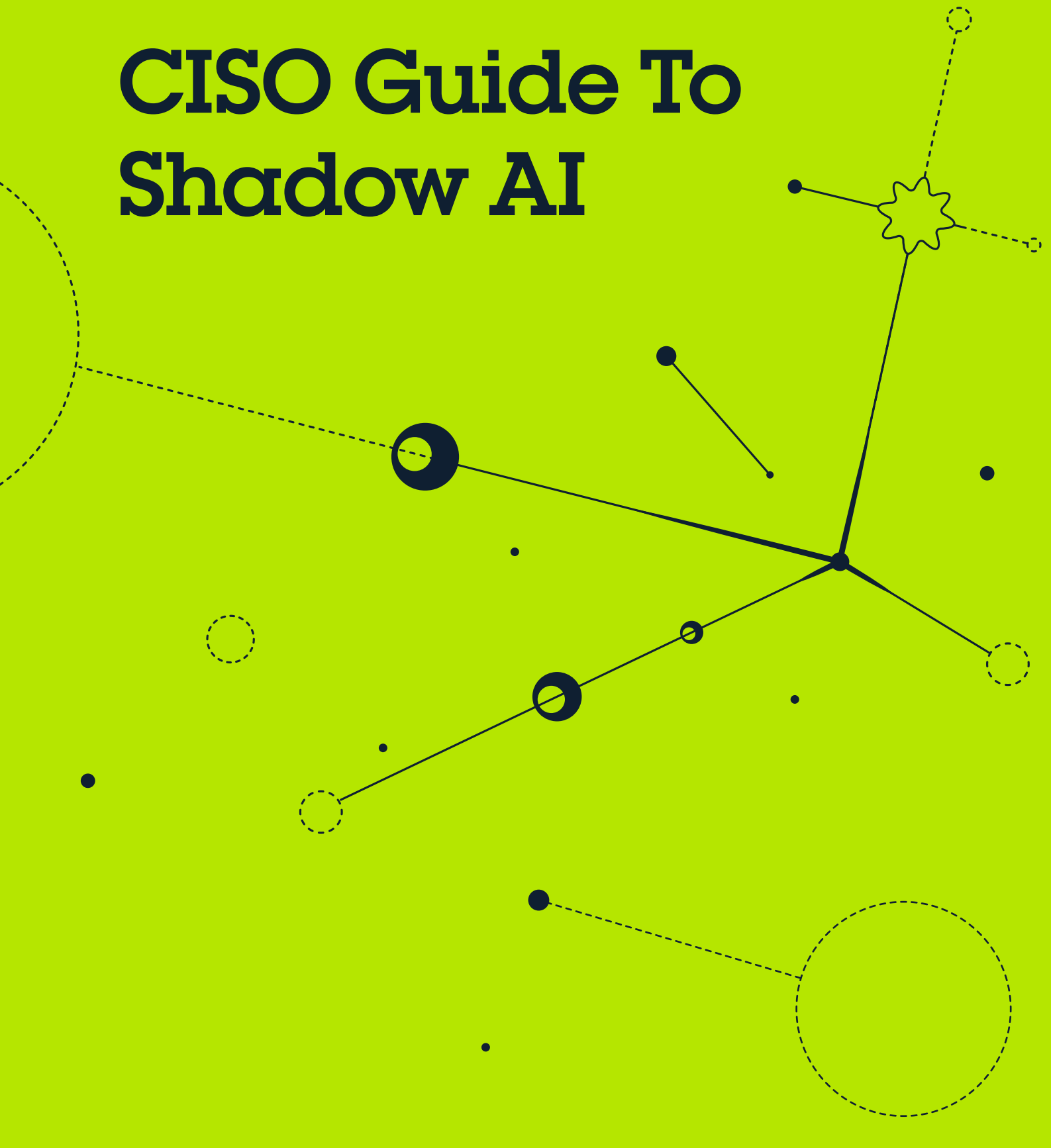
reco

CISO Guide To Shadow AI



Shadow AI represents a critical security challenge that extends beyond traditional shadow IT concerns. While shadow IT encompasses unauthorized technology usage, shadow AI represents a more dangerous subset - where well-meaning employees unknowingly expose enterprise data through AI systems that permanently retain and learn from every interaction.

