CYBER ZONES INSIGHT

by Cyber Zones

Insider Threat Detection & Behavioral Visibility Platform

Absolute Sovereignty Over Behavioral Intelligence

Insight is an on-premise insider threat detection platform developed by the Innovation & Research Division. It provides high-confidence visibility to detect insider risks through evidence-based monitoring.

1

Zero Cloud Dependency

Operates entirely within your internal environment.

2

Zero External Transmission

Complete network isolation with zero outbound data requirements.

3

Full Data Control

Uncompromised ownership of storage and access.

The Guarantee: Maximum privacy. Full data ownership. Secure internal operation.

Centralized Architecture for Controlled Scalability

The Endpoint Lens

Insight Agent

- Installed directly on monitored endpoints.
- Collects system activity and behavioral data with an ultra-lightweight footprint.
- Communicates securely back to the centralized hub.

Server-Agent

The Core Brain

Insight Server

- Central monitoring console
- Data aggregation and storage
- Risk scoring and alerting engine
- Reporting and visualization

Rapid Deployment Model

From installation to high-confidence visibility with zero external dependencies.

Step 1: Install Server

Fully on-premise deployment within the internal network.

Step 2: Deploy Agents

Lightweight deployment across endpoints with immediate device registration.

Step 3: Start Monitoring

Immediate visibility into user and system activity.

Beyond monitoring. Insight is an evidence-driven insider threat detection platform engineered to identify suspicious behavior and early indicators of compromise instantly.

Comprehensive Behavioral Visibility

Live Monitoring

Real-time visibility of active user sessions.

App & Window Tracking

Deep tracking of active processes and application window focus.

Network Activity

Upload/download tracking and precise bandwidth usage patterns.

Web Activity

Domain-level browsing visibility.

File Operations

Triggers on file copy, move, delete, and access patterns.

Threat Detection & Multi-Signal Correlation

Detection Logic Filters

RAW DATA STREAM 1

RAW DATA STREAM 2

RAW DATA STREAM 3

Filter 1: Insider Threat Indicators

- Abnormal file access & data staging
- Execution of offensive tools (credential dumpers, remote access)

Filter 2: Behavioral Pattern Analysis

- After-hours system usage & sudden spikes in activity
- Excessive distinct domain access

Filter 3: Compromise Indicators

- Suspicious process execution & unusual system patterns

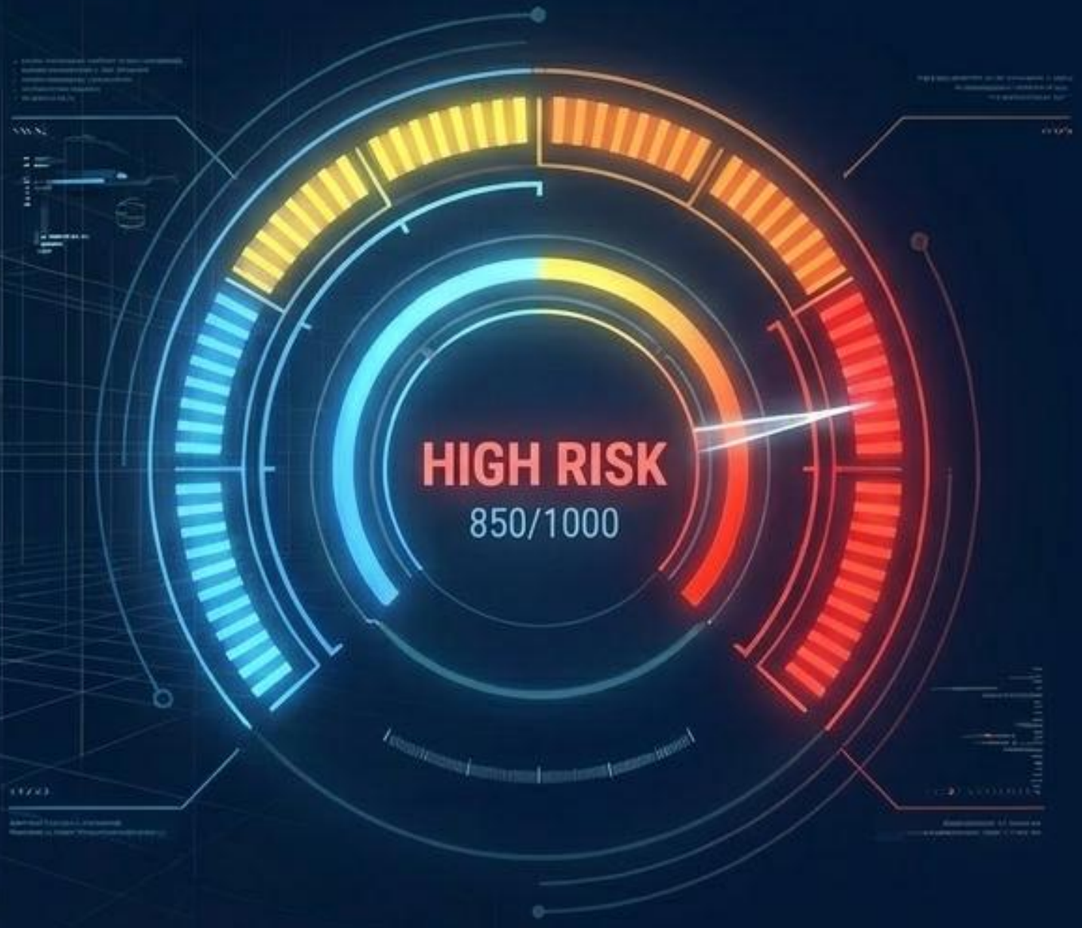
The Output Layer - Multi-Signal Correlation

