iboss®

CAPABILITY SOLUTION BRIEF

Chat-based Gen-AI Monitoring & DLP

Secure AI Interactions with Monitoring and Data Loss Prevention

Overview

The Problem

AI tools like Microsoft Co-Pilot, Grok, Chat GPT, and Google Gemini are transforming productivity, but they pose serious risks. Sensitive data in prompts or file uploads can leak to unauthorized parties, causing breaches and compliance failures.

Many organizations lack visibility into AI usage, leaving them unable to stop data loss. Existing security tools often miss AI interactions, creating a protection gap. This demands a solution to secure AI safely and meet regulations.

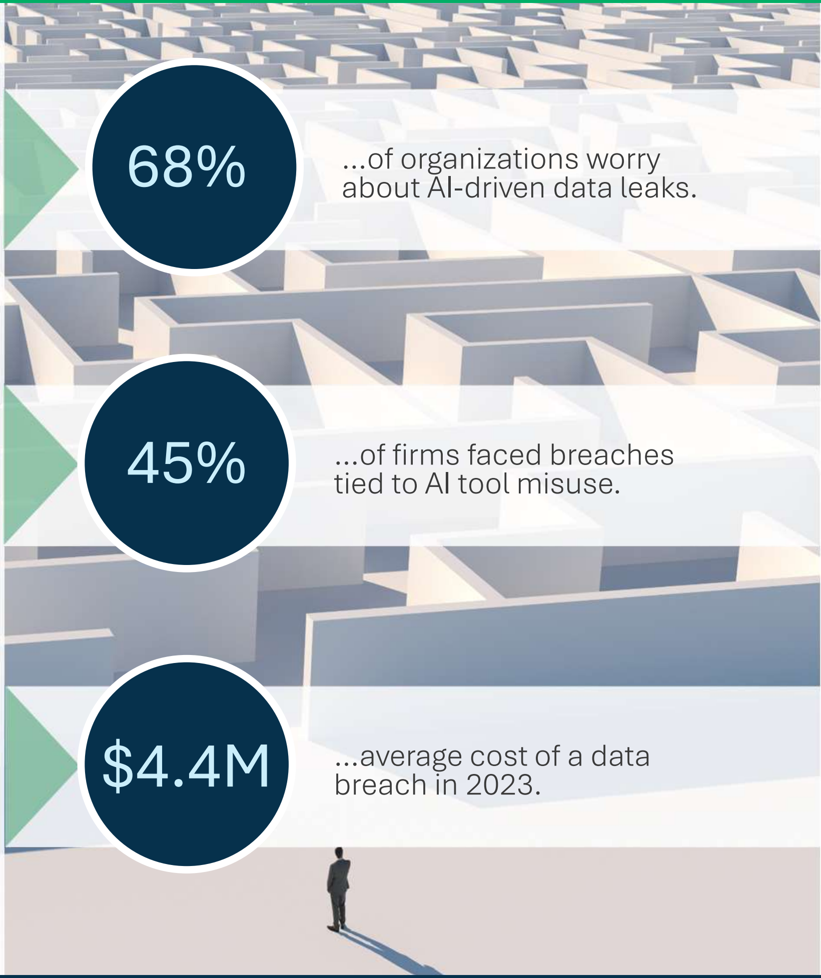
The Impact

Uncontrolled AI usage threatens organizations with data leaks and penalties.

Data Exposure:
Sensitive info shared with AI can reach unauthorized hands.

Compliance Risks:
Unprotected data may lead to fines and reputation loss.

Business Disruption:
Breaches from AI misuse can halt operations and trust.



68% ...of organizations worry about AI-driven data leaks.

45% ...of firms faced breaches tied to AI tool misuse.

$4.4M ...average cost of a data breach in 2023.

Solution Overview

Our AI Monitoring & DLP capability delivers total oversight of all Chat-based Gen-AI Toolset interactions, protecting sensitive data while supporting AI adoption. It records all AI conversations, giving clear visibility into usage patterns.

Features like blocking risky prompts and files, plus real-time alerts, stop data loss and ensure compliance. This lets organizations use AI's power securely, avoiding breaches or fines.

Integrated with our Zero Trust SASE platform, it unifies security across all tools and locations, simplifying management for IT and security teams.

Key Capabilities

Conversation Recording
Logs full AI chats for audits and insights.

Data Blocking
Stops sensitive prompts and uploads to AI models.

