AI Risk and Implementation Assessment: Zapier

Appendix

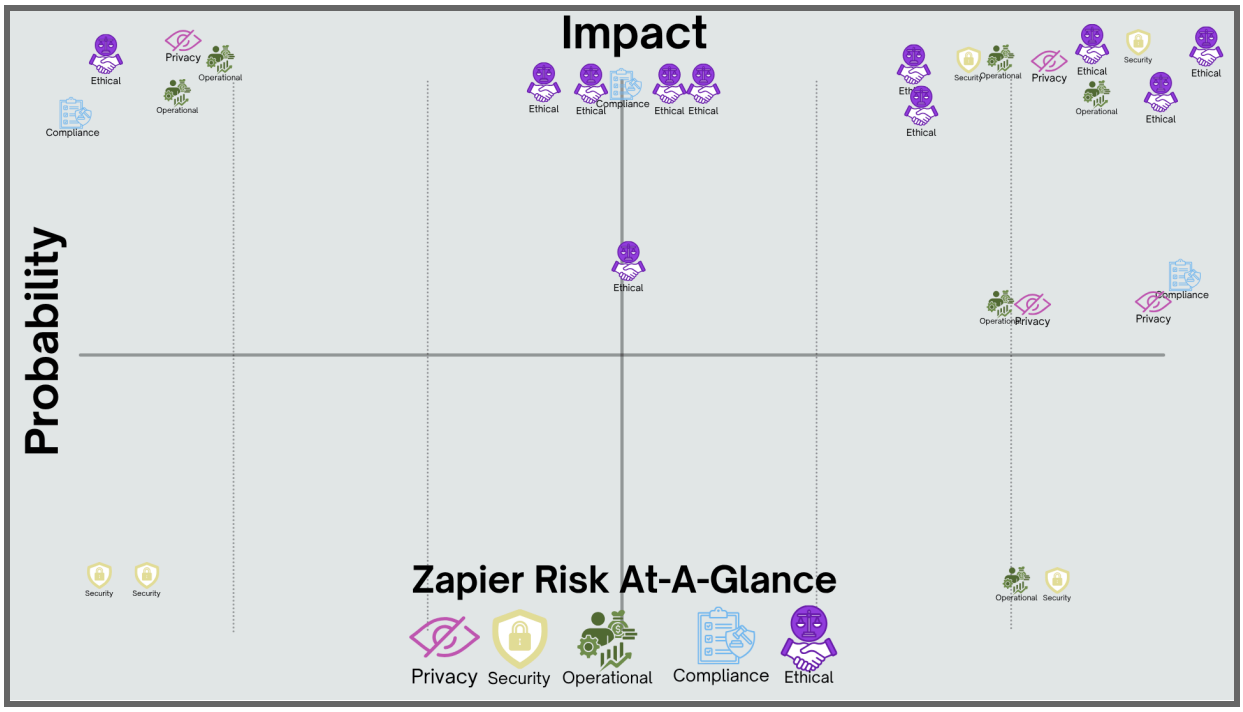

Figure 1: Zapier's Probability and Impact Matrix. Figure shows the probability and impact of 27 identified risks, grouped by the risk category so organizations know where to focus their governance and risk mitigation strategies.