Current Landscape

Recent data shows that while 45% of executives have adopted a "wait and watch" approach to AI adoption, 75% of employees are already actively using AI tools at work.[1] This disconnect between cautious leadership and productivity-seeking employees has led to significant security incidents, with one in five companies experiencing data leakage due to employees using generative AI.

Critical Risks

Organizations face several key challenges with shadow AI adoption:

1. Data Exposure

Recent studies show that 27% of corporate data input into AI tools is sensitive, nearly triple the amount from the previous year.[2] Once data is uploaded to AI systems, it becomes permanently accessible and cannot be recalled.

2. Unauthorized Access

Office workers are 77% more likely than remote workers to expose sensitive data through AI tools, with this risk increasing fivefold when logging in from offsite.[3] This risk intensifies when employees use personal accounts that lack enterprise security protections.

3. Compliance Violations

Organizations face potential regulatory violations, fines, and insurance claim denials when employees use unauthorized AI tools. The most significant concerns are cybersecurity (54%), privacy (53%), and liability (46%).[4]

1 "Robinson, Bryan. "Shadow AI: The Controversial 2024 Trend That Could Create Disaster, Experts Say." Forbes, August 2, 2024, https://www.forbes.com/sites/bryanrobinson/2024/08/02/shadow-ai-the-controversial-2024-trend-that-could-create-disaster-experts-say/
2 "Shadow AI: How Employees Are Leading the Charge in AI Adoption and Putting Company Data at Risk." Cyberhaven, May 21, 2024, https://www.cyberhaven.com/blog/shadow-ai-how-employees-are-leading-the-charge-in-ai-adoption-and-putting-company-data-at-risk
3 "Shadow AI on the Rise: Sensitive Data Input by Workers Up 156%." SC World, March 2024, https://ww.scworld.com/news/shadow-ai-on-the-risesensitive- data-input-by-workers-up-156
4 "Using Generative AI to Strengthen Cybersecurity." KPMG LLP, August 2023, https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/2023-GenAIcybersecurity.pdf

Implementation Strategy

Rather than implementing outright bans, which often drive usage underground, organizations must develop comprehensive security frameworks that balance protection with productivity. With 92% of organizations acknowledging moderate to high implementation risks, CISOs must focus on:

- Creating clear channels for requesting AI tool access
- Establishing role-based permission frameworks
- Implementing continuous monitoring of access patterns
- Maintaining detailed audit trails

The key to successful shadow AI management lies in acknowledging that employees typically adopt these tools with good intentions while implementing necessary controls to protect sensitive data.

Understanding AI Security Risks

It's everywhere now, like mushrooms after the rain: AI. For every tool or piece of software, there now seems to be an additional layer of "AI" on top, whether users – or their security and IT administrators – want it.

This explosive growth of AI tools has created a security crisis that transcends traditional shadow IT concerns. While shadow IT encompasses unauthorized technology usage, shadow AI represents a distinct and more dangerous subset where well-meaning employees unknowingly expose enterprise data through AI systems that permanently retain and learn from every interaction. Recent data shows that while 45% of executives have adopted a "wait and watch" approach to AI adoption, 75% of employees are already actively using AI tools at work, creating a critical disconnect between organizational readiness and employee innovation. This gap between cautious leadership and productivity-seeking employees has led to the rapid rise of shadow AI incidents, as workers inadvertently expose sensitive data through AI tools – many of which are now built into their established business tools – that can never truly "forget" what they learn.

