grip

FROM *CHAOS*

TO CONTROL

GOVERNING SAAS + AI RISK
ACROSS THE MODERN ENTERPRISE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2026, AI is now a reality for every modern enterprise.
Over the past several years, and especially throughout 2025, AI has rapidly spread across organizations. Driven by both board-level competitive mandates and widespread employee adoption of productivity tools, AI risk has expanded throughout nearly every enterprise, often with limited visibility or oversight from IT and security teams.
This intersection of executive-mandated AI adoption and employee-driven AI use has created conditions that increase data exposure and breach risk.

As a result, in 2026 executives are confronting a new operating reality: AI is already embedded in the enterprise, most risk now enters through SaaS, and governing AI is no longer an IT concern. Rather, it is a core business responsibility.

This report is written for executive leadership teams, including CEOs, CFOs, General Counsel, CISOs, and board risk committees responsible for governing enterprise risk.

Bottom line for executives

AI is not a future risk, nor is it "just an IT problem." And crucially, governing it is not optional. It is now one of the most influential forces shaping how modern businesses operate and take on risk.

Organizations that recognize this early can move faster with confidence, protecting innovation while reducing exposure before it becomes a business issue. Managing this reality requires a unified control plane that spans SaaS, AI, identities, and integrations, not another standalone tool or policy.

<THE SCOPE OF AI>

In this report, "AI" refers not only to standalone tools, but to embedded AI features, agents, copilots, browser extensions, and API-connected integrations operating inside everyday SaaS platforms.

THE STATE OF SAAS + AI SECURITY

This snapshot is grounded in aggregated, anonymized telemetry from real-world enterprise SaaS environments monitored by Grip Security and highlights the scale, speed, and largely unseen nature of AI-driven risk across modern SaaS environments. AI is no longer confined to a handful of approved tools, it is embedded across thousands of environments, integrations, and workflows that touch sensitive data every day. The chapters that follow unpack these data points in detail, showing how AI risk accumulates, where visibility breaks down, and what effective governance looks like in practice.

100%
of analyzed organizations operate SaaS environments with embedded AI

139.5
AI-enabled SaaS environments per organization

3,891
average SaaS environments per enterprise

490%
year-over-year spike in public SaaS attacks

80%
of documented incidents involve PII and/or customer data

<NOTE>
"Attacks" and "incidents" refer to documented SaaS and AI-related events observed or aggregated by Grip's telemetry and incident dataset (see Methodology).

<SALESLOFT DRIFT: A WARNING SIGNAL>

AI has reshaped the risk landscape, with third-party SaaS integrations now the most common delivery path for enterprise exposure. The August 2025 Salesloft–Drift breach offered a clear preview of what's ahead. A single set of stolen OAuth credentials triggered cascading impact, exposing hundreds of millions of records across thousands of connected services, including Google, Salesforce, Cloudflare, Palo Alto Networks, and Zscaler. This is the moment for leaders to reassess the sprawl of SaaS integrations quietly introducing opaque third-party risk across the organization.

Learn more about the Salesloft Drift breach at grip.security or info@grip.security

<BOARD CALL OUT>

AI risk is already material, operational, and systemically embedded.

23,021
SaaS + AI apps analyzed without SSO or approved adoption.

CHAPTER 01

VISIBILITY BEFORE POLICY

THE STARTING POINT FOR AI GOVERNANCE

<KEY TAKEAWAYS>

- AI adoption is already embedded across the enterprise, largely outside direct executive control
- SaaS vendors, not internal teams, are driving the pace and scope of AI introduction
- Visibility, not policy, is now the starting point for AI governance

<KEY STATS>

Grip's analysis found that embedded AI is now universal across enterprise SaaS environments, operating at a scale that outpaces traditional governance:

100%

of analyzed organizations operate SaaS environments with known, embedded AI components

139.5

AI-enabled SaaS environments per organization

Many teams still believe AI adoption is a strategic choice they can plan, approve, and control. In practice, AI is already embedded across the business through the SaaS environments employees rely on every day, making adoption less a decision and more an operating reality. AI agents introduce a new level of risk.

Unlike human users, agents operate continuously, act autonomously and unpredictably, and often retain long-lived access through tokens or OAuth grants. This allows them to move data, trigger actions, and make decisions at machine speed, dramatically increasing blast radius when governance is absent.

<BOARD CALL OUT>

The greatest AI risk is not internal development, it is uncontrolled adoption through third-party SaaS.

<MOST RISKY AI COMPONENTS IN SAAS>

These components introduce persistent access, automated decision-making, and data movement that often operate beyond traditional security and governance review.

Agents

Non-Human Identities (NHIs)

Copilots

API-Connected Integrations

Browser Extensions

AI has not entered the enterprise through a single initiative or formal rollout. It arrives quietly through vendor product updates, embedded features, copilots, and integrations that expand functionality without explicit approval or contract changes.

These additions frequently bypass legal review, security assessments, and governance workflows, creating an illusion of control even as AI usage grows underneath.

As a result, many AI decisions are effectively being made by SaaS vendors rather than by the organization itself. This introduces risk across data handling, identity access, compliance, and customer trust, often without leadership awareness.

The good news? Executives who recognize this early gain a meaningful advantage, shifting from reacting to unknown AI usage to governing it deliberately, protecting innovation while retaining control of the business.

SAAS AS THE AI RISK DELIVERY SYSTEM

<KEY TAKEAWAYS>

- SaaS has become the primary delivery mechanism for AI into the enterprise, often without explicit approval.
- Every SaaS vendor is now an AI vendor, extending third party risk far beyond procurement visibility.
- AI risk scales at SaaS speed, faster than traditional oversight, controls, or governance models.

<KEY STATS>

9 Average SaaS environments per customer exposed by the SalesLoft–Drift breach

3,891 Average SaaS environment footprint per organization analyzed

23,021 SaaS environments used with no SSO or approved adoption

SaaS fundamentally changed how software enters the enterprise. It removed friction from purchasing, deployment, and adoption, shifting control away from centralized IT toward business teams and individual users. AI accelerates this shift even further.

<BOARD CALL OUT>

AI Risk = (SaaS Scale) × (AI Depth)

Where SaaS made software easy to buy, AI makes decisions easy to outsource, embedding automated logic directly into everyday business workflows.

The result is a new third party risk model that most organizations did not plan for. Each SaaS environment is no longer just a tool, it is now a potential AI provider making decisions, processing sensitive data, and influencing outcomes outside direct enterprise control. Every embedded AI feature introduces new data flows, new training exposure, and new decision logic, often governed by vendor policies rather than internal standards.

Risk compounds quickly in highly integrated SaaS environments. Shadow SaaS becomes shadow AI, and interconnected environments amplify exposure across identity, data, and access paths.

As the Salesloft Drift breach demonstrated, what appears as a single vendor relationship at the board level can represent dozens of AI-driven integrations operating beyond visibility, creating inherited risk that scales faster than governance can react.

HOW GRIP HELPS

- Discovers AI adoption at its root: SaaS environments
- Establishes an enterprise-wide baseline of AI adoption tied to real usage, access, and data

WHERE AI RISKS ACTUALLY LIVE

<KEY TAKEAWAYS>

- AI risk is not being ignored, it is being missed by design.
- Governance programs focus on approved tools, while real AI usage lives elsewhere.
- Executives cannot manage AI risk until it is made visible across identities, browsers, and integrations.

<KEY STATS>

UNSEEN POINTS OF EXPOSURE, AVERAGE PER ORGANIZATION

514
Average OAuth grants

49,856
OAuth grants actively used by identities

67%
Organizations with at least 1 risky OAuth scope

Most AI governance efforts begin with good intent.
Organizations create policies, reviews, and committees focused on officially approved AI tools.
But approved AI tools are not the core problem.
The problem is structural.

<BOARD CALL OUT>

The greatest AI risk is not misuse.
It is unmanaged use.

