SecureWatch

AI-Powered SIEM & XDR Platform

FedRAMP High Authorized | DoD IL4/IL5 Ready

Wazuh SIEM/XDR Engine | Agentic AI Layer | AWS GovCloud + Bedrock/Claude

---

Service & Pricing Guide

Enterprise-grade security monitoring with built-in AI that turns every analyst into a threat hunter — at a fraction of the cost of legacy SIEM platforms.

FedRAMP High Authorized | 421 NIST 800-53 Controls

Agentic AI: Auto-Decoders | NL Threat Hunting | OSCAL KSI Automation

FISMA High | DFARS 252.204-7012 | DoD IL4/IL5 | CMMC Ready

AWS GovCloud (US) | Bedrock/Claude | FIPS 140-2 Validated

Platform Overview

SecureWatch is a fully managed, FedRAMP High Authorized SIEM and XDR platform that combines the proven Wazuh open-source engine with a proprietary Agentic AI layer powered by AWS Bedrock and Anthropic's Claude. Authorized at the High impact level — the most rigorous FedRAMP baseline — and hosted exclusively on AWS GovCloud with FIPS 140-2 validated encryption, SecureWatch is purpose-built for Department of Defense agencies, intelligence community support contractors, and civilian agencies with High-impact information systems.

What sets SecureWatch apart is not just its authorization level, but what it does with it. The integrated AI layer automates the three highest-cost categories of security operations labor: log source onboarding, threat investigation, and compliance reporting. Every feature of the AI layer — including natural language threat hunting, automated decoder generation, and real-time OSCAL reporting — is included in the base subscription at no additional charge.

The Agentic AI Layer

Deployed as a GovCloud-native AI sidecar using AWS Bedrock and Anthropic's Claude, the proprietary AI layer automates the highest-cost categories of human analytical labor. Every AI interaction is fully auditable with complete query provenance for chain-of-custody compliance.

Auto-Decoder Generation	Natural Language Threat Hunting	Automated KSI & OSCAL Reporting
Reduces onboarding of legacy agency hardware from weeks to minutes. The AI ingests raw sample log output from any source — mainframes, SCADA/ICS devices, bespoke agency applications — and produces validated Wazuh decoder XML and correlation rules. Each decoder undergoes automated regression testing before production deployment.	Empowers Tier 1 analysts to execute Tier 3 forensic investigations through conversational queries, directly addressing the federal cybersecurity talent gap. Plain-language prompts are translated into optimized OpenSearch DSL queries, MITRE ATT&CK tactic correlations, and visual kill-chain reconstructions. Every query is logged with full provenance.	Translates live security telemetry into machine-readable OSCAL artifacts for the FedRAMP PMO, enabling continuous authorization without manual documentation overhead. Maintains real-time mapping between Wazuh detection rules, NIST 800-53 control families, and FedRAMP 20x Key Security Indicators. Drift detection alerts fire within minutes.

Core SIEM/XDR Capabilities

Threat Detection & Response	Compliance & Monitoring	Infrastructure Security
Real-time log analysis and correlation with automated threat intelligence integration, active response, and optional 24x7 managed detection for High-impact environments.	Continuous compliance monitoring mapped to NIST 800-53 Rev 5 High baseline, FISMA, CMMC, DFARS, and HIPAA with automated evidence collection.	File integrity monitoring, DISA STIG and CIS benchmark assessment, vulnerability detection with CVE enrichment, rootkit/malware scanning, and cross-region DR.

Pricing

SecureWatch uses a transparent, per-agent pricing model with volume discounts that reward growth. An “agent” is any endpoint — server, workstation, container, or network device — running the Wazuh agent and reporting to the platform.

All AI capabilities are included in the base subscription at every tier. There are no add-on charges for auto-decoder generation, natural language threat hunting, or automated KSI/OSCAL reporting. Pricing reflects our FedRAMP High authorization, DoD IL4/IL5 readiness, and the full Agentic AI layer.

Volume Tier Pricing

Tier	Agent Count	Per Agent Per Month	Per Agent Per Year	Example Annual Cost
Tier 1	1 – 250	**$28**	$336	$42,000 (125 agents)
Tier 2	251 – 1,000	**$23**	$276	$172,500 (625 agents)
Tier 3	1,001 – 5,000	**$19**	$228	$684,000 (3,000 agents)
Tier 4	5,000+	**$15**	$180	$1,350,000 (7,500 agents)

Includes: FedRAMP High (421 controls) + Auto-Decoder Generation + NL Threat Hunting + OSCAL KSI Automation + Full SIEM/XDR + Compliance Dashboards

Your entire agent count is priced at the single tier that corresponds to your total — pricing is not blended. As you grow into a higher tier, your per-agent cost decreases retroactively.

Pricing Examples

Scenario	Agents	Tier	Monthly	Annual
Small DoD contractor	75	Tier 1	$2,100	$25,200
Mid-size GovCon HQ	400	Tier 2	$9,200	$110,400
Agency program office	2,500	Tier 3	$47,500	$570,000
DoD enterprise rollout	8,000	Tier 4	$120,000	$1,440,000

What's Included

Every SecureWatch subscription includes the complete platform, including the full Agentic AI layer, with no hidden feature gates, no premium tiers, and no per-query AI charges.

Agentic AI Layer (Included at All Tiers)

- Auto-Decoder Generation: AI-powered log parser creation for any source — mainframes, SCADA/ICS, bespoke agency applications — reducing onboarding from weeks to minutes with automated regression testing
- Natural Language Threat Hunting: conversational forensic investigations that translate plain-language prompts into OpenSearch DSL queries, MITRE ATT&CK correlations, and visual kill-chain reconstructions
- Automated KSI/OSCAL Reporting: real-time generation of digitally signed OSCAL JSON artifacts mapped to FedRAMP 20x Key Security Indicators, with drift detection alerting within minutes
- Full Query Provenance: every AI interaction logged with generated query, result set hash, and analyst acknowledgment for complete chain-of-custody compliance and audit trail

Core SIEM/XDR Platform

- Fully managed Wazuh engine with multi-AZ high availability, automated failover, and zero single points of failure
- Real-time log collection, normalization, and correlation across all enrolled agents
- File integrity monitoring (FIM) with configurable policies and real-time alerting
- Vulnerability detection and CVE enrichment with prioritized remediation guidance
- Configuration assessment against CIS Benchmarks and DISA STIGs
- Rootkit and malware detection with automated response capabilities
- Custom rule creation and tuning for organization-specific detection logic

Compliance & Reporting

- Continuous compliance monitoring: NIST 800-53 Rev 5 High, FISMA, CMMC, DFARS, HIPAA
- Pre-built compliance dashboards with exportable evidence packages for audit and ATO support
- Automated monthly ConMon reporting aligned to FedRAMP High requirements
- Customer Responsibility Matrix (CRM) documenting inheritable controls from our High authorization
- DoD IL4/IL5 reciprocity documentation for streamlined DoD ATO processes

Infrastructure & Security

- AWS GovCloud (US) exclusively, with FIPS 140-2 validated encryption at rest and in transit
- Per-tenant isolation: dedicated KMS encryption keys, network micro-segmentation, strict RBAC
- 99.9% uptime SLA with multi-AZ high availability and automated cross-region disaster recovery
- 90-day hot log retention included; configurable WORM-compliant cold archival up to 7 years

- Zero-trust architecture with AWS PrivateLink, WAF, and Shield Advanced DDoS protection

Support & Onboarding

- Dedicated onboarding engineer for agent deployment, platform configuration, and AI feature enablement
- Business-hours technical support (8x5 EST) via email and ticketing portal
- Platform documentation, agent deployment guides, API reference, and AI feature tutorials
- Quarterly business reviews with threat landscape briefings and optimization recommendations

Optional Add-Ons

The following optional services complement your SecureWatch subscription. The AI layer is ***not*** an add-on — it is included in every subscription. These are supplementary services for customers with specific operational requirements.

Add-On	Pricing	Description
24x7 Premium Support	**$3/agent/mo**	Around-the-clock support with 1-hour critical response SLA, dedicated TAM, and priority escalation for High-impact environments.
Extended Log Retention	**$1.50/agent/mo per 90-day block**	Extend hot log retention beyond 90 days, in 90-day increments up to 2 years. WORM-compliant with Object Lock.
Managed Detection & Response (MDR)	**$6/agent/mo**	SecureWatch cleared analysts monitor 24x7, triage alerts, execute response playbooks, and provide incident commander support.
Custom Integration Development	**Scoped per engagement**	Custom decoders, rules, and integrations with SOAR, ticketing, GRC, or DoD platforms (ACAS, eMASS, HBSS).
Compliance Package (CRM + Inheritance)	**$7,500 one-time**	Complete CRM and FedRAMP High control inheritance documentation for your own authorization packages.
Dedicated Tenant Infrastructure	**Custom**	Physically isolated compute, storage, and networking beyond logical tenant separation.
Cross-Domain / SIPR Integration	**Custom**	Architecture support for cross-domain solutions connecting to classified environments. Requires separate authorization.

Competitive Comparison

SecureWatch delivers superior capabilities to legacy SIEM platforms — with built-in AI and a FedRAMP High authorization that most competitors cannot match — at 40-55% lower cost. Estimated comparison for 1,000 agents:

	SecureWatch	Splunk Cloud	Elastic Cloud	Microsoft Sentinel	CrowdStrike Falcon
Est. Annual Cost (1,000 agents)	**$228,000**	$500K+	$300K+	$350K+	$400K+
FedRAMP Level	✓ HIGH	Moderate	Moderate	✓ High	Moderate
DoD IL4/IL5	✓	Limited	Limited	✓	Limited
Built-In AI / LLM	**✓ Included**	$$ Add-on	$$ Add-on	$$ Add-on	$$ Add-on
AI Threat Hunting	✓ NL Queries	Splunk AI Assistant $$	Elastic AI Assistant $$	Copilot Security $$	Charlotte AI $$
Auto Log Onboarding	✓ AI Decoders	✗ Manual	✗ Manual	✗ Manual	✗ Manual
OSCAL / KSI Automation	✓ Real-time	✗	✗	Limited	✗
SIEM + XDR	✓ Both	Add-on	Add-on	Add-on	✓ XDR only
FIM + Vuln + Config	✓ All Included	$$$ Add-ons	Partial	$$ Add-ons	Partial
421 High Controls	✓	✗	✗	✓	✗
Open Source Core	✓ (Wazuh)	✗	Partial	✗	✗

Competitor AI capabilities (Splunk AI Assistant, Elastic AI Assistant, Copilot for Security, Charlotte AI) are all premium add-ons at additional cost. SecureWatch includes AI capabilities in the base subscription.

Billing & Contract Terms

Billing Options

Monthly billing: Invoiced on the first of each month based on peak active agent count from the prior month. No long-term commitment required. AI usage is unlimited — no per-query charges.

Annual prepayment: 10% discount on per-agent pricing with annual commitment and prepayment. Committed agent count with ability to add at contracted tier rate.

Multi-year agreements: Custom pricing for 3- and 5-year terms aligned with federal budget cycles, IDIQ task orders, and DoD program timelines.

Tier Determination

Your pricing tier is determined by total active agents across your organization. All agents are priced at a single tier — not blended. As your count grows into a higher tier, the new lower rate applies retroactively. There is never a penalty for growth.

Service Level Agreement

SLA Metric	Commitment
Platform Availability	99.9% monthly uptime with multi-AZ failover
Log Ingestion Latency	< 5 minutes from agent transmission to searchable index
Alert Delivery	< 2 minutes from detection to notification
AI Query Response	< 30 seconds for NL threat hunting queries
Decoder Generation	< 5 minutes for new log source decoder creation
KSI/OSCAL Update	< 15 minutes from telemetry change to OSCAL artifact
Support (Standard)	4-hour Critical / 8-hour High (business hours)
Support (Premium)	1-hour Critical / 4-hour High (24x7)
Incident Notification	Within 1 hour of confirmed tenant security incident
DR Recovery	RTO: 4 hours | RPO: 1 hour (cross-region failover)

Getting Started

Onboarding to SecureWatch is fast, especially with the AI layer accelerating what used to take weeks.

Step 1: Discovery & Scoping (1–2 meetings)

We map your environment: agent count, OS mix, network topology, classification levels, compliance requirements, and legacy log sources. For DoD customers, we coordinate connection approval and CDS requirements as needed.

Step 2: Tenant Provisioning (2–3 business days)

We provision your isolated environment in AWS GovCloud with dedicated encryption keys, micro-segmented networking, configured dashboards, compliance policy mappings, and AI features enabled and ready.

Step 3: Agent Deployment + AI-Powered Log Onboarding

Deploy the Wazuh agent using your existing tools (SCCM, Ansible, GPO, BigFix). For legacy or custom log sources that don't have pre-built decoders, our AI Auto-Decoder pipeline generates validated parsers and correlation rules in minutes — no manual decoder development required. This is where the AI layer has its most immediate impact: what used to take weeks of professional services time now happens automatically.

Step 4: Tuning & Go-Live (2–4 weeks)

We tune detection rules, configure compliance policies against applicable STIGs and CIS benchmarks, and validate alerting workflows. Your analysts can begin using natural language threat hunting queries immediately. KSI/OSCAL reporting begins generating artifacts on day one.

Ready to get started?

Schedule a demo to see the AI layer in action, or request a tailored quote for your environment.

info@securewatch.us