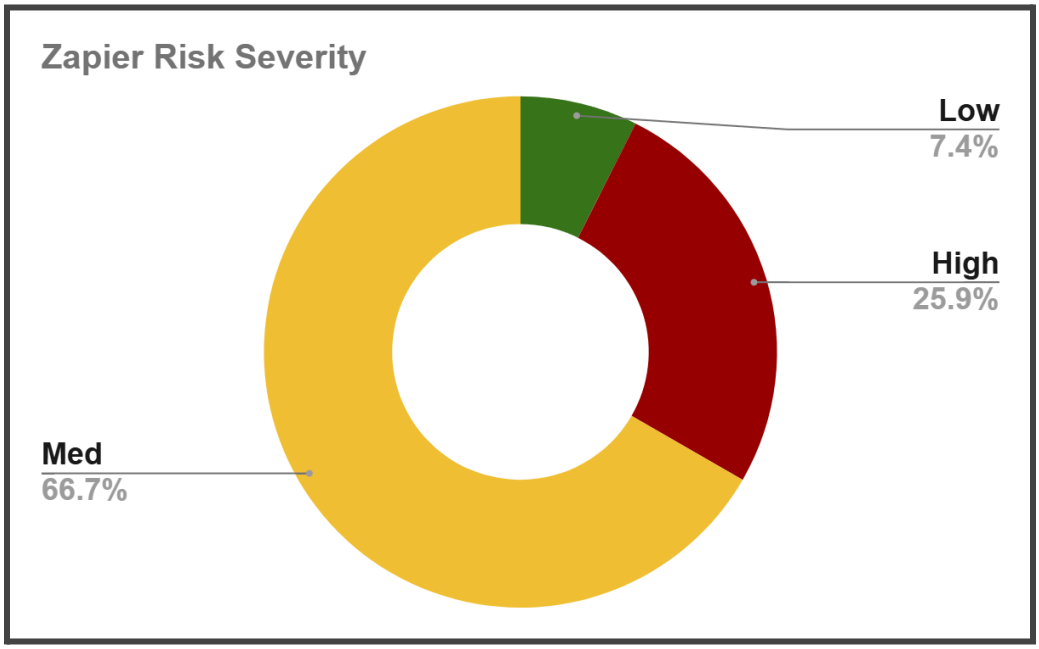

Figure 2: Zapier's Risk Severity. Figure shows that integrating Zapier into an organization has a balanced risk posture, with most risk falling in the mid-range category for impact and likelihood of occurrence.

Top 5 Critical Risks

RISK #	RISK CATEGORY	IDENTIFIED RISK	PROBABILITY	IMPACT	RISK RATING
R1	Privacy Ethical	Data Flow and Contextual Integrity	High	High	3
R2	Security	Data Exposure and Storage	High	High	3
R3	Operational	System Reliability and Validity	High	High	3
R4	Operational Ethical	Transparency, Explainability, & Interpretability and Socio-Technical Accountability	High	High	3
R5	Ethical	Job Displacement and Transparency	High	High	3

Table 1: Top 5 Critical Risk of Zapier adoption. Rating schema 1=Low, 2=Med, 3=High

27 Identified Risks

RISK #	RISK CATEGORY	IDENTIFIED RISK	PROB-ABILITY	IMPACT	RISK RATING
R6	Ethical	Algorithmic Guardrails	High	High	3
R7	Security	Weak Authentication	High	High	3
R8	Privacy	Model Training and Data Usage	High	Low	2
R9	Privacy	Third-Party Sharing	High	Low	2
R10	Privacy	Partnerships	Med	High	2
R11	Security	Real-Time Data Failures	Low	High	2
R12	Operational	Vendor Dependency	Low	High	2
R13	Operational Ethical	Skills Atrophy	Med	High	2
R14	Operational	Intellectual Property Usage	High	Low	2
R15	Operational	Increased Costs	High	Low	2
R16	Compliance	Shared Responsibility without control	High	Low	2
R17	Compliance	Accountability	High	Med	2
R18	Compliance	Regulatory Knowledge Gaps	Med	High	2
R19	Ethical	AI-First Culture Over Human-Centricity	High	Med	2
R20	Ethical	Internal Workforce Bias	High	Med	2
R21	Ethical	Informed Consent	High	Low	2
R22	Ethical	Model Training and Data Usage	High	Med	2
R23	Ethical	Creative Agency and Intellectual Property	High	Med	2
R24	Ethical	Paradox of Normalization	Med	Med	2
R25	Ethical	Ecological Cost and Planetary Boundaries	High	Med	2
R26	Security	Technical Vulnerabilities	Low	Low	1
R27	Security	Encryption and API Risks	Low	Low	1

Detailed Risk Considerations and Implications

RISK CATEGORY	IDENTIFIED RISK	CONSIDERATIONS AND IMPLICATIONS
Security	Authentication Weaknesses	While Zapier recommends Two-Factor Authentication (2FA), it is not compulsory. A historical breach was specifically traced back to a 2FA misconfiguration on an employee account, causing potential harm to those whose data was leaked.
Security	Technical Vulnerabilities	Security reports identify several technical risks, including unsafe Content Security Policy (CSP) implementation (increasing XSS risks), lack of HTTP Only cookies, and the absence of DNSSEC, which could allow third parties to forge domain records.
Security	Encryption and API Risks	Use of weak cipher suites in TLS 1.2 and the increased attack surface created by every third-party integration pose ongoing security challenges.
Security	Real-Time Data Failures	Generally speaking, if automation tools do not use real-time data, there's an increased risk of failure to detect critical threats or zero-day vulnerabilities, leading to unnoticed exploitation.
Security	Data Exposure and Storage	Historical security reviews highlight that Zapier has utilized "global storage" where weak, user-chosen keys could allow unauthorized access to PII and authentication tokens. Additionally, a 2025 breach revealed that customer data had been inadvertently copied to repositories for debugging purposes. Again, what are the safety ramifications of this potential data exposure.