AI usage does not concentrate where governance expects to find it. It spreads quietly through embedded features, OAuth connections, browser extensions, and user-driven workflows that sit outside formal approval paths.

This creates a dangerous governance blind spot.

OAuth grants provide persistent access to sensitive systems, while browser extensions introduce AI capabilities directly into daily workflows. Yet these entry points rarely trigger security or legal review, even as they become the places where AI operates most freely.

As AI feature releases accelerate, guidance and adoption controls built for pre-AI landscape simply cannot keep pace. New AI capabilities appear through routine SaaS updates, not new procurement cycles. The result is shadow AI at scale, unmanaged usage embedded deeply into the enterprise operating fabric.
Until organizations confront this visibility gap, AI risk will continue to grow quietly, unchecked, and misunderstood at the executive level.

HOW GRIP HELPS

- Continuously discovers AI tenants, embedded features, and integrations across SaaS
- Identifies AI operating outside security, legal, and governance review
- Exposes hidden AI risk across identities, OAuth grants, and browser extensions

LEGACY CONTROLS

BUILT FOR A WORLD THAT NO LONGER EXISTS

<KEY TAKEAWAYS>

- Traditional security controls were built for a centralized world and no longer cover SaaS- and AI-driven risk on their own
- The control gap stems from tools not built for SaaS and AI context, not from failed implementation
- Security must shift from static controls to continuous, identity-aware governance

Traditional security models were designed for centralized, predictable IT environments, where applications, users, and data lived inside clearly defined boundaries. As SaaS and AI have reshaped how work gets done, many long-standing security practices still play an important role, but they no longer deliver the coverage or control required to manage modern enterprise risk on their own.

The result is not a failure of individual tools, but a growing mismatch between how security is applied and how today's environments actually operate.

>> PERIMETER-FIRST SECURITY

Designed for on-premise networks and fixed locations, perimeter controls break down in SaaS-first, remote environments where identities, data, and AI workflows live entirely outside the network. Protections are still necessary, but no longer sufficient, as identity and access have become the true enforcement plane.

>> CASB / SSE / SASE / EDGE SECURITY PLATFORMS

These solutions are powerful but complex, often generating high volumes of noise and requiring significant tuning, integration, and operational maturity. They work best for organizations with large budgets and specialized teams, leaving most enterprises under-protected or partially deployed.

>> ENDPOINT SECURITY (EDR\XDR)

Endpoint tools are highly effective at protecting managed devices, but they provide limited visibility into SaaS-to-SaaS activity, API integrations, browser extensions, and non-human identities (NHI). Critical risk now lives well beyond the endpoint, where these tools have no reach.

>> IAM-ONLY SECURITY MODELS

Identity platforms control access at login, but they rarely provide ongoing visibility into what users, agents, and integrations actually do once access is granted. Without continuous monitoring and context, excessive permissions and risky behavior go undetected.

>> VENDOR QUESTIONNAIRES AND SELF-REPORTED INVENTORIES

Annual reviews and attestations rely on incomplete, outdated, or optimistic reporting that cannot keep pace with the speed of SaaS and AI adoption. By the time risk is documented, environments have already changed.

>> MANUAL GOVERNANCE AND POLICY ENFORCEMENT

Spreadsheet-driven inventories and human-led approval workflows cannot scale to thousands of environments, embedded AI features, and automated integrations. Governance becomes reactive, fragmented, and disconnected from real usage.

YOUR SAAS + AI FOOTPRINT IS BIGGER THAN YOU THINK

<KEY TAKEAWAYS>

- Your SaaS and AI footprint is far broader than approved tools and vendor lists suggest.
- AI is embedded inside trusted, everyday SaaS environments, not just standalone AI tools.
- Visibility, not policy, is the first prerequisite to securing AI-driven environments.

AI Governance teams often believe they understand their SaaS and AI environment because they know the major platforms the business depends on. The reality is very different. You cannot secure what you cannot see, and most organizations have never actually seen their full SaaS and AI footprint laid out end to end.

