vendor tools or informal AI integrations could expose sensitive data—and compliance teams may not even know they exist.

The Global Ripple Effect:

Just as GDPR reshaped data privacy, the EU AI Act is pushing global AI compliance forward.

- U.S.: State-by-state patchwork
- Asia-Pacific: Balancing security with innovation
- Middle East: Focus on ethical AI over restrictions

Companies taking a "wait and see" approach to AI compliance are already behind.

Shadow AI isn't just a technical risk—it's a legal and regulatory liability.

3. The AI Boom: Moving Too Fast, Breaking Security

The AI space is moving at breakneck speed. New platforms launch almost daily,competing to attract users, integrate with businesses, and promise groundbreaking efficiency. But in the rush to scale, security is often an afterthought.

Most AI startups prioritize growth over governance, focusing on onboarding users and refining their models—while neglecting fundamental security controls. This creates massive risks, both for the platforms themselves and for the companies feeding them sensitive data.

What Happens When AI Platforms Grow Too Fast?

When a new AI tool experiences rapid adoption, security gaps emerge:

- Weak authentication – Minimal security checks allow unauthorized access.
- Misconfigured databases – Sensitive information is stored without proper protection.
- Unsecured APIs – Open access to backend systems enables data scraping and exploitation.
- Lack of compliance oversight – Regulatory requirements are overlooked in favor of speed.

These vulnerabilities make AI platforms a high-value target for attackers.

The Aftermath of an AI breach

Once an AI company suffers a breach, the damage extends far beyond the platform itself:

- Login credentials leaked – Employees reusing passwords put corporate accounts at risk.
- Confidential company data exposed – Uploaded reports, contracts, and customer information become publicly accessible.
- Weaponized phishing attacks – Stolen data helps hackers craft convincing emails to infiltrate networks.
- Regulatory penalties – Companies unknowingly violating data protection laws face hefty fines.

Why This Matters To Your Business

If AI security is an afterthought for the tools your team relies on, then your sensitive data is at risk. Without visibility into which AI tools employees are using, businesses are left exposed to breaches that are outside of their control.

The speed of AI adoption shouldn't come at the cost of security. But for many businesses, that’s exactly what’s happening.

4. The DeepSeek AI Breach: What Went Wrong?

DeepSeek AI, a fast-growing AI platform, recently suffered a major security breach that exposed sensitive system data. Here's what went wrong:

- Unsecured Database: A misconfigured system left over a million log lines publicly accessible with no authentication.
- Exposed API Keys: Hackers could have used these keys to manipulate data, extract information, or escalate their access.
- Lack of Oversight: There was no clear monitoring of who had access to what—leaving sensitive business data vulnerable.

For businesses that rely on AI tools, this isn't just DeepSeek's problem—it's yours too. If your employees are using AI without security oversight, your customer data, financial reports, and internal conversations could be at risk.

5. AI Breaches: How They Lead to Ransomware and Financial Fraud

A stolen login, a single email, or leaked API keys—this is all it takes for an AI security failure to spiral into a full-scale cyberattack.

The Real-World Cost of an AI Breach

Scenario 1: The Fake CFO Scam

According to an FBI investigation, hackers infiltrated the email account of a CFO at Unatrac Holding Ltd. by using phishing techniques. They monitored emails for weeks, learning how the CFO communicated.

Then, posing as the CFO, they instructed employees to process fraudulent wire transfers—leading to $11 million in financial losses before the fraud was detected.

Scenario 2: AI Breach → Ransomware Attack

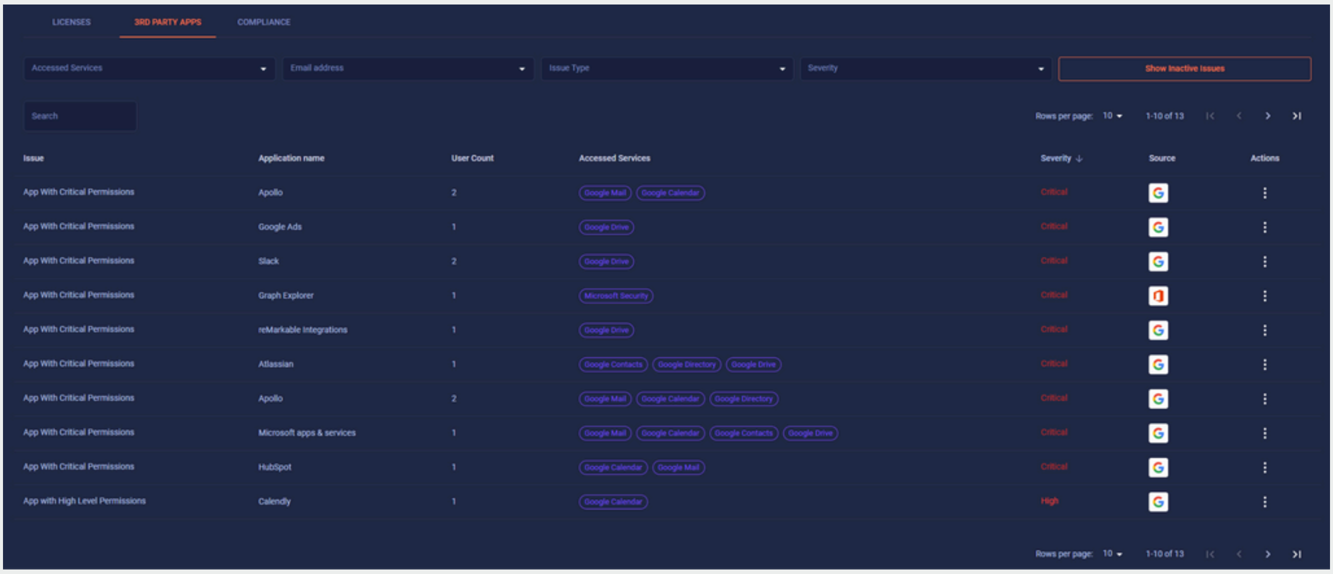
AI tools store valuable business data. If an AI company is breached, hackers can use that data to craft highly personalized phishing emails targeting employees.

1. An AI platform is hacked → Exposing customer invoices, project details, and credentials.
2. Hackers send fake emails to employees → Using real company data to appear legitimate.
3. An employee unknowingly clicks a malicious link → Giving attackers access to company systems.
4. Ransomware is deployed → Locking files and demanding payment.

💰 **The average ransomware payout in 2025 exceeds $5 million per attack.**

These attacks aren't theoretical—they're happening now. AI platforms must be secured before they become a liability for businesses worldwide.

6. The Solution: Gaining Full AI Visibility and Control



Issue	Application name	User Count	Accessed Services	Severity ↓	Source	Actions
App With Critical Permissions	Apollo	2	Google Mail Google Calendar	Critical	G	⋮
App With Critical Permissions	Google Ads	1	Google Drive	Critical	G	⋮
App With Critical Permissions	Slack	2	Google Drive	Critical	G	⋮
App With Critical Permissions	Graph Explorer	1	Microsoft Security	Critical		⋮
App With Critical Permissions	reMarkable Integrations	1	Google Drive	Critical	G	⋮
App With Critical Permissions	Atlassian	1	Google Contacts Google Directory Google Drive	Critical	G	⋮
App With Critical Permissions	Apollo	2	Google Mail Google Calendar Google Directory	Critical	G	⋮
App With Critical Permissions	Microsoft apps & services	1	Google Mail Google Calendar Google Contacts Google Drive	Critical	G	⋮
App With Critical Permissions	HubSpot	1	Google Calendar Google Mail	Critical	G	⋮
App with High Level Permissions	Calendly	1	Google Calendar	High	G	⋮

Security teams need a centralized way to monitor and manage AI usage across the organization.

How FrontierZero Helps :

- AI Usage Visibility – Detect all AI applications employees are using.
- Access Control Enforcement – Monitor third-party integrations and risky logins.
- Compliance Tracking – Ensure AI usage aligns with evolving regulatory requirements.

AI security is no longer a future concern—it is an immediate challenge that demands action.

🔍 Are you confident your company's AI usage is secure?

📊 See the full picture—before it's too late.

Final Thoughts: The AI Security Challenge for CSOs

AI adoption is inevitable, but without proper security measures, organizations are exposed to compliance risks, data breaches, and financial losses.

Security leaders must act now to gain visibility, enforce compliance, and mitigate AI security threats before regulators—and attackers—force them to do so.

Get full AI security visibility today!

Click here to Start a free trial of FrontierZero today!