Incident Alerts
Flags high-risk actions with instant notifications.

	What We Solve	How We Solve It	Customer Benefits
Conversation Recording	No visibility into AI chats hampers risk detection efforts.	We record every Chat-based Gen-AI conversation fully, creating an audit trail.	Detailed logs offer proof of compliance and aid forensic reviews.
Data Blocking	Sensitive data sent to AI tools risks leaks and violations.	We block prompts and files with sensitive info before they hit AI systems.	Data stays secure, keeping compliance intact without slowing AI use.
Incident Alerts	Slow reaction to AI risks delays threat containment.	We auto-create incidents and alert admins when sensitive data is at risk.	Fast alerts cut response time, boosting proactive risk control.

Why Now?

AI use is surging - 75% of organizations aim to adopt it by 2025. Yet 60% lack controls to secure AI data, and regulations are tightening. Acting now prevents breaches and fines as AI grows critical.

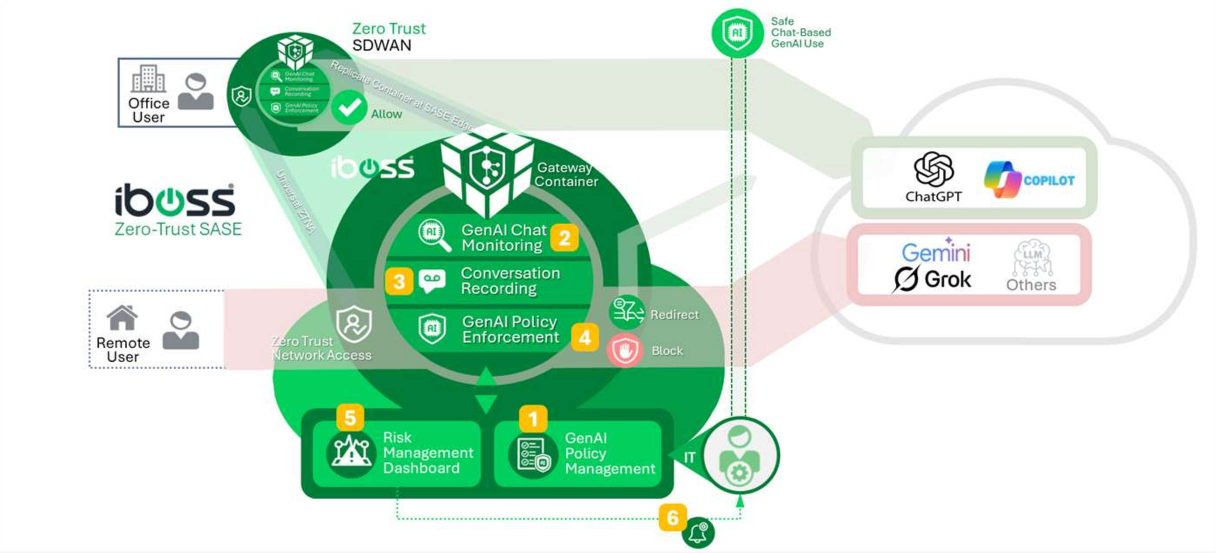
Additional Resources

iboss Chat-based GenAI Monitoring & DLP Value Brief

Visit iboss.com/platform/chat-based-gen-ai-protection for more information

Request a Demo Today

How It Works



1. **Set GenAI Policies**
   Define sensitive data types like PII or financial info.

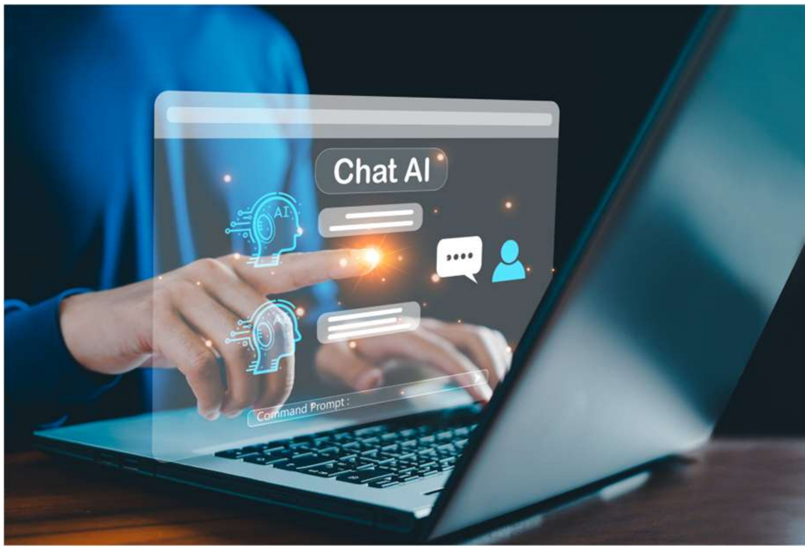
2. **Enable Monitoring**
   Turn on AI Monitoring & DLP in our platform.

3. **Capture Chats**
   Record all Chat-based GenAI interactions fully.

4. **Block Risks**
   Stop sensitive data from reaching AI models instantly.

5. **Flag Incidents**
   Create incidents for policy breaches automatically.

6. **Send Alerts**
   Notify admins of risks in real time for quick action.



Unified Controls

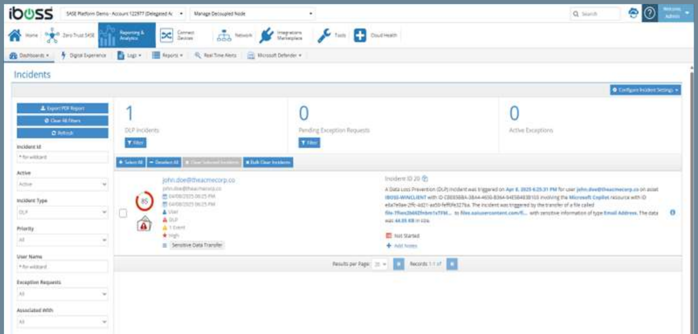
Adds AI oversight to our single policy framework.

Unified Protection

Extends Zero Trust to AI, locking down data access.

Unified Visibility

Shows AI activity in one view with all traffic.



Incidents

1 DLP Incidents

0 Pending Exception Requests

0 Active Exceptions

Incident Id: * for wildcard

Active: Active

Incident Type: DLP

Priority: All

User Name: * for wildcard

Exception Requests: All

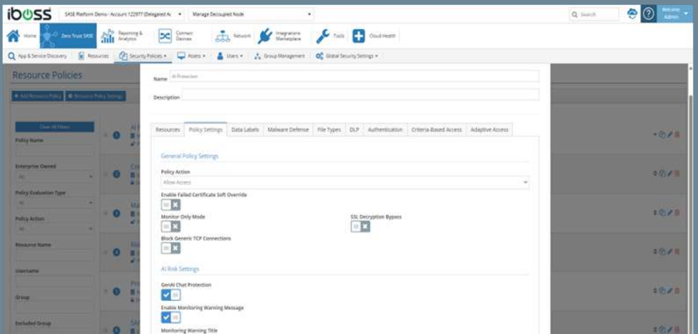
Associated With: All

john.doe@theacmecorp.co
john.doe@theacmecorp.co
04/08/2025 06:25 PM
04/08/2025 06:25 PM
85
User
DLP
1 Event
High
Sensitive Data Transfer

Incident ID 20

A Data Loss Prevention (DLP) incident was triggered on Apr 8, 2025 6:25:31 PM for user john.doe@theacmecorp.co on asset IBOSS-WINCLIENT with ID [illegible] involving the Microsoft Copilot resource with ID [illegible]. The incident was triggered by the transfer of a file called file-[illegible]... to files.oaiusercontent.com/fi... with sensitive information of type Email Address. The data was 44.05 KB in size.

