Sekoia Defend XDR SaaS Platform

Service Description

January 2026

secon.

ConnectProtect Managed Extended Detection and Response

Sekoia is a cloud-native SOC and extended detection and response platform that helps public sector teams detect, analyse, and respond to cyber threats in real time. It unifies threat intelligence, detection, and automated response on a single console.

The service combines contextualised cyber threat intelligence with live telemetry and automation. This gives you accurate alerts with lower false positives, faster mean time to detect and respond, and clearer insight across your IT estate.

Sekoia integrates with existing security systems and supports a wide range of logs, endpoints, cloud services, and network controls. The platform lets your teams prioritise real threats, automate repetitive tasks, and focus effort on investigation and remediation.

The service supports UK Government security standards and reporting needs. You get operational dashboards, threat context, and audit evidence that align with assurance requirements.

Sekoia is available as a SaaS service on G-Cloud, enabling fast procurement, scalable deployment, and clear cost control for central and local government, NHS bodies, and other public organisations.

sekoia

Sekoia Defend
Modern Security Operations, Your Way

Sekoia Defend is a SaaS solution built to meet the evolving needs of security teams —from those just starting their SOC journey to global enterprises managing complex, distributed environments. Whether you're modernizing legacy SIEM tooling or orchestrating advanced hybrid defenses, Sekoia Defend scales with you.

Core

Ideal for teams starting their SOC journey or modernizing outdated SIEM tools. Core includes everything needed for centralized visibility, real-time threat detection, and automated response —with built-in AI assistance and CTI enrichment from day one.

Advanced

Designed for mature security teams needing more control and scale. Advanced adds on-prem SOAR capabilities, expanded threat intelligence management (via custom IoC collections), and fine-grained role-based access controls—making it a strong fit for regulated or hybrid environments.

Prime

Built for high-scale enterprises. Prime includes everything in Advanced, plus full multi-community management, AI-powered incident handling, and full access to Sekoia's premium threat intelligence. Perfect for teams managing large, complex, or distributed environments with high operational demands.

FLEXIBLE DATA RETENTION & TRANSPARENT PRICING

All Sekoia Defend plans include 30 days of hot storage by default, with the option to extend or supplement with archival storage for up to one year.

You can choose between predictable, asset-based pricing (2GB, 3GB, or 5GB per asset per month) or opt for a flexible, volume-based model. Usage is fully transparent and tracked in-platform, giving you complete control over your budget. Our fair-use policy also accounts for real-world conditions —allowing data ingest spikes during security incidents without penalizing your operations.

ANALYST-VALIDATED

Gartner

"[Sekoia] are innovating with advanced detection and remediation capabilities, leveraging generative AI, ITDR, and preemptive security."
TECHSCAPE FOR DETECTION AND RESPONSE STARTUPS 2025

FORRESTER

"[Sekoia named] a notable vendor in The Security Analytics Platform Landscape"
SECURITY ANALYTICS PLATFORM LANDSCAPE 2024

sekoia

Feature	Why It Matters	How It Works	Core	Advanced	Prime
Endpoint Agent	Gain endpoint-level visibility	Lightweight agent for Windows, Linux, macOS collects telemetry securely	✓	✓	✓
Third-Party Integrations	Aggregate telemetry from all tools	200+ integrations with top vendors (Microsoft, CrowdStrike, Fortinet, etc.)	✓	✓	✓
Custom Intakes	Ingest unique data sources	Build new integrations using a guided event	✓	✓	✓
Asset Discovery	Understand your attack surface	Visualize infrastructure to prioritize risks and support investigations	✓	✓	✓
Open API	Automate and integrate	Full API access for data sharing and custom workflows	✓	✓	✓
Detection Content Library	Identify threats with precision	1000+ MITRE-mapped rules built and maintained by CTI experts	✓	✓	✓
Anomaly Detection	Spot suspicious behavior early	ML-powered analysis detects deviations from normal activity	✓	✓	✓
Retrohunt	Uncover past threats	Historical logs are scanned against new IoCs automatically	✓	✓	✓
Sigma support	Correlate detection logic	Sigma rules natively supported and correlated in real time	✓	✓	✓
CTI Context in Alerts	Triage with confidence	Alerts are enriched with real-time threat intelligence	✓	✓	✓
AI Assistant (ROY)	Augment analyst workflow	In-platform AI guides analysts through detection and response	✓	✓	✓
Sekoia Operating Language	Hunt and investigate	Advanced query builder supports hunting, audit, and reporting	✓	✓	✓
Custom Dashboards	Visualize what matters	Build dashboards to match your workflows and KPIs	✓	✓	✓
Cloud SOAR	Automate and respond in the cloud	Drag-and-drop playbooks for detection, enrichment, and response	✓	✓	✓
Notebooks	Centralize investigations	Collaborative workspace for documenting and reusing investigations	✓	✓	✓
IoC Collections	Import external threat intel	Import IoCs from remote sources to complement Sekoia intelligence		500k	5m
Role based access control	Adapt permissions to match users roles	Create granular user roles beyond default permissions		✓	✓
On-prem SOAR	Respond across hybrid infrastructure	Unified playbooks for SaaS and on-prem environments		✓	✓
Multi-Community Management	Manage complex environments	Multi-tenancy architecture supports large organisations to manage multiple communities			✓
AI Cases	Speed up incident response	Group related alerts in real time, enriching context for faster triage			✓
Premium CTI [1]	Stay ahead of evolving threats	Access to Sekoia's full threat research and strategic intelligence	Optional	Optional	✓ [2]