< 10 MOST COMMON SAAS AND AI ENVIRONMENTS IDENTIFIED:

pdfFiller · BROADCOM · wrike · ups · grammarly · amazon · ATLASSIAN · Lucid · monday.com · zapier

<BOARD CALL OUT>

Lack of end-to-end SaaS and AI visibility has turned shadow adoption into widespread enterprise risk.

The fastest way to understand this gap is to look at real world adoption. The most common SaaS and AI environments span productivity, HR, marketing, learning, travel, infrastructure, and automation. Many are household names, deeply trusted, and widely deployed.

What is less obvious is how extensively AI is embedded inside these platforms, influencing content creation, decision making, automation, and movement of data without triggering separate approval or review.

This is the blind spot leaders must confront. Your environment likely looks like this list, broad, diverse, and interconnected, even if your official inventory suggests otherwise.

AI does not arrive labeled as "AI risk." It arrives quietly inside platforms the business already trusts, and it scales before governance ever catches up.

< TOP 10 SAAS AND AI ENVIRONMENTS WITH THE LARGEST USER BASES IDENTIFIED:

GitLab · Informatica · splunk> · qualtrics.XM · WordPress · monday.com · Jenkins · amazon · ATLASSIAN · Lucid

HOW GRIP HELPS

- Continuously discovers every SaaS environment and embedded AI capability
- Identifies where AI is embedded inside commonly trusted SaaS environments
- Correlates SaaS and AI adoption to real user activity and behavior
- Connects visibility directly to risk context, prioritization, and action

SAAS + AI INCIDENTS ARE BUSINESS INCIDENTS

<KEY TAKEAWAYS>

- AI is no longer an experimental or future risk, it is already driving real business incidents.
- AI failures rarely look like classic cyberattacks, they surface as data exposure, compliance failures, and loss of trust.
- Executive teams must treat AI incidents with the same seriousness as financial, legal, and operational events.

<KEY STATS>

56 SaaS environments exposed per customer during incidents

68% Documented breaches exposing PII

80% Incidents involving PII and or customer data

490% Increase in public SaaS attacks from 2024 to 2025

<BOARD CALL OUT>

Most AI incidents won't trigger an alert. They'll trigger a headline.

For years, AI risk was discussed as experimental, theoretical, or future-facing. That era is over. AI is now fully embedded across SaaS environments that run core business processes, putting the technology in direct contact with customer data, employee records, intellectual property, and regulated systems.

The most common AI incident pattern today is subtle: an embedded AI feature gains access through an OAuth grant, processes or exposes sensitive data, and propagates impact across connected SaaS environments. Because these failures rarely resemble classic attacks, they often bypass SOC tooling entirely and surface through audits, customers, or regulators, rather than traditional security alerts.

When AI controls fail, the impact isn't simply technical. The fallout can expose sensitive data, disrupt core business operations, and erode trust.

But risk isn't solely defined by proximity to sensitive data. AI-driven incidents rarely resemble traditional breaches. There may be no ransomware note, no obvious system outage, and no immediate security alert. Instead, the damage often appears as unintended data leaks through prompts or training, compliance violations tied to data handling, or third-party exposure that ripples across integrated SaaS environments.

As SaaS and AI environments become more interconnected, scale amplifies the risk. A single failure can expose dozens of environments and tens of thousands of identities at once. This is why AI incidents increasingly surface in board discussions, audit findings, and public headlines. Which means AI risk isn't contained by technical controls alone. It becomes a leadership issue, whether teams are prepared or not.

HOW GRIP HELPS

- Detects AI data access and misuse patterns across SaaS environments
- Identifies AI driven exposure involving PII, customer data, and sensitive systems
- Supports audit, legal, and regulatory evidence for AI governance and incident response

HOW SAAS + AI RISK VARIES BY INDUSTRY

<KEY TAKEAWAYS>

- SaaS and AI adoption is universal, but risk exposure varies dramatically by industry.
- Highly regulated sectors show some of the highest levels of shadow SaaS and shadow AI usage.
- Industry leaders are not reducing AI adoption, they are working with technology partners to help them govern it with visibility and control.