Table 2 lists each risk, its category, implications and considerations. Yellow = Security, Green = Operational, Blue = Compliance, Purple = Ethical

RISK CATEGORY	IDENTIFIED RISK	CONSIDERATIONS AND IMPLICATIONS
Operational	Vendor Dependency and Lock-in	Heavy reliance on Zapier creates a risk where downtime, incidents, or broken workflows at Zapier directly disrupt the organization's functions. There are also concerns regarding what happens to "Zaps" and agents if a company decides to leave the platform.
Operational	Skills Atrophy	Over-reliance on automation can lead to declining manual troubleshooting skills among staff, making it harder for them to intervene when automated systems encounter unexpected issues.
Operational	System Reliability and Validity	Zapier workflows often fail due to issues with API rate limits, changes in connected apps, and authentication failures. This poses a significant risk as organizations face decreased productivity as a result of intermittent failures. At times, Zapier automation tools may recommend inaccurate or incorrect automations, so it is critical for organizations to add human oversight and monitoring to reduce the probability of less than optimal automations. Additionally both the automation zaps or triggers may fail and so organizations must 1) identify what low risk tasks should be considered for automation, 2) pilot those automations, and 3) develop processes to monitor automation workflows to prevent the most damage
Operational	Intellectual Property Usage	Zapier’s Terms of Service allow them to use customer logos and trademarks for marketing purposes without compensation or prior consent. Additionally, an organization's reputation is used before they even have a chance to rate the platform.
Operational	Transparency, Explainability, and Interpretability	For many basic automations in Zapier, such as drafting an email at a specific time each day is fairly straightforward based on the input. However, agents, created by organizations to make decisions pose operational risks related to transparency, explainability, and interpretability. Since Zapier's AI automations and agents have black box capabilities, it's the logic and reasoning for certain decisions is unknown. This poses a risk for the organization when the responsible party cannot explain why a decision was made or an automation was executed.
Operational	Maintenance Costs	Hidden costs range from implementation and sustainment. Implementation costs include: resources allocated to research, workflow creation, organizational design, and training. Sustainment costs include the labor required for troubleshooting broken workflows, API failures, downtime for Zapier security incidents, and consistent updates to maintain compatibility between platforms.

RISK CATEGORY	IDENTIFIED RISK	CONSIDERATIONS AND IMPLICATIONS
Compliance	Shadow AI	Approximately 63% of practitioners report using unapproved AI tools, and 51% of leaders admit governance frameworks are lagging, indicating a significant compliance gap with either internal procedures, sector regulations or jurisdictional laws. Organizations should not adopt Zapier without first assessing and evaluating their internal compliance management and governance culture.
Compliance	Shared Responsibility	Under Enterprise Agreements, confidentiality is a joint responsibility, meaning the customer shares the burden of protecting sensitive information alongside Zapier.
Compliance	Accountability	Organizations have to develop clear guidelines and processes that ensure ownership and accountability measures are in place when using agents. Zapier agents can be created in a team environment, meaning multiple individuals possess the authority to create, modify, and delete automations and agents. Due to the accessibility to CoPilot in Zapier, anyone in an organization can create automations or agents in a matter of minutes. However, there are risk associated with this type of creative freedom when something inevitably goes wrong.
Compliance	Regulatory Knowledge Gaps	There is a risk that implementation partners (like SoftSnow) may not fully understand geographical or industry-specific laws when redesigning workflows, potentially leading to non-compliance.