Often these employees' – or organizations' – efforts to enhance productivity creates a perfect storm of risk that security and technology leaders must address through comprehensive security frameworks rather than outright prohibition as recent studies indicate that 15% of employees regularly post company data into AI tools, with over a quarter of that data being sensitive information.[5]

5 “Over a Third of Employees Secretly Sharing Work Info with AI." Infosecurity Magazine, February 2024, https://www.infosecurity-magazine.com/news/third-employees-sharing-work-info/

Current Landscape

The seemingly exponential growth of AI tools has created unprecedented visibility challenges for security teams. While many executives maintain a cautious "wait and watch" approach, employees are actively seeking productivity gains through easily accessible AI tools, often bypassing organizational security by using personal accounts that lack enterprise security controls. Recent studies show that 55% of data loss protection events now involve users sharing personally identifiable information with generative AI sites, highlighting even further how quickly this problem has grown in a short time.[6]

Risk Profile

1. Data Exposure

The most severe risk stems from permanent data exposure through model sharing and training. When employees input sensitive information into consumer AI tools, that data becomes irretrievable as it enters the AI makers' black box of training models. Recent studies show that 38% of employees share sensitive work information without permission, often simply trying to improve their productivity.[7]

2. Unauthorized Access

AI operators gain persistent access to corporate information through human review of customer prompts and training data. This risk intensifies when employees use personal accounts that lack enterprise security protections, creating a natural security degradation compared to corporate identity providers.

3. Compliance Violations

Organizations face potential regulatory violations, fines, and insurance claim denials when employees use unauthorized AI tools. The most significant concerns are cybersecurity (54%), privacy (53%), and liability (46%).

Business Impact

The accelerated adoption cycles of AI tools and their integrations into employees' business tools have compressed decision-making timeframes, challenging security teams' ability to implement appropriate controls. This acceleration has already led to significant incidents, with 92% of organizations acknowledging moderate to high implementation risks.

6 "Gen AI Risk: 55% of Company Data Loss Involves Personal Info." AI Magazine, February 2024, https://aimagazine.com/ai-applications/gen-airisk-55-of-company-data-loss-involves-personal-info

7 “38% of AI-Using Employees Admit to Sending Sensitive Work Data." SC World, April 2024, https://www.scworld.com/news/38-of-ai-using-employeesadmit-to-sending-sensitive-work-data

Detection and Visibility

The complexity of shadow AI creates unprecedented visibility challenges that extend beyond traditional shadow IT detection methods. While shadow IT tools can often be identified through network monitoring, shadow AI presents unique challenges due to its ability to embed itself within approved applications and operate through personal accounts.

Detection Challenges

The most critical detection challenges stem from AI's unique ability to mask its presence within legitimate business operations. Recent studies show that 55% of data loss protection events involve users sharing personally identifiable information with generative AI sites, often through seemingly normal business activities.

Application Integration

AI mechanisms frequently embed themselves within standard business critical applications, making traditional detection methods ineffective. These tools often appear as legitimate business applications, masking their AI capabilities and data access requirements behind standard functionality.

Data Transfer Patterns

Organizations face significant challenges in monitoring data movement between corporate and personal identities. The complexity increases when employees use personal accounts that naturally have less security than corporate identity providers, creating a security degradation that's difficult to detect.

Permanent Data Exposure

Once employees begin uploading data to AI systems, that information can never be fully recalled or erased. This permanence creates a unique challenge where detection must focus on prevention rather than remediation, as traditional data recovery methods prove ineffective.

Configuration Management

Shadow AI often manifests through subtle configuration changes and access patterns that may appear legitimate despite unauthorized AI usage. These changes can occur when vendors integrate new AI features into existing tools, making it difficult to distinguish between authorized and unauthorized AI usage.

Implementation Strategy

Organizations must implement multi-layered detection approaches that can identify both obvious and subtle forms of AI usage. This includes:

- Continuous monitoring of data transfer patterns
- Regular audits of application configurations
- Implementation of SSPM solutions for visibility
- Integration with existing security tools

The key to successful detection lies in maintaining continuous visibility while balancing security requirements with legitimate business needs for AI adoption. Organizations must acknowledge that employees typically adopt these tools with good intentions - seeking to improve efficiency rather than cause harm.

Continuous Monitoring Requirements

Organizations must implement multi-layered detection approaches that can identify both obvious and subtle forms of AI usage. Traditional network monitoring proves insufficient, as AI mechanisms often appear as standard application traffic. Recent studies show that one in five UK companies have experienced data leakage due to employees using generative AI, highlighting the critical need for enhanced visibility.

The most challenging aspect of shadow AI detection involves monitoring data movement between corporate and personal identities. Organizations must track:

Corporate Data Flow

When employees input sensitive information into consumer AI tools, that data becomes irretrievable. Recent studies show that 27% of corporate data employees put into AI tools was sensitive in early 2024, nearly triple the amount from the previous year.

Application Integration

AI mechanisms embedded within standard applications can mask their presence, making traditional detection methods ineffective. With 80% of companies using AI or in the process of incorporating AI, organizations must implement monitoring solutions that can identify AI capabilities within approved applications.

SSPM Implementation

My SaaS Security Posture Management (SSPM) has emerged as a critical component for maintaining visibility into shadow AI usage. SSPM provides:

- Continuous posture management across the SaaS environment
- Unified risk assessment and compliance monitoring
- Clear visibility into SaaS environment connections
- Real-time monitoring of user activities and data access patterns

The key to successful detection lies in maintaining continuous visibility while balancing security requirements with legitimate business needs for AI adoption. Organizations must acknowledge that employees typically adopt these tools with good intentions - seeking to improve efficiency rather than cause harm.

Identity and Access Management

Securing AI systems requires robust identity and access management controls that extend beyond traditional IAM frameworks. With over 80% of legal documents exposed through non-corporate AI accounts and half of all organizations experiencing source code exposure through unauthorized AI tools, organizations must implement comprehensive access controls that address both sanctioned and shadow AI usage.[8]

Access Control Architecture

Office workers are 77% more likely than remote workers to expose sensitive data through AI tools, with this risk increasing fivefold when logging in from offsite. Organizations must implement strict role-based permissions that consider both location and role-based risk factors while maintaining productivity.

Data Protection Requirements

Recent studies reveal concerning patterns in sensitive data exposure through AI tools:

- Legal documents represent the highest risk category, with over 80% exposed through non-corporate accounts
- Source code exposure affects half of all organizations using AI tools
- Research and development materials face significant exposure through personal accounts
- HR and employee records require particular protection due to privacy regulations

8 "Q2 2024 AI Adoption and Risk Report." Cyberhaven Labs, May 2024, https://info.cyberhaven.com/hubfs/Content%20PDF/Cyberhaven%20Q2%202024%20AI%20Adoption%20and%20Risk%20Report%20052024.pdf

Authentication Framework

Organizations must implement strong authentication mechanisms that can identify and control AI tool usage while maintaining productivity. Customer support, source code, and R&D material represent the top sensitive data types exposed through unauthorized AI usage, highlighting the need for contextual authentication controls.

Implementation Strategy

Rather than implementing outright bans, which often drive usage underground, organizations should develop a comprehensive IAM strategy that:

- Creates clear channels for requesting AI tool acces
- Establishes role-based permission frameworks
- Implements continuous monitoring of access patterns
- Maintains audit trails of AI tool usage

The key to successful IAM lies in balancing security requirements with legitimate business needs for AI adoption, acknowledging that employees typically adopt these tools with good intentions while implementing necessary controls to protect sensitive data.

Third-Party SaaS Security and AI

Modern organizations face unique security challenges as AI capabilities become embedded within SaaS applications. With 92% of organizations acknowledging moderate to high implementation risks, securing third-party AI tools requires a comprehensive approach that extends beyond traditional vendor assessment methods.[9]

Vendor Assessment

Organizations must thoroughly evaluate AI vendors' security practices across several critical domains. Recent studies show cybersecurity (54%), privacy (53%), and liability (46%) rank as the top risks when implementing AI solutions through third-party vendors.

Security Controls

Strong vendor security practices must include robust data encryption, role-based access controls, and regular security assessments. Organizations need clear visibility into data storage locations, retention policies, and privacy protection mechanisms, particularly given that 27% of corporate data input into AI tools is classified as sensitive.

9 "Using Generative AI to Strengthen Cybersecurity." KPMG LLP, August 2023, https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/2023-GenAIcybersecurity.pdf

Integration Security

Third-party AI tools often require extensive access to organizational systems, creating new attack surfaces and vulnerabilities. Organizations must implement strict API access controls and regular security assessments while maintaining continuous monitoring of data flows between systems.

Data Protection

Organizations must establish comprehensive data protection measures that address:

- Clear data storage locations and retention policies
- Transparent data access and sharing policies
- Strong privacy protection mechanisms
- Comprehensive compliance frameworks

Incident Response

Organizations must establish clear procedures for AI-related incidents involving third-party tools, including defined roles and responsibilities, clear communication channels, and documented response procedures. Regular testing ensures these procedures remain effective and current. The key to successful third-party AI security lies in maintaining continuous visibility while acknowledging that employees typically adopt these tools with good intentions - seeking to improve efficiency rather than cause harm.

Monitoring and Incident Response

Modern organizations require sophisticated monitoring and incident response protocols that extend beyond traditional security frameworks. With over 25% of sensitive corporate data being input into AI tools, organizations must implement comprehensive monitoring strategies that can identify and respond to AI-specific threats.

Continuous Monitoring Requirements

Organizations must implement multi-layered detection approaches that can identify both obvious and subtle forms of AI usage. Traditional network monitoring proves insufficient, as AI mechanisms often appear as standard application traffic. Recent studies show that one in five companies have experienced data leakage due to employees using generative AI, highlighting the critical need for enhanced visibility.

Data Transfer Patterns

The most challenging aspect of shadow AI detection involves monitoring data movement between corporate and personal identities. Office workers are 77% more likely than remote workers to expose sensitive data through AI tools, with this risk increasing fivefold when logging in from offsite.[10]

Risk Detection Mechanisms

Organizations must implement specific monitoring mechanisms for AI-related risks:

1. Data Exposure

The most severe risk stems from permanent data exposure through model sharing and training. When employees input sensitive information into consumer AI tools, that data becomes irretrievable - everything uploaded to the internet remains forever.

2. Unauthorized Access

AI operators gain persistent access to corporate information through human review of customer prompts and training data. This risk intensifies when employees use personal accounts that lack enterprise security protections.

3. Compliance Violations

Organizations face potential regulatory violations, fines, and insurance claim denials when employees use unauthorized AI tools. The most significant concerns are cybersecurity (54%), privacy (53%), and liability (46%).

Implementation Strategy

Rather than implementing outright bans, which often drive usage underground, organizations should develop a comprehensive monitoring strategy that:

- Creates clear incident response channels
- Establishes role-based monitoring frameworks
- Implements continuous visibility tools
- Maintains detailed audit trails

The key to successful monitoring lies in balancing security requirements with legitimate business needs for AI adoption, acknowledging that employees typically adopt these tools with good intentions while implementing necessary controls to protect sensitive data.

10 "Surge in Shadow AI Accounts Poses Fresh Risks to Corporate Data." TechNewsWorld, May 2024, https://www.technewsworld.com/story/surge-inshadow-ai-accounts-poses-fresh-risks-to-corporate-data-179299.html

Employee Education and Training

Modern organizations must develop comprehensive training programs that address the unique challenges of shadow AI usage. With 75% of employees already using AI tools despite only 45% of executives having formal strategies, education becomes a critical component of risk management.