Not Started



Resource Policies

Policy Name

Enterprise Owned: All

Policy Evaluation Type: All

Policy Action: All

Resource Name

Username

Group

Excluded Group

Name: AI Protection

Description

General Policy Settings

Policy Action: Allow Access

Enable Failed Certificate Soft Override: ☒

Monitor Only Mode: ☒

SSL Decryption Bypass: ☒

Block Generic TCP Connections: ☒

AI Risk Settings

GenAI Chat Protection: ☑

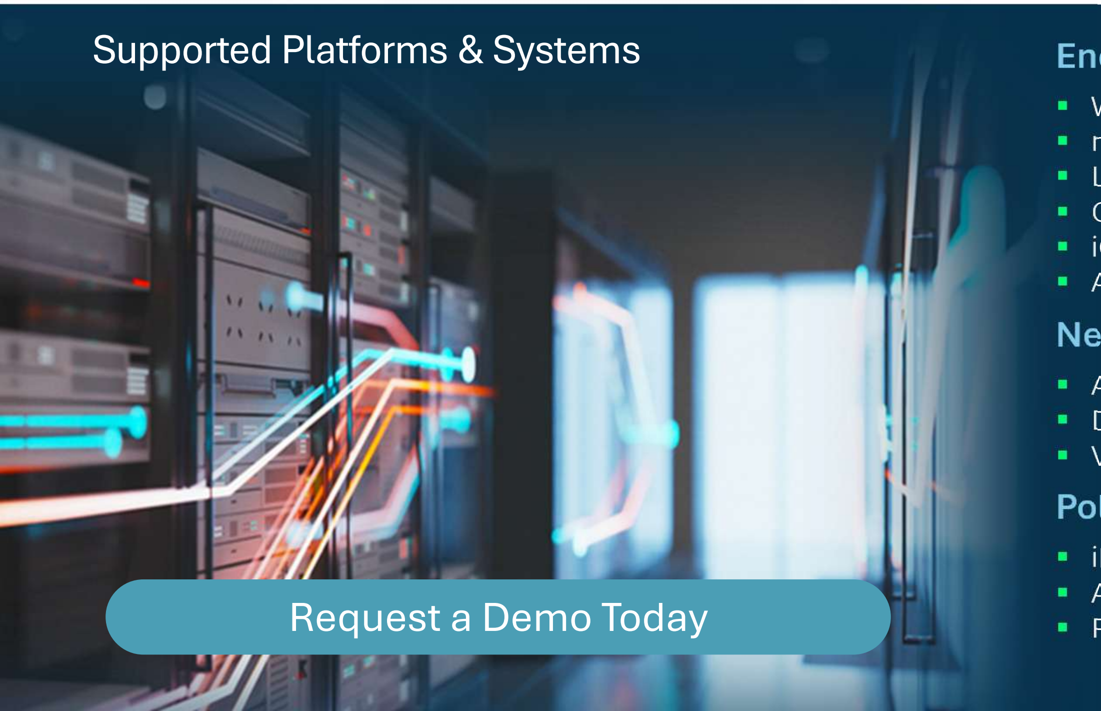
Enable Monitoring Warning Message: ☑

Monitoring Warning Title

Feature Details

Feature	Description
Chat Recording	Logs all AI talks for audit and review.
Data Blocking	Halts sensitive info from AI exposure.
Incident Creation	Auto-flags risky AI actions.
Real-Time Alerts	Warns admins of threats instantly.
Past Chat Review	Shows prior AI talks for compliance.
Multi-AI Support	Covers all Chat-based Gen-AI.
SIEM Sync	Sends logs to external SIEM systems.
Custom Policies	Sets rules for sensitive data types.
User Tracking	Monitors who uses AI and how.
Compliance Reports	Builds audit-ready data reports.