<KEY STATS>

Accelerating Industry Adoption of Shadow SaaS and AI Environments

	% SHADOW APPS	YOY ADOPTION INCREASE
MANUFACTURING	89%	52%
INSURANCE	88.7%	42.1%
RETAIL	90.2%	50.6%
FINANCE	89.1%	39.3%
HOSPITALS & PHYSICIAN CLINICS	87.7%	46.5%
SOFTWARE	89.4%	36.6%
BUSINESS SERVICES	89.4%	35.2%
HOSPITALITY	82.4%	33.4%
REAL ESTATE	92.4%	48.3%
TELECOMMUNICATIONS	84.6%	51.2%

<BOARD CALL OUT>

Industry leaders don't differ in AI adoption. They govern it better.

SaaS and AI adoption has become table stakes across every industry. From manufacturing floors to hospital systems, from financial services to retail operations, SaaS environments and embedded AI capabilities now underpin daily business execution.

What differs sharply is not whether AI is used, but how much of that usage is visible and governed.

Highly regulated industries consistently show some of the highest levels of shadow SaaS and shadow AI adoption.
Manufacturing, finance, healthcare, and insurance environments combine complex operational systems with aggressive SaaS growth, creating sprawl that far outpaces formal oversight.

Managed AI adoption remains a small fraction of total usage, even as year-over-year growth accelerates across nearly every sector.

This uneven risk profile explains why peer comparisons matter at the executive level. Leaders often assume their organization is uniquely exposed, or uniquely behind. The data shows a different reality. Most peers are adopting AI at similar speed. The differentiator is governance maturity, the ability to see what is actually in use, understand where data and decisions flow, and apply controls proportionate to industry specific risk.

HOW GRIP HELPS

- Provides industry specific SaaS and AI risk benchmarks grounded in real usage
- Enables peer comparison without guesswork or self reporting bias
- Helps executives understand where their organization sits relative to industry norms and leaders

FROM VISIBILITY TO CONTROL

OPERATIONALIZING SAAS + AI GOVERNANCE

<KEY TAKEAWAYS>

- The path forward is control through visibility and continuous oversight.
- Winning organizations govern AI where it actually lives: inside SaaS, identities, and integrations.
- AI governance succeeds when treated as third party risk management, not innovation theater.

<KEY OBSERVATIONS>

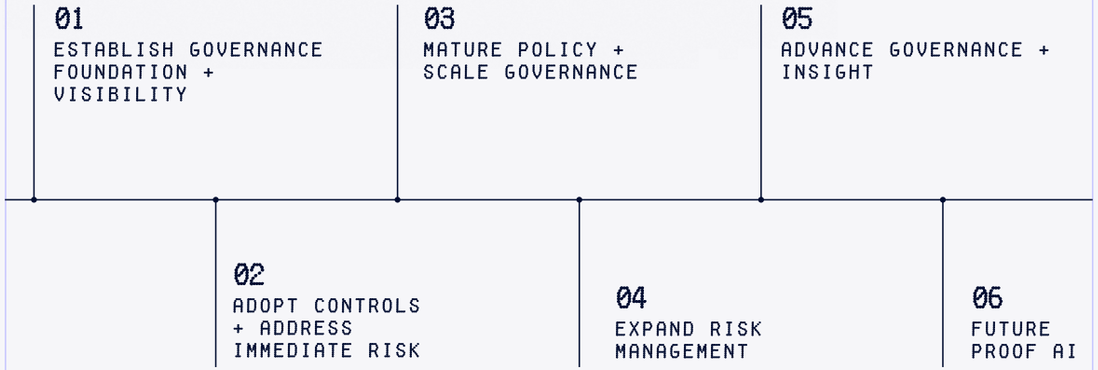
- **AI ADOPTION** continues to outpace formal governance by multiples, driven by SaaS updates and integrations.
- **AI USAGE REMAINS UNMANAGED** at the point of identity, access, and data flow.
- **CONTINUOUS DISCOVERY AND OVERSIGHT** reduce downstream audit, incident, and response costs.