Awareness Programs

Organizations must create targeted awareness programs that help employees understand the risks of unauthorized AI tool usage without stifling innovation. These programs should focus on the permanent nature of data exposure and the importance of using approved tools. Recent studies show that office workers are 77% more likely than remote workers to expose sensitive data through AI tools, highlighting the need for location-specific training approaches.

Security Culture

Rather than implementing outright bans, which often drive usage underground, organizations should foster a culture of responsible AI adoption. This includes:

- Creating clear channels for requesting new AI tool approval
- Establishing feedback mechanisms for tool suggestions
- Developing collaborative solutions between security and business units
- Maintaining open dialogue about AI usage and needs

Risk Communication

Organizations must effectively communicate the specific risks of shadow AI usage while acknowledging employees good intentions. Training should emphasize that over 80% of legal documents exposed through non-corporate AI accounts become permanently available, helping employees understand the lasting impact of their decisions. [11]

Implementation Strategy

The education program should enable rather than restrict, focusing on providing secure alternatives to shadow AI while maintaining necessary security controls. With customer support (16%), source code (13%), and R&D material (11%) being the top sensitive data types exposed, organizations must prioritize training for employees handling these critical data types.

11 Unauthorized AI is Eating Your Company Data Thanks to Your Employees." CSO Online, June 2024, https://www.csoonline.com/article/2138447/unauthorized-ai-is-eating-your-company-data-thanks-to-your-employees.html

Reco: Reducing AI Data Exposure At Scale

Reco is a leading SaaS Security Posture Management (SSPM) solution that helps organizations discover shadow AI, secure their AI implementations and mitigate the unique risks associated with AI-powered SaaS applications. By leveraging advanced AI and machine learning capabilities securely baked into the core of the product, Reco provides comprehensive visibility, continuous monitoring, and automated security checks across an organization's SaaS environment, including AI systems and integrations.

Key features of Reco's AI security solution include:

AI-powered SaaS discovery and monitoring: Reco can automatically discover and monitor AI-powered SaaS applications that are unauthorized within an organization's environment, providing real-time visibility into their configurations, user activities, and data access. Identify when AI apps are connected to other SaaS platforms (e.g. ChatGPT accessing SharePoint) and monitor data-sharing activities.

Copilot readiness: Automatically detect if a copilot (e.g. Microsoft AI assistant) is enabled within your tenant, and track data consumption and usage.

Anomaly detection and risk prioritization: Reco's AI algorithms establish baselines for normal behavior and can detect anomalies or deviations that may indicate potential security threats or misuse. These anomalies are then prioritized based on risk levels, enabling security teams to focus on the most critical issues first.

Automated security and compliance checks: Reco leverages AI and automation to continuously assess the security posture of AI-powered SaaS applications, identify potential compliance violations, and provide proactive recommendations for remediation.

Enforce controls: Connect to any SaaS AI apps to review their security settings via API, ensuring posture management for compliance. Align AI tool usage with security policies and industry regulations including MITRE, NIST CSF, and more.

Integration with existing security tools: Reco seamlessly integrates with an organization's existing security infrastructure, such as Security Information and Event Management (SIEM) and Governance, Risk, and Compliance (GRC) platforms, enabling a holistic and coordinated approach to AI security and risk management. Reco's AI security solution is built on a foundation of advanced AI and machine learning technologies, enabling it to effectively monitor and secure AI systems within an organization's SaaS environment. By leveraging AI to monitor AI, Reco can:

Understand and adapt to the complexities of AI systems: Reco's AI algorithms are designed to comprehend and adapt to the intricate decision-making processes and dynamic nature of AI systems, ensuring accurate monitoring and detection of potential threats or anomalies.

Continuously learn and improve: Reco's AI solution is designed to continuously learn and improve based on new data and security patterns, enabling it to stay ahead of emerging threats and adapt to evolving AI technologies and use cases and provide continuous compliance.

