FEATURE BENEFIT SHEET

Security Insights & Incident Management

Gain Real-Time Visibility, Control, and Rapid Response Capabilities to Effectively Manage and Mitigate Security Incidents

The Challenge

Organizations face an overwhelming volume of security threats, from data breaches and phishing attempts to malware infections and insider risks. Security teams struggle with incident visibility due to siloed tools, fragmented logs, and manual correlation efforts, leading to delayed response times and higher exposure to attacks.

Additionally, security teams are inundated with a constant stream of alerts from various security tools, many of which lack context or prioritization. A Gartner study found that only 4% of alerts are investigated due to resource constraints and high alert volumes. This alert fatigue makes it difficult to differentiate between critical threats and false positives, increasing the risk of missed incidents and data breaches. Without a unified incident management system, organizations remain vulnerable to evolving security threats.

The Solution

iboss' **Security Insights & Incident Management** provides a centralized, workflow-driven solution for security teams to monitor, investigate, and remediate threats in real time. By aggregating incidents across the network, including DLP violations, malware infections, phishing attempts, and, optionally, AI risks, it eliminates the need for security teams to manually correlate disparate logs. Built-in incident lifecycle management tracks every event from detection to resolution, reducing response times.

With real-time alerts, detailed event timelines, and administrator assignments, Security Insights & Incident Management accelerates response efforts, helping teams prioritize and mitigate the most critical threats efficiently. Organizations can proactively protect data, reduce dwell time, and strengthen compliance, all while minimizing workload and improving overall threat management capabilities.

204

It takes organizations an average of **204** days to identify a data breach and 73 days to contain it

88%

Approximately **88%** of all data breaches are caused by an employee mistake

264%

Ransomware attacks have increased by **264%** over the last five years

Why iboss?

Centralized Insight & Incident Management

Gain full visibility and control over security incidents with a centralized solution that streamlines detection, investigation, and response.

Real-Time Threat Detection

Instantly identify and mitigate security threats with automated alerts, incident timelines, and seamless administrator assignments.

Seamless Workflow Integration

Assign incidents, track statuses, and collaborate across teams with intuitive workflows that accelerate threat resolution.

Fully Unified + Fully Distributed

Unified Controls:
Ensure consistent incident detection, response, and enforcement by applying centralized security policies across all users, devices, and locations.

Unified Protection:
Correlate security events generated from any user or device, categorizing incidents by risk level, and automate remediation to minimize threat impact.

Unified Visibility:
Deliver notifications with detailed context to administrators, ensuring quick response and proactive risk mitigation.

FEATURE BENEFIT SHEET

Security Insights & Incident Management

Gain Real-Time Visibility, Control, and Rapid Response Capabilities to Effectively Manage and Mitigate Security Incidents

Feature Capability	Feature Benefit
Centralized Insights & Incident View Provides a unified solution that aggregates all security incidents, eliminating the need to sift through multiple tools and logs.	**Comprehensive Visibility** Gain a single-pane-of-glass view of all security incidents across your organization to simplify threat detection.
Real-Time Alerts Instantly notify security teams when an incident is detected, ensuring threats are addressed before they escalate.	**Rapid Threat Response** Receive notifications when an incident occurs, reducing the time to respond and mitigate risks.
Detailed Incident Timelines Track the full sequence of events leading to an incident, providing deeper forensic insight into security threats.	**Enhanced Incident Analysis** Understand the root cause and progression of security events to improve investigation and remediation.
Incident Assignment & Management Allow security teams to assign incidents to the right personnel, track progress, and ensure accountability.	**Efficient Incident Resolution** Enable teams to organize, prioritize, and manage incidents effectively, ensuring faster response and threat mitigation.
DLP & Phishing Incident Monitoring Detect and flag sensitive data leaks and phishing interactions, helping organizations proactively mitigate risks.	**Proactive Data Protection** Prevent data exfiltration and reduce phishing-related threats by identifying risky behaviors in real time.
Infected Device Detection Identify and alert security teams when devices communicate with known malware command-and-control (CnC) servers.	**Early Threat Containment** Detect potentially compromised devices early to prevent lateral movement and further infection.
Customizable Incident Rules Allow administrators to configure incident triggers based on allowed, blocked, or always-on criteria for tailored threat detection.	**Adaptive Security Controls** Fine-tune incident creation settings to align with your organization's risk tolerance and compliance needs.
PDF Export & Reporting Enable security teams to generate incident reports for compliance, audits, and executive summaries.	**Simplified Compliance & Audits** Easily document security incidents and responses for regulatory adherence and organizational transparency.

Conclusions

- **Traditional security tools lack full incident visibility**
  Relying on siloed security solutions leaves gaps in incident detection, making it harder to identify and mitigate threats effectively.
- **Consistent incident response requires a unified platform**
  A centralized solution ensures security teams can monitor, investigate, and resolve incidents across all users and devices with a consistent workflow.
- **Faster threat response reduces risk exposure**
  Real-time alerts, automated workflows, and intuitive incident management help security teams minimize dwell time and prevent potential breaches.

More Information

Contact Us

The iboss Zero Trust SASE platform delivers comprehensive security and compliance from a single, centralized console. With built-in encryption, seamless policy enforcement, and full visibility across your Users & Applications real-estate, the platform simplifies management while protecting sensitive data across all devices and locations.

Request a Demo Today