Most executives arrive at AI governance conversations after a period of anxiety. The environment feels chaotic, adoption appears uncontrolled, and risk seems to be accelerating faster than teams can respond. The way out is not more policy or slower innovation. It is a shift in how AI is governed in practice.

<BOARD CALL OUT>

AI adoption is unavoidable. Governance determines whether it creates value or risk.

< 6 PHASES OF AI GOVERNANCE >



Winning organizations start by accepting reality. Governance must move to where AI actually operates. That means treating AI as part of the SaaS and identity strategy, not a standalone initiative owned by a single team or committee.

The most important shift is operational. Approval-based models break down at SaaS speed.

AI features change weekly, integrations appear daily, and users adapt faster than governance cycles can approve.

Leaders who succeed replace static approvals with continuous oversight, discovery, and risk-based controls. AI becomes a managed third-party risk, monitored continuously, aligned to business outcomes, and governed with the same rigor as any critical supplier.

HOW GRIP HELPS

- Delivers unified visibility across SaaS, AI, identities, and integrations
- Enables continuous governance aligned to real business risk and outcomes
- Acts as a control plane for the AI enabled enterprise, replacing chaos with control

SAAS + AI TRENDS TO WATCH IN 2026

01

SAAS BREACHES ACCELERATE AS AGENTIC CORES EXPAND

Agentic AI is rapidly increasing SaaS blast radius. After a 490% year-over-year breach increase in 2025, 2026 is likely to push even higher limits as autonomous workflows outpace existing security controls.

02

THIRD PARTY RISK BECOMES THE BREACH EPICENTER

Cascading failures move from edge case to norm. Incidents like Salesloft Drift signal how a single vulnerability can expose thousands of interconnected customers almost instantly.

03

AI SECURITY PLATFORMS TRIGGER TOOL CONSOLIDATION

CISOs cannot buy, integrate, or operate dozens of niche tools. Expect rapid consolidation as AI Security Platforms absorb point solutions across AI discovery, agent analysis, identity risk, and automated response.

04

AI REGULATION GETS MESSIER BEFORE IT GETS CLEARER

US states, federal agencies, and global regulators are moving in different directions. Conflicting mandates, unclear scope, and uneven enforcement will increase compliance friction throughout 2026.

05

AI ADOPTION GIVES WAY TO AI GOVERNANCE

After two years of unchecked expansion, organizations shift focus from enablement to control. CISOs increasingly partner with roles like VP of AI Governance to rein in risks ignored during adoption momentum.

06

IDENTITY BECOMES THE CONTROL PLANE FOR AI RISK

As agents, tokens, and non-human identities proliferate, identity sprawl becomes the primary amplifier of AI-driven risk. Security programs pivot toward identity centric visibility to understand who or what can act, access data, and make decisions.

07

BOARDS DEMAND AI RISK ANSWERS, NOT EXPERIMENTS

"What AI do we use?" becomes "What AI can hurt us?" Boards will increasingly demand measurable risk reduction, clear ownership, and defensible governance, not experimentation.

AI risk is already embedded in your SaaS environment. The difference in 2026 will be who can see it, measure it, and govern it with confidence. Grip gives security and business leaders a unified control plane for SaaS and AI risk, turning uncertainty into visibility and visibility into control.

AI IS PART OF HOW YOUR BUSINESS OPERATES. GRIP HELPS YOU CONTROL IT.

LEARN MORE AT

- grip.security
- info@grip.security

BOARD-LEVEL QUESTIONS FOR SAAS + AI GOVERNANCE

AI adoption throughout SaaS environments has accelerated faster than governance capabilities, creating explosive risk that is already embedded in everyday business operations. These questions help boards assess how their teams are taking the concrete actions needed to discover, measure, and control that risk in practice.

- How do we determine where AI is embedded in the SaaS environments we use?
- How do our teams identify AI usage that operates outside approved or managed adoption paths?
- How do we inventory and govern non-human identities and AI agents?
- How do we assess and control OAuth grants and third-party integrations?
- How do we validate what data AI systems can access and act on?
- How do we detect AI-driven risk that won't trigger traditional security alerts?
- How do we measure AI risk in a way that can be tracked over time?
- How do we evaluate exposure to cascading third-party AI incidents?
- How do we ensure clear ownership and accountability for AI governance outcomes?
- How do we adapt governance as SaaS and AI change week to week?