(1) See Sekoia intelligence data sheet for full information. (2) For communities with more than 3000 assets

CHOOSING THE RIGHT PLAN

If you're looking to...	Choose...
Launch or modernize your SOC with core XDR and automation	Core
Add on-premise orchestration, stricter controls, and expanded threat intel	Advanced
Manage large-scale or multi-tenant environments with AI support and premium CTI	Prime

GET STARTED

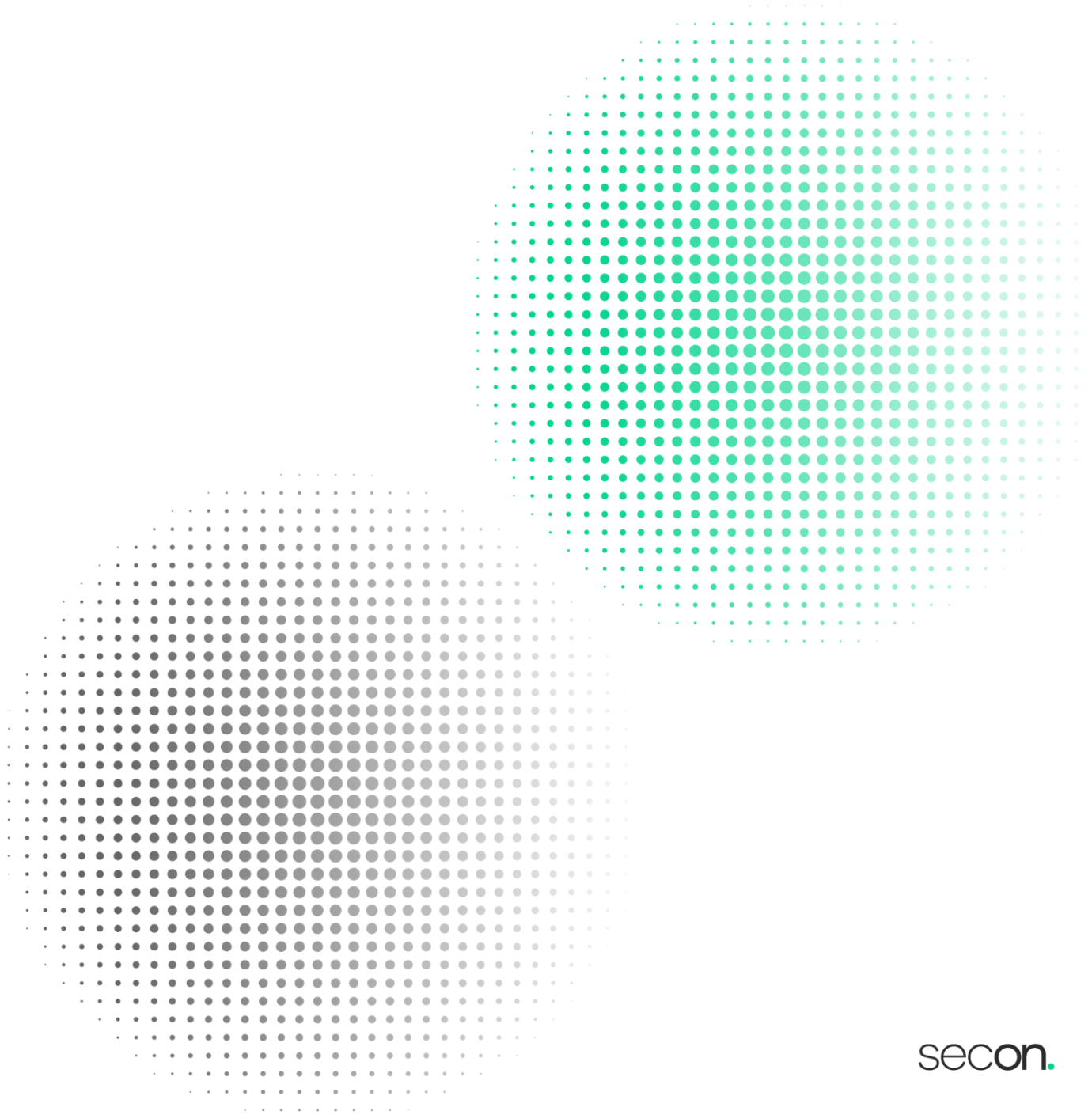
Sekoia Defend offers a faster, smarter way to secure your organization.

Ready to modernize your SOC?

Contact us to schedule a demo

secon.

Thank you.



secon.