Supported Platforms & Systems



Request a Demo Today

Endpoint Cloud Connector

- Windows
- macOS
- Linux
- ChromeOS
- iOS
- Android

Network Connector

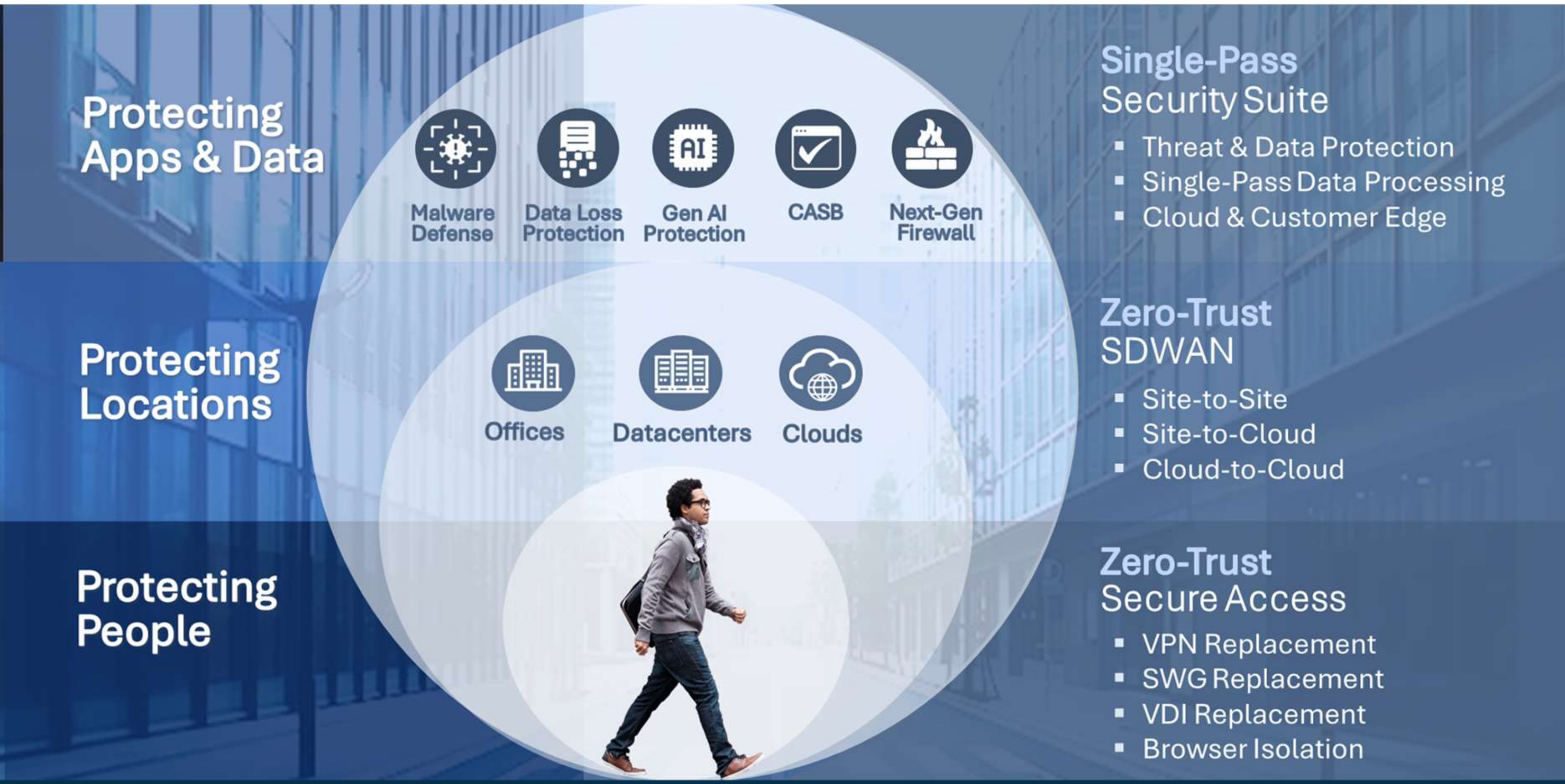
- AWS
- Docker
- VMware OVF

Policy Enforcement Points

- iboss Global Cloud (100+ POPs)
- Azure
- Private Locations

Feature Details

iboss is a Zero Trust SASE platform that secures all connections through a single, cloud-based service. It replaces multiple point products such as VPN, Secure Web Gateway, SD-WAN, firewall, CASB, and Browser Isolation with one unified solution. This helps organizations control access, contain threats, and protect data across any network. By using identity-based ZTNA for private access, iboss reduces risks associated with legacy VPNs. Its cloud-delivered SWG inspects traffic, including HTTPS, and enforces advanced malware defenses and data loss prevention. Inline and out-of-band CASB features guard SaaS applications, while SD-WAN capabilities simplify office connectivity and reduce bandwidth costs. Through a single console, iboss lowers costs, unifies policies, and delivers consistent protection for all users, devices, and locations.



Protecting Apps & Data

Malware Defense · Data Loss Protection · Gen AI Protection · CASB · Next-Gen Firewall

Single-Pass Security Suite

- Threat & Data Protection
- Single-Pass Data Processing
- Cloud & Customer Edge

Protecting Locations

Offices · Datacenters · Clouds

Zero-Trust SDWAN

- Site-to-Site
- Site-to-Cloud
- Cloud-to-Cloud

Protecting People

Zero-Trust Secure Access

- VPN Replacement
- SWG Replacement
- VDI Replacement
- Browser Isolation

Fully, Unified, Full Distributed

Unified Controls

Implement a single policy framework across every location and user, eliminating the complexity of managing separate solutions.

Unified Protection

Apply consistent security controls for web, cloud, and private apps, reducing exposure and preventing threats everywhere.

Unified Visibility

Leverage a single console for real-time logging and reporting, enabling faster investigations and stronger oversight across the organization.

Contact Us:

✉ sales@iboss.com ☎ 877-742-6832 www iboss.com

Request a Demo Today