Detects repeated suspicious behaviors and compound threats (e.g., after-hours activity + file access + data transfer) within short time windows.

Behavioral Risk Scoring Engine

Applying dynamic prioritization to high-risk endpoints and behaviors.

CYBER ZONES INSIGHT
by Cyber Zones



The Scoring Model (Inputs):

- Alert severity and type weighting.
- Frequency of suspicious activity.
- Time-based decay (recent activity carries higher impact).
- Behavioral intensity and after-hours usage.

The Operational Value (Outputs):

- Immediate identification of high-risk devices.
- Data-backed prioritization of investigation efforts.
- Early detection of insider threats before critical exfiltration.

Strategic Alignment with Global Frameworks

MITRE ATT&CK Classification

Automatic Event Enrichment:

Formally classifies execution, network visibility, repeated behavioral patterns, and data exfiltration.

Outcome: Standardized classification and improved investigation workflows.

CIS Critical Security Controls

Measurable Coverage Maps to:

- **CIS 1:** Asset Inventory (unmanaged device discovery)
- **CIS 5:** Account Management (session tracking)
- **CIS 8:** Audit Logging (centralized logs)
- **CIS 13:** Network Monitoring (behavior visibility)

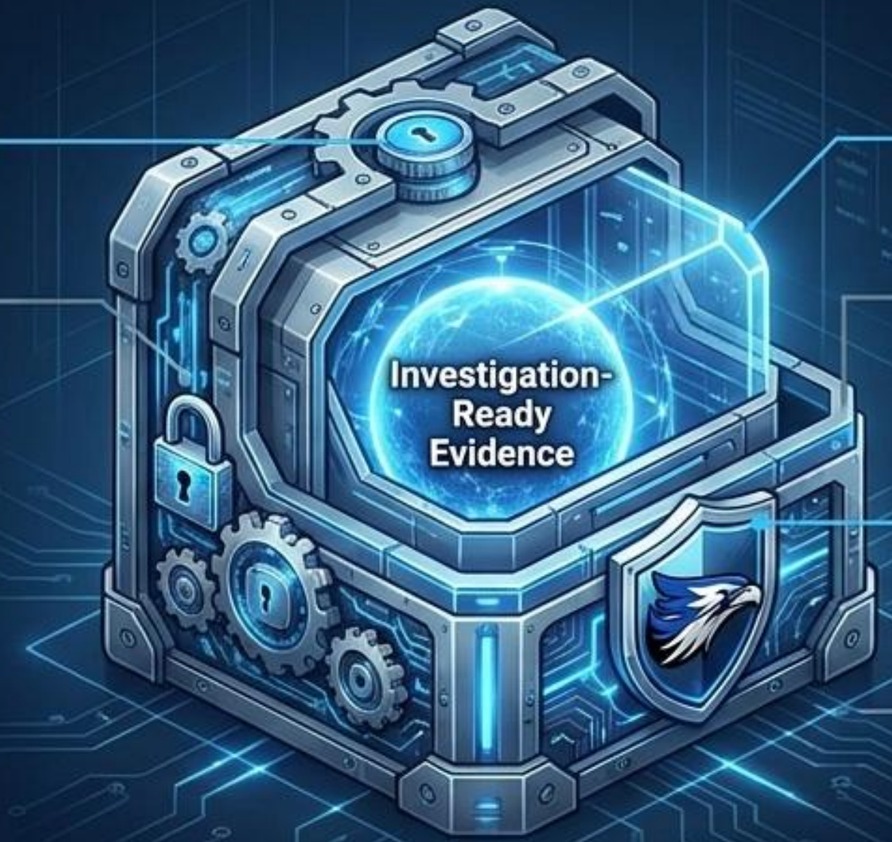
Outcome: Governance visibility and compliance support.

The Gold Standard: Evidence Integrity

Core Principle: Insight relies on verifiable evidence, not inferred assumptions.

Layer 1: Non-Repudiation

Cryptographically signed event logs guarantee data origin and prevent modification.



Layer 2: Tamper-Evident Storage

Read-only enforcement of collected events protects against deletion or alteration.

Layer 3: Visual Proof

Context-rich visual verification ensures collected evidence can be validated flawlessly during investigations.

Business Outcome: Completely supports HR disciplinary processes, internal investigations, and legal/compliance reviews.

Professional, Verifiable Reporting

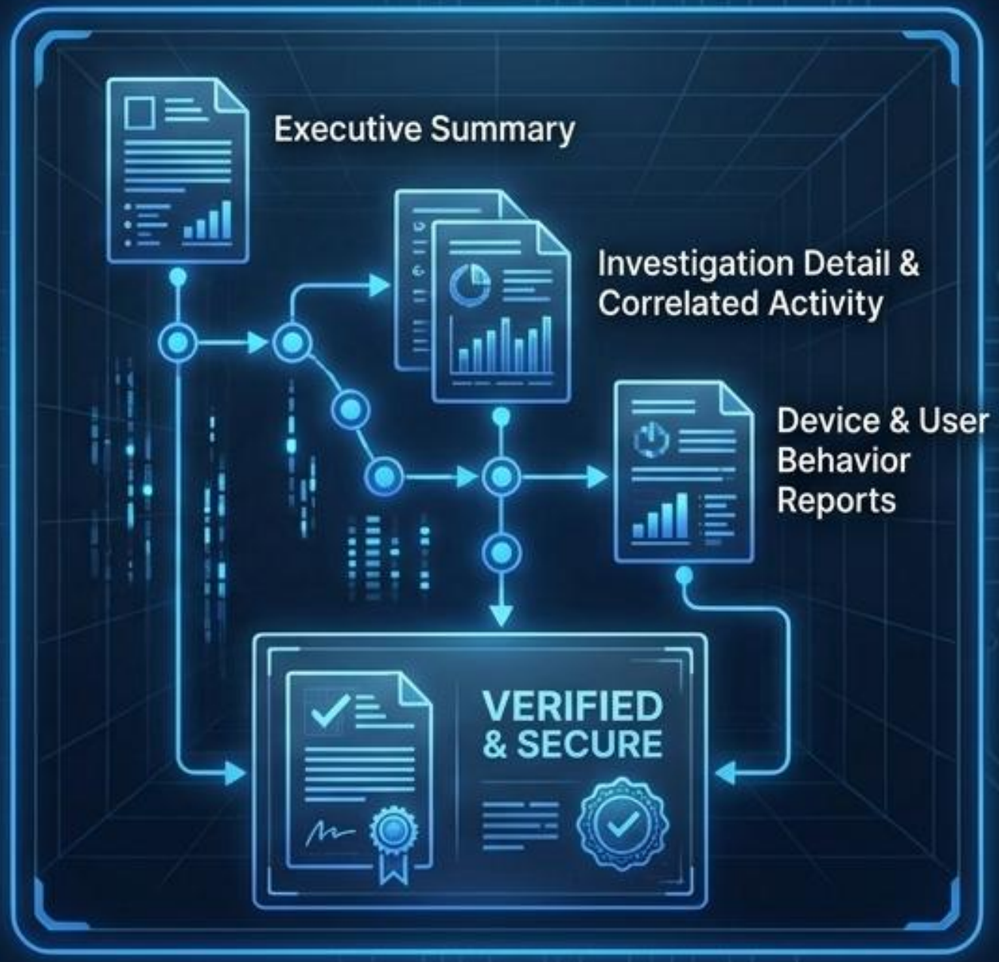
Structured outputs designed for operational, investigative, and executive use.

