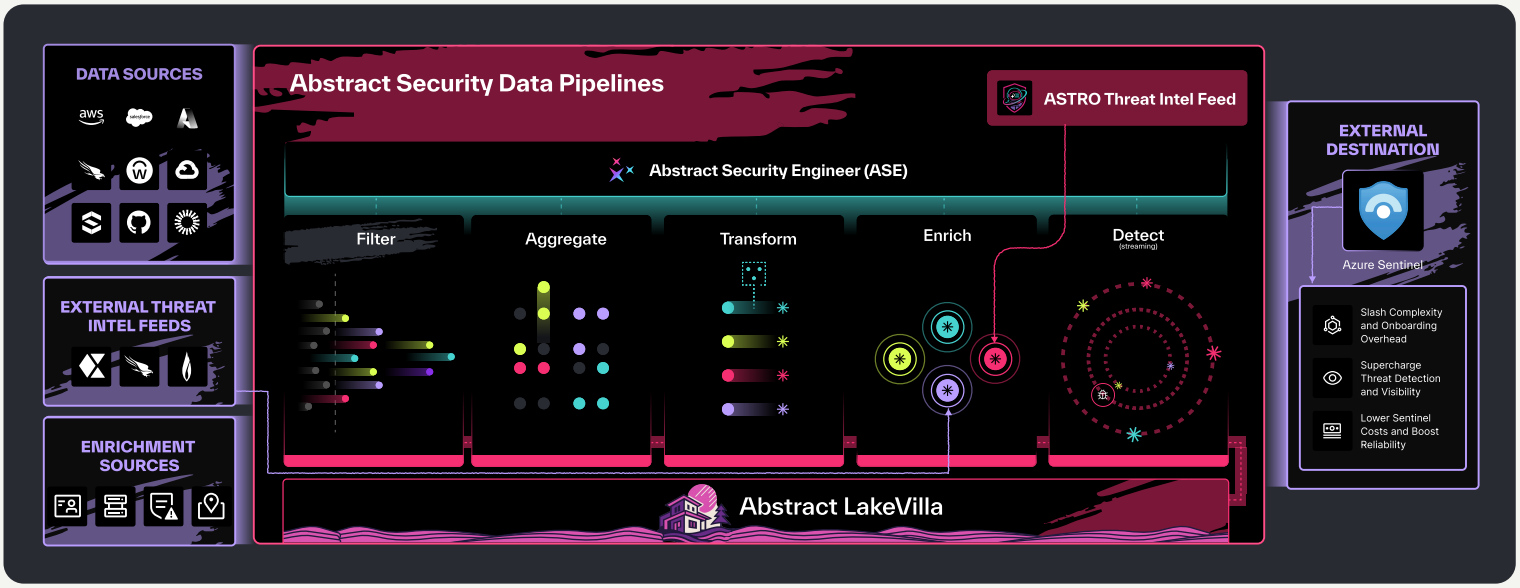
abstract security

Abstract + Microsoft Sentinel: Better Together

Microsoft Sentinel delivers native visibility and analytics across the Microsoft cloud and Windows ecosystem, backed by powerful KQL and built-in threat intelligence. Abstract Security complements Sentinel with real-time streaming detections, cost-efficient data pipelines, and no-code integrations for SaaS and multi-cloud sources — **helping teams maximize security outcomes while reducing operational overhead.**



Top 3 Reasons to Use Abstract with Microsoft Sentinel

01. Easier Data Onboarding Across the Modern Stack

- **Microsoft Sentinel** ingests data through Azure-native connectors and requires individual Data Collection Rule configurations.
- **Abstract** adds no-code SaaS, Syslog, and API integrations with global policies that eliminate manual scripting and maintenance.
- **Together:** Security teams onboard diverse data sources quickly, without custom pipelines or extra overhead.

02. Faster, More Flexible Detections

- **Microsoft Sentinel** supports 512 scheduled rules and 50 near real-time rules, with batch latencies of 5–15 minutes.
- **Abstract** enables thousands of streaming detