

DATA SHEET

Trellix Wise™ for Private Cloud

The core of your agentic SOC

Highlights

True agentic support:

Investigate, remediate, and proactively hunt for threats in minutes by reducing thousands of raw alerts into a manageable set of high-confidence verdicts

Tailored results:

Calibrates based on security, organization, and procedural context to deliver tailored, threat investigations that reduce false positives and align incident responses with business risk.

Absolute sovereignty:

Deploys and runs entirely within your infrastructure, fully supporting air-gapped networks so sensitive data never leaves your perimeter and you can maintain 100% local agentic reasoning and operations.

Predictable costs, unmetered defense tailed incident analysis:

Provided as a single flat-fee subscription with zero metering, usage caps, or surprise overages as alert volumes grow.

Today's attackers use AI to move at machine speed and resource constrained SOC's are struggling to keep pace. To keep up, organizations are quickly evolving their SOC's into an agentic SOC, but until now, that has meant sending your most sensitive security data to a cloud you don't ultimately control and paying unpredictable, usage-based fees as AI adoption grows.

Trellix Wise for Private Cloud solves this by delivering the essential pieces of an agentic SOC program that can operate 100% inside your own environment under a predictable, flat-fee subscription allowing you to detect and respond to AI-driven attacks without giving up control of your data or budget.

Three needs, one offering

An agentic SOC program must satisfy three non-negotiable requirements at once: an ability to successfully stop an AI-fueled attack, understanding and control over where and how the AI uses your data and how it formed its response, and a means to predictably plan for its operational costs. Trellix Wise for Private Cloud delivers all three in a single offering. It investigates every alert, hunts continuously, and stages governed responses entirely within your boundary, under a flat-fee subscription with no metering.

1. Execution and efficacy at AI speed

- Automated alert triage and investigation: Automatically examines alerts the moment they arrive, linking low-level events and threat intelligence to catch complex attacks that traditional tools miss, freeing analysts to focus on high-impact strategic initiatives.

- Multi-agent investigative execution: Breaks each investigation across specialized agents that gather corroborating evidence, decode hidden artifacts, and pivot across indicators to reach a high-fidelity verdict—applying the same rigorous workflow to every alert helping scale your SOC team.
- Battle tested investigative and hunting frameworks: Investigations and hunts follow two codified methodologies — TRACE (Triage, Range, Analyze, Counteract, Enhance) and CHASE (Conceptualize, Hunt, Assess, Signal, Enhance). Each enforces an evidence-backed exit at every phase and loops back when context is missing, hardening reasoning against the bias and hallucination that derail generic AI

2. Absolute sovereignty and auditable trust

- Transparent white-box reasoning: Provides full visibility into observed data, reasoning chains, and calibrated confidence scores so analysts retain full operational authority.
- Zero external data exposure: In air-gapped operations, ensures all processing, reasoning, and context retention remain fully contained inside your infrastructure.
- Auditable evidence: Delivers clear, fact-based verdicts backed by complete agent audit trails, allowing teams to QA decisions, build trust in AI reasoning, and phase in automation as confidence improves.

3. Unmetered AI defense and predictable costs

- Scale without budget creep: Expand your SOC output without the linear expenses of extra headcount or the unpredictability of consumption-based token fees.
- Flexible capacity control: You dictate performance by choosing the underlying hardware capacity,
- Access your data where it resides: Trellix Wise for Private Cloud weaves into your existing systems without the need for data shifts or additional data storage.

How does Trellix Wise for Private Cloud work?

Trellix Wise for Private Cloud operates as a decentralized reasoning layer over your existing security stack rather than a centralized data store. On alert ingestion, it issues federated queries against your SIEMs, data lakes, and security tools, then structures the returned telemetry into localized entity-relationship knowledge graphs, eliminating duplicate indexing or migration into a separate repository. Three specialized agents—Investigation, Remediation, and Hunting—execute deterministic workflows mapped to T1–T3 analyst functions, producing structured, evidence-backed case output. All model inference, knowledge graphs, retained context, and reasoning stages run on customer-controlled hardware inside the security perimeter, up to fully air-gapped deployment. The mechanics below detail how data is read, reasoned over, scored, and acted upon.