Core Features

- HTML-based activity reports with verifiable timelines.
- Correlated activity mapping.
- Device-level behavior tracking.
- Export-ready investigation summaries.

Designed For

- C-Level and Management
- Security and Incident Response Teams
- Human Resources and Legal Departments



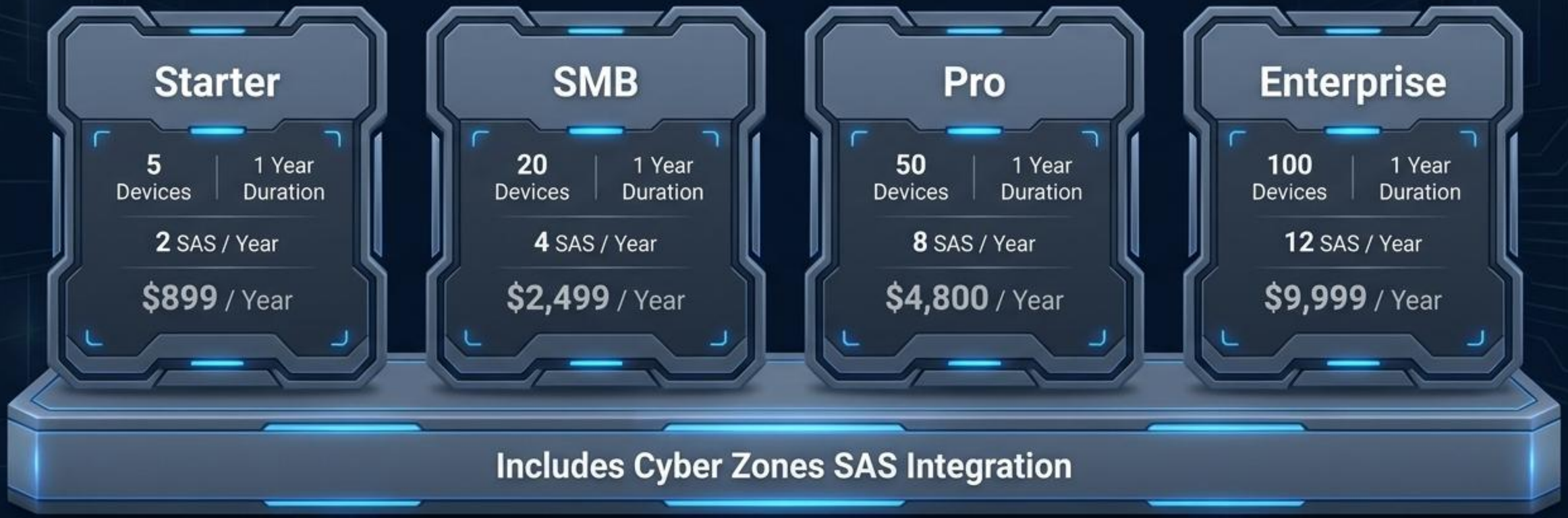
The Insight Differentiation

Capability	Traditional Tools	Insight
Monitoring	Basic tracking	Behavioral visibility
Detection	Limited	Insider threat detection
Evidence	Weak / non-structured	Investigation-ready
Deployment	Cloud / complex	On-premise, simple
Analysis	Manual	Structured + mapped
Reporting	Basic logs	Professional reports

Moving organizations from passive monitoring to actionable, evidence-driven threat identification.

Deployment Tiers & Pricing Architecture

Scalable, transparent pricing for any organizational footprint.



Engineered to solve: Suspicious employee behavior, compromised endpoint identification, internal incident response, and compliance support.

CYBER ZONES