RISK CATEGORY	IDENTIFIED RISK	CONSIDERATIONS AND IMPLICATIONS
Ethical	Human-Centricity vs. AI-First	Concerns exist regarding Zapier's partnership with SoftSnow, whose mission is to rapidly scale "AI-First" cultures across organizations. This may be a potential risk depending on an organization's existing culture and values. If an organization's goal is rapid AI acceleration, then this may not pose a risk; however, organizations should be cautious about quick, large-scale workflow overhauls that may prioritize tools over people, potentially leading to reduced employee engagement or a feeling that work has become mechanical.
Ethical	Job Displacement and Transparency	While automation can free up cognitive space for innovation, it also carries the fear of job loss if not managed with clear communication and change management. Psychological safety is disrupted when advanced AI tools, such as Zapier, are integrated without effective organizational development practices
Ethical	Internal Workforce Bias	Organizations may face a decrease in organizational morale, team cohesiveness, and employee engagement by adopting Zapier. There may be perceived bias, discrimination when organizations determine who and what functions will be authorized to use automation and/or agents and be considered for workflow redesigns.
Ethical	Algorithmic Guardrails	Zapier's Acceptable Use Policy prohibits using AI for exploiting targeted groups, doxing, or high-risk automated decisions without a human in the loop, yet the responsibility for enforcing ethical algorithm guardrails often falls on the user.
Ethical	Informed Consent	The Cookie Notice uses vague language regarding how disabling functional cookies impacts specific services, which may prevent users from making fully informed decisions. This is a concern for smaller businesses that do not have dedicated security support and governance.
Ethical	Model Training and Data Usage	Zapier's Data Protection Addendum indicates user data and de-identified "derived data" may be used for model training. This poses ethical considerations, since Zapier benefits from the model training and the owner of the data is not compensated.
Ethical	Socio-Technical Accountability	Due to Zapier's black box capabilities, Zapier's agents may make biased and discriminatory decisions. By the time the organization realizes, the damage has likely been done.

RISK CATEGORY	IDENTIFIED RISK	CONSIDERATIONS AND IMPLICATIONS
Ethical	Labor Replacement vs. Compensation	As organizations use Zapier automation and agents for productivity gains, it is inevitable for tasks to be redistributed from the employees to AI. However, organizations are using employee-derived data (communications, logic, templates, etc.) to train the Zapier agents. This results in a potential ethical risk of replacing employees without compensating them for their hours, data, ideas, solutions, and voice.
Ethical	Creative Agency and Intellectual Property	Using AI-enabled tools poses risk to human agency for employees. Organizations run the risk of infringing on creative and artistic agency when automation and AI-agents become company requirements. Organizations must address the risk of creating a culture of disengaged talent because ambitious and purpose-driven employees may prefer to perform functions without AI. Though the employee isn't replaced, they may lose their sense of agency which may have psychological impacts.
Ethical	Contextual Integrity	Companies should be aware of privacy and data protection requirements for their customers when using Zapier. The risk of handing over customer data to a third-party platform that also uses third party applications poses data flow risks (i.e. data being used outside of its original intended context)
Ethical	Paradox of Normalization	By automating individual functions/tasks, organizations run the risk of becoming less diverse, inclusive, and innovative. Work tasks, processes, and products managed by Zapier automations and agents may result in bias against individuals whose work styles or products vary from the automated standard or the "norm". There is risk of becoming homogenous and stagnant if AI becomes the only standard.
Ethical	Ecological Cost and Planetary Boundaries	Specific carbon footprint, water usage, and other planetary costs for Zapier were nonexistent. Zapier does not have any environmental or sustainability policies publicly shared, so organizations that value sustainability will need to consider the risk of AI-powered automation to the environment. Organizations run the risk of automating processes en masse that return minor efficiency and productivity gains, while depleting planetary resources.

Phased Rollout Timeline

Phase 1: Foundation & Pilot (Months 1-2)

Goal: Establish governance infrastructure and test with low-risk department

Month 1: Governance Infrastructure Setup

- **Establish Zapier Center of Excellence (CoE)**
  - Identify CoE members (IT lead, business process owner, compliance, security)
  - Define roles, meeting cadence, decision-making authority
  - Set up communication channels (Slack/Teams, email distribution)
- **Develop core governance documents**
  - Zapier Acceptable Use Policy
  - Approval workflow process
  - Risk assessment template
  - Incident response playbook
- **Technical setup**
  - Configure Zapier Enterprise settings (SSO, user provisioning, audit logs)
  - Set up monitoring dashboards
  - Create approval ticketing system

Month 2: Pilot Department Launch

- **Select pilot department** (criteria: tech-savvy, low-risk processes, supportive leadership)
- **Conduct pilot kickoff meeting**
  - Share vision: "Help us design governance that enables innovation"
  - Set expectations: "We'll learn together and refine processes"
- **Pilot activities**
  - Train 10-15 pilot users on governance + Zapier
  - Create 5-10 pilot automations through new approval process
  - Weekly check-ins: What's working? What's frustrating?
- **Learning capture**
  - Document pain points in approval process
  - Refine governance policies based on feedback
  - Identify champions for next phase