SAAS + AI GOVERNANCE CHECKLIST

This checklist outlines a practical, early-to-mid stage framework for governing AI across SaaS environments, turning scattered AI usage into measurable, defensible control without slowing the business.

- [ ] **Establish AI Governance Ownership**
  Grip's AI dashboard provides a shared system of record for AI oversight across teams and supports executive-level visibility into AI risk posture.
- [ ] **Discover AI and Shadow AI Usage**
  Grip continuously discovers AI tools, embedded AI features, OAuth integrations, and extensions across SaaS environments, exposing Shadow AI that exists outside approved workflows.
- [ ] **Map AI to Identity, Access, and Data**
  Grip correlates AI tools to real user identities, permissions, and connected data sources to show who can access what data through AI.
- [ ] **Classify and Tier AI Risk**
  Grip applies risk scoring and tiering based on usage patterns, access levels, and data exposure, enabling risk-based governance instead of blanket restrictions.
- [ ] **Define and Enforce AI Usage Policies**
  Grip translates AI governance policies into enforceable workflows that flag, restrict, or remediate risky AI usage across SaaS and AI tools.
- [ ] **Enable Safe AI Adoption**
  Grip allows approved AI tools and use cases to be enabled with guardrails, reducing the likelihood that employees turn to unsafe alternatives.
- [ ] **Prepare for AI Incidents**
  Grip provides incident-ready context showing which users accessed which AI tools, what data was involved, and how exposure occurred, accelerating response and investigation.
- [ ] **Monitor AI Behavior Continuously**
  Grip continuously monitors AI usage, new integrations, permission changes, and embedded AI feature expansion to detect drift and emerging risk.
- [ ] **Reevaluate AI Governance Every 90 Days**
  Grip trend reporting and historical visibility allow teams to reassess AI adoption, risk posture, and policy effectiveness on a quarterly cadence.
- [ ] **Align AI Governance to Business Outcomes**
  Grip ties AI risk to business impact by highlighting where AI access and exposure intersect with critical operations, financial systems, and sensitive data.

READY TO OPERATIONALIZE AI GOVERNANCE?

Grip delivers continuous visibility, risk-based control, and board-ready insight across your AI-enabled SaaS ecosystem.

LEARN MORE AT

- grip.security
- info@grip.security

METHODOLOGY

This report is based on aggregated, anonymized telemetry and risk analysis drawn from real world enterprise SaaS environments monitored by Grip Security. The data reflects observed SaaS and AI usage, identity activity, integrations, and risk signals across a diverse set of organizations, industries, and company sizes. Rather than relying on surveys or self reported inventories, the findings are grounded in direct observation of how SaaS environments, embedded AI features, OAuth grants, browser extensions, and non human identities are actually used in production environments.

Metrics and benchmarks in this report were calculated by normalizing data across customer environments and analyzing trends over time, including year over year adoption growth and incident exposure patterns. Where industry comparisons are presented, organizations were grouped by primary sector to highlight differences in adoption scale, visibility, and unmanaged risk. All insights are presented in aggregate to protect customer confidentiality, with a focus on identifying systemic patterns that affect executive decision making, AI governance strategy, and enterprise risk management rather than individual company performance.

SPECIAL THANKS

Special thanks to the Grip Security Engineering Team and Data Analysis Team, whose expertise and collaboration made this report possible.

In particular, **Brian Conry**, **Amit Muzikanski**, **Yanay Granit**, **Daniel Engelke, Chad Holmes, Margo Shramchenko, Aviv Sinai** and **Vicki Michaeli** played a critical role in bringing the insights in this report to life.

grip

FROM CHAOS TO CONTROL

GOVERNING SAAS + AI RISK
ACROSS THE MODERN ENTERPRISE