CAPABILITY VALUE BRIEF

# Secure Chat-based AI with Monitoring & DLP

## Protect Sensitive Data in AI Interactions with Comprehensive Oversight

## The Challenge

### The Problem

Organizations adopting AI tools like Microsoft like Microsoft Co-Pilot, Grok, Chat GPT, and Google Gemini face risks of sensitive data exposure, leading to compliance violations and security breaches. Without proper controls, AI interactions can inadvertently share confidential information, posing significant threats to data integrity and regulatory adherence.

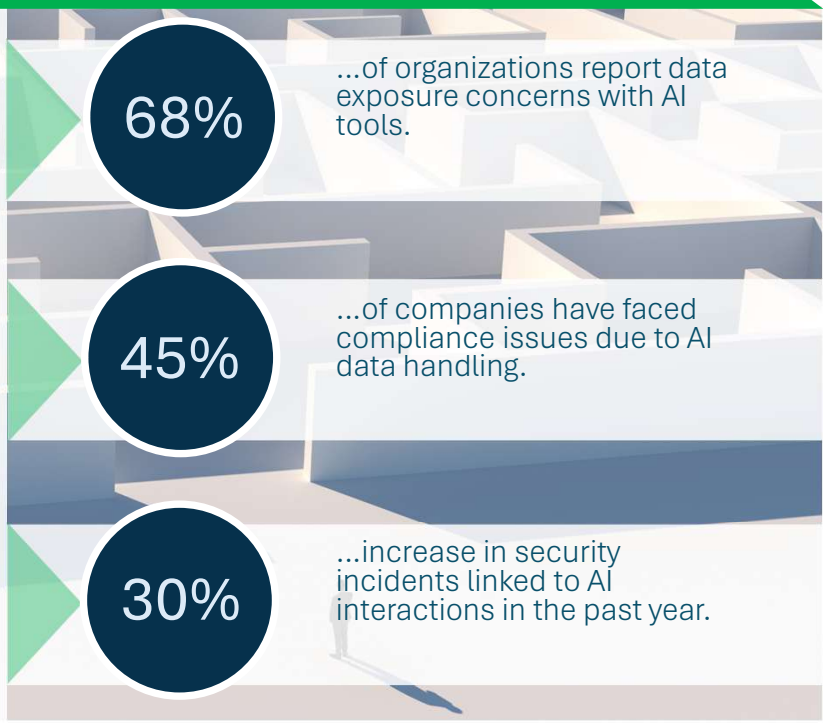
### The Impact

Unmonitored AI interactions can result in data breaches, regulatory fines, and operational disruptions.

**Data Exposure Risks:**
Sensitive information shared with AI can be accessed by unauthorized parties, leading to data leaks.

**Compliance Violations:**
Failure to protect data can result in hefty fines and damage to the organization's reputation.

**Operational Disruptions:**
Security breaches can halt business operations, causing financial losses and eroding stakeholder trust.




### The Solution

The iboss Chat-based GenAI Monitoring & DLP Capability provides a robust solution to secure AI interactions. By monitoring and recording conversations with Chat-based GenAI (and other AI) tools, organizations gain full visibility into AI usage. This capability blocks sensitive data from being uploaded or prompted to AI models, preventing potential data loss. Advanced features include incident creation for high-risk interactions and alerting administrators to take immediate action. Historical conversation logs enable forensic analysis and training, ensuring continuous improvement in AI usage policies.

With support for multiple AI tools and integration with external SIEM systems, iboss offers a comprehensive approach to AI security. This unified solution not only protects sensitive data but also ensures compliance with regulatory requirements, allowing organizations to leverage AI safely and effectively.

## Key Takeaways

**Enhanced Data Security**
Prevents sensitive data from being exposed during AI interactions, safeguarding organizational assets.

**Regulatory Compliance**
Ensures adherence to data protection regulations, reducing the risk of fines and reputational damage.

**Operational Continuity**
Minimizes disruptions by proactively managing security risks associated with AI usage.

## Fully Unified, Fully Distributed

**Unified Controls**
All AI monitoring and DLP features are managed through iboss's single, intuitive platform.

**Unified Protection**
Extends iboss' comprehensive security framework to cover AI interactions seamlessly.

**Unified Visibility**
Provides centralized logging and reporting for all AI-related activities across the organization.



sales@iboss.com 877-742-6832 iboss.com

CAPABILITY VALUE BRIEF

# Secure AI with Monitoring & DLP

## Protect Sensitive Data in AI Interactions with Comprehensive Oversight

## The Challenge

| Key Features | Key Benefits |
|---|---|
| **Full Conversation Recording**<br>Captures entire dialogues between users and AI tools for audit and analysis. | **Improved Accountability**<br>Enables tracking of AI usage patterns and identification of potential misuse. |
| **Sensitive Data Blocking**<br>Prevents prompts and file uploads containing sensitive information. | **Data Loss Prevention**<br>Stops confidential data from being shared with AI models, protecting privacy. |
| **Incident Management**<br>Automatically creates incidents for high-risk interactions and alerts administrators. | **Rapid Response**<br>Allows quick action to mitigate potential security threats from AI usage. |
| **Historical Analysis**<br>Allows review of past AI conversations for forensic investigations. | **Enhanced Forensics**<br>Provides detailed logs for understanding and improving AI interaction policies. |
| **Multi-Tool Support**<br>Extends monitoring and protection to other AI chat tools like ChatGPT. | **Comprehensive Coverage**<br>Ensures security across various AI platforms used within the organization. |
| **SIEM Integration**<br>Forwards log events to external SIEM systems for centralized security management. | **Streamlined Operations**<br>Integrates with existing security infrastructure for efficient monitoring. |

## Conclusions

### Secure AI Adoption
iboss enables organizations to embrace AI tools confidently by mitigating data exposure risks.

### Maintain Compliance
The capability ensures adherence to data protection regulations, avoiding costly penalties.

### Operational Efficiency
By preventing disruptions and streamlining security, iboss enhances overall business continuity.



## Additional Resources

iboss Chat-based GenAI Monitoring & DLP Solution Brief

Visit iboss.com/GenAI Risk Module for more information

**Request a Demo Today**

sales@iboss.com 877-742-6832 iboss.com