Deliverables:

- CoE operational
- Governance policies v1.0 published
- 5-10 governed automations live
- Lessons learned report

Success Metrics:

- Pilot users report governance process as "manageable" (survey)
- 80% of pilot Zaps approved within 48 hours
- Zero high-risk automation incidents

Phase 2: Expanded Pilot (Months 3-4)

Goal: Validate governance at moderate scale, refine processes

Month 3: Expand to 3 Departments

- **Select departments with different use cases**
    - Example: Sales (CRM automation), Finance (approval workflows), HR (onboarding)
- **Governance policy updates**
    - Incorporate lessons from Phase 1
    - Publish Governance Playbook v2.0
    - Create department-specific guidance
- **Training cohort 2**
    - 30-50 additional users trained
    - Include "train the trainer" for department champions
- **CoE evolution**
    - Add business unit representatives to CoE meetings
    - Shift from weekly to bi-weekly meetings

Month 4: Stabilization & Optimization

- **Monitor automation adoption across 3 departments**
- **Conduct mid-point assessment**
    - Governance process efficiency
    - User satisfaction
    - Control effectiveness
- **Address emerging challenges**
    - Approval bottlenecks? Add approval delegates
    - Low adoption? Increase training/support
    - Too many restrictions? Refine risk tiers

Deliverables:

- 30-50 governed automations across 3 departments
- Governance Playbook v2.0
- Department champions identified
- Mid-point assessment report

Success Metrics:

- 90% of automations approved within 48 hours
- 70% user satisfaction with governance process
- All high-risk Zaps have documented approval

Phase 3: Scaled Rollout (Month 5)

Goal: Expand to majority of organization, stress-test governance

Month 5: Launch to 6 Departments

- **Select remaining medium/high-automation departments**
- **Mass training rollout**
    - 100-150 users trained
    - Self-service training resources available (videos, job aids)
- **Governance capacity expansion**
    - Approval workflow: Add approval delegates to reduce bottlenecks
    - CoE: Add office hours for real-time support
- **Communication campaign**
    - Leadership messages: "Governance enables safe innovation"
    - Success stories from pilot departments
    - FAQ addressing common concerns

Deliverables:

- 100+ governed automations across 6 departments
- Self-service training library
- Expanded approval delegate network

Success Metrics:

- 85% of automations approved within SLA
- 75% user satisfaction
- <5% policy violations

Phase 4: Enterprise-Wide Adoption (Month 6)

Goal: Full organizational rollout, governance as "business as usual"

Month 6: Company-Wide Launch

- **All employees with business need get Zapier access**
- **Final training push**
    - Remaining users trained
    - Refresher training for early adopters
- **Governance normalization**
    - Governance integrated into onboarding for new hires

    - Zapier governance part of annual compliance training
- **Celebrate early wins**
    - Showcase automation success stories
    - Recognize departments/individuals modeling best practices
- **180-day assessment**
    - Comprehensive governance review
    - Control effectiveness testing
    - User experience research (surveys, focus groups)
    - Process efficiency analysis

Deliverables:

- Enterprise-wide Zapier access with governance
- 180-day assessment report with recommendations
- Governance integrated into BAU processes

Success Metrics:

- 80%+ enterprise adoption rate
- <10% approval process escalations
- Zero critical governance incidents

Phase 5: Optimization & Maturity (Months 7-12)

Goal: Continuous improvement, advance governance maturity

Months 7-11: Continuous Improvement Cycle

- **Quarterly CoE reviews**
    - Policy updates based on lessons learned
    - Emerging risk identification
    - Automation landscape analysis
- **Advanced capabilities**
    - Automated compliance checking (if technically feasible)
    - Advanced analytics on automation patterns
    - Predictive risk modeling
- **Maturity advancement**
    - Assess current maturity level (likely Level 2-3)
    - Develop plan to reach Level 4 (Managed)

Month 12: Annual Assessment

- **Comprehensive annual governance audit**
    - Policy compliance
    - Control effectiveness
    - Cultural adoption

    - Risk landscape changes
- **Strategic planning**
    - Next year's governance priorities
    - Emerging AI capabilities to govern (new Zapier features)
    - Organizational changes requiring governance adaptation