Provide intelligent and context-rich recommendations: Reco can provide intelligent context-rich recommendations for securing AI systems, optimizing configurations, and implementing best practices for AI governance and risk management.

By combining cutting-edge AI technologies with SSPM expertise, Reco empowers organizations to securely adopt and integrate AI into their operations, mitigating risks while unlocking the benefits of these powerful technologies.

CISO's Shadow AI Security Checklist

As CISOs navigate the complexities of AI adoption, it is essential to have a comprehensive checklist to ensure that security measures are effectively implemented and maintained. This checklist serves as a guiding framework for CISOs to address critical aspects of securing shadow AI:

Detection and Visibility

- [ ] Implement multi-layered detection approaches for AI usage
- [ ] Deploy SSPM solutions for continuous monitoring
- [ ] Establish data transfer pattern monitoring
- [ ] Configure alerts for unauthorized AI tool usage
- [ ] Set up audit trails for AI system activities

Access Controls

- [ ] Implement strict role-based permissions
- [ ] Configure location-based access restrictions
- [ ] Deploy strong authentication mechanisms
- [ ] Establish clear channels for AI tool requests
- [ ] Review third-party vendor access controls

Data Protection

- [ ] Identify sensitive data exposure points
- [ ] Implement data classification systems
- [ ] Configure encryption requirements for AI interactions
- [ ] Establish data retention policies
- [ ] Deploy data loss prevention controls

Ongoing Management

Policy Development

- [ ] Create formal AI governance framework
- [ ] Establish clear roles and responsibilities
- [ ] Define acceptable AI tool usage guidelines
- [ ] Develop incident response procedures
- [ ] Document compliance requirements

Employee Training

- [ ] Implement AI security awareness programs
- [ ] Create tool request procedures
- [ ] Establish feedback mechanisms
- [ ] Deploy role-specific training modules
- [ ] Document approved AI tool alternatives

Vendor Management

- [ ] Evaluate AI vendor security practices
- [ ] Review data handling procedures
- [ ] Assess compliance frameworks
- [ ] Monitor vendor configurations
- [ ] Establish incident response protocols

Regular Review

Monitoring Requirements

- [ ] Review detection mechanisms quarterly
- [ ] Update monitoring tools and procedures
- [ ] Assess effectiveness of controls
- [ ] Evaluate new AI security risks
- [ ] Update incident response procedures

Compliance Verification

- [ ] Verify regulatory compliance
- [ ] Review audit findings
- [ ] Update security controls
- [ ] Assess policy effectiveness
- [ ] Document improvements needed

About Reco

Reco is the leader in **Dynamic SaaS Security** – the only approach that eliminates the SaaS Security Gap. This gap is driven by SaaS Sprawl – the proliferation of apps, AI, and identities; the challenge of keeping their configurations secure amidst constant updates, and the challenge of finding threats hidden within an ever-growing number of events.

Dynamic SaaS Security by Reco keeps pace with this sprawl, no matter how fast it evolves, by covering the entire SaaS lifecycle – cradle to grave. It tracks all apps, SaaS-to-SaaS connections, Shadow SaaS, AI Agents, and Shadow AI tools, including their users and data, and adds support for new apps in days, not quarters. It maintains airtight posture and compliance – even as apps and AI Agents are added or updated. And it also ensures accounts remain secure, access privileges are minimized, and alerts are provided for critical threats.

Reco's AI-based graph technology connects in minutes and provides immediate value to security teams to continuously discover all SaaS applications including sanctioned and unsanctioned apps, shadow apps, associated identities from both humans and machines, their permission level, and actions.

Reco uses advanced analytics around persona, actions, interactions and relationships to other users, and then alerts on exposure from misconfigurations, over-permission users, compromised accounts, and risky user behavior.

This comprehensive picture is generated continuously using the Reco Knowledge Graph and empowers security teams to take swift action to effectively prioritize their most critical points of risk. Reco uses a low-code/no-code approach to add a new SaaS integration in 3-5 days.

Schedule a Demo