Reads data where it lives

On alert ingestion, the system issues federated queries against existing SIEMs, data lakes, and security tools, then normalizes the returned telemetry into entity-relationship knowledge graphs. Correlation executes over this graph structure, eliminating duplicate indexing or data migration into a separate store.

Role-aligned agent architecture

Three specialized agents—Investigation, Remediation, and Hunting—map to T1–T3 analyst functions. Each executes a deterministic workflow (enrichment, correlation, hypothesis generation, verdict) across all inbound alerts continuously, producing structured case output rather than an opaque classification.

Runs entirely on your hardware with local operation

Model inference, knowledge graphs, retained context, and every reasoning stage execute on customer-controlled hardware inside the security perimeter, up to fully air-gapped deployment. No environment, investigation, or identity data traverses the boundary, and capability is unchanged in disconnected operation.

Evidence-weighted confidence scoring

Each verdict carries a calibrated confidence score derived from the specific evidence set, with MITRE ATT&CK mapping and a reconstructed event timeline. Insufficient or absent telemetry is reflected as reduced confidence and flagged explicitly rather than inferred.

Gated, promotable response controls

Remediation connectors operate read-only by default and require explicit promotion to active enforcement. RBAC governs agent and operator scope; high-impact actions enforce human-in-the-loop approval. All agent decisions and tool invocations are written to an immutable audit log.

The agents

What sets an agentic SOC apart from traditional approaches is the use of agentic AI to support SOC analysts throughout their workday. Trellix Wise for Private Cloud deploys three specialized agents—Investigation, Remediation, and Hunting—all included in a customer's license fee.

Investigation

Designed as an always-on first responder, the Trellix Wise for Private Cloud Investigation Agent automatically evaluates, correlates, and triages every incoming alert in minutes rather than hours or days. It learns your organization's unique operational rhythms by ingesting local context, user roles, and maintenance patterns to identify what's real, and what a false positive looks like.

Remediation

You decide what Trellix Wise for Private Cloud can enforce, and when. Every action is scoped to the confidence thresholds and permissions your team sets, high-impact moves like isolating a host wait for analyst confirmation, and a persistent "Abort All" halts every connected tool in seconds. One governed action, through infrastructure you already trust.

Hunting

The most dangerous threats never trip a rule, they live in the gaps. Our Hunting Agent doesn't wait for an alert, it actively goes looking, turning intelligence into continuous hunts across your telemetry. Proactive security that surfaces what detections miss, able to hunt within your environment, and never needing to connect to the cloud.

Specifications

Deployment	▪ VMWARE ESX i- (single GPU) 8.0 Update 3g ▪ VMWARE ESXi - (multi GPU) vSphere 9 U1 ▪ KVM - Almalinux 9.6 ▪ Hyper-V - Windows Server 2022 ▪ Harvester.io - 1.3.2+ ▪ AWS (G7e.24xlarge+ or P5.4xlarge) ▪ GCP (a3-ultra or a3-high-gpu-2g) ▪ Azure support only for WISE-VM3000 (Standard_NC24ads_A100_v4)
Agents	▪ Investigation ▪ Remediation ▪ Hunting

Compliance standards

Trellix Wise for Private Cloud is built to meet enterprise compliance and security standards.

- FIPS 140-3
- Common Criteria (CC) evaluation in progress

Virtual infrastructure specifications

Model	WISE-VM3000	WISE-VM5000	WISE-VM7000
CPU	24	32	48
RAM	128	192	256
GPU (NVIDIA H200)	1	2	4
Disk	2 TB	5 TB	10 TB

Contact your account team for a [demo](#), and learn more about Trellix Wise at trellix.com.