Deliverables:

- 360-day assessment report
- Governance maturity scorecard
- Year 2 strategic plan

Success Metrics:

- Governance maturity Level 3 or higher achieved
- 85%+ employee satisfaction with governance
- Sustained zero critical incidents
- 95%+ automation compliance rate

Sample Communication Strategy Timeline

Phase	Primary Message	Channels	Frequency
Pre-Launch	"We're implementing governance to enable safe innovation"	Leadership emails, team meetings	Monthly
Pilot	"We're learning together - your feedback shapes our approach"	Pilot team meetings, CoE updates	Weekly
Expansion	"Governance is working - here's how it helps you"	Town halls, success stories	Bi-weekly
Enterprise	"Governance is how we work now - here's support"	All-hands, training, intranet	Weekly → Monthly
Optimization	"We're continuously improving - keep the feedback coming"	Quarterly reviews, surveys	Quarterly

References: Zapier Internal Documents and Policies

Documentation, Process, or Feature	URL	Date
Privacy Policy	https://zapier.com/privacy	23 Jan 2025
Data Protection Addendum	https://zapier.com/legal/website-terms-of-use	23 Jan 2025
Services Supplemental	https://zapier.com/privacy/services-supplemental-notice	23 Jan 2025
GDPR Supplemental Notice	https://zapier.com/privacy/gdpr-supplemental-notice	24 Jan 2025
US States Supplemental Notice	https://zapier.com/privacy/us-states-supplemental-notice	24 Jan 2025
Applicant Supplemental Notice	https://zapier.com/privacy/applicant-supplemental-notice	24 Jan 2025
Cookie Notice	https://zapier.com/privacy/cookie-notice	24 Jan 2025
Acceptable Use Policy	https://zapier.com/legal/acceptable-use-policy	25 Jan 2025
Terms of Service	https://zapier.com/legal/terms-of-service	25 Jan 2025
Enterprise Agreement	https://zapier.com/legal/enterprise-agreement	27 Jan 2025
Developer Platform Terms	https://zapier.com/developer-platform/tos	27 Jan 202
Website Terms of Use	https://zapier.com/legal/website-terms-of-use	
EU Standard Contractual Clauses	https://zapier.com/legal/standard-contractual-clauses	
Data Collection or Approval Request	https://help.zapier.com/hc/en-us/articles/38911356044941-Review-a-Zapier-data-collection-or-approval-request#h_01K2ZSG2TYPQDN59RV3RNRGAC5	
Data Privacy Framework Certification (Zapier's)	https://www.dataprivacyframework.gov/	

References: Articles, Journals, Studies

Title	Source	Date	URL
Zapier Hacked	Tech Startups	Mar 4, 2025	https://techstartups.com/2025/03/04/zapier-hacked-customer-data-accessed-in-security-breach/
Soft Snow Becomes Zapier Silver Solution Partner, Expanding AI Automation Services	Biz Journals	Jan 13, 2026	https://www.bizjournals.com/chicago/press-release/detail/12270/SoftSnow
Top 4 Zapier Security Risk	Infotech	Mar 16, 2021	https://www.infosecinstitute.com/resources/general-security/top-4-zapier-security-risks/
5 Risks of Automation and How to Mitigate Them	Glee Matic		https://gleematic.com/5-risks-of-automation-and-how-to-mitigate-them/
The Hidden Cost of Automation	eLearning Industry	Apr 1, 2025	https://elearningindustry.com/the-hidden-costs-of-automating-your-workflow-what-no-one-tells-you
Process Automation Transformation Risks		Nov 1, 2025	https://www.pwc.com/us/en/services/audit-assurance/library/process-automation-transformation-risks.html
6 Hidden Risk of IT Automation	CIO	Apr 2, 2024	https://www.cio.com/article/190962/6-hidden-risks-of-it-automation.html
Upguard's Security Reports -	Upguard Security Report	Feb 3, 2026	https://www.upguard.com/security-report/zapier
Zapier Partner with Newtonx to Reveal How Entereprises Measure AI ROI		Nov 3, 2025	https://www.newtonx.com/press/zapier-partners-with-newtonx-to-reveal-how-enterprises-measure-ai-roi/
Zapier AI Orchestration	Zapier	Jul 17, 2025	https://zapier.com/blog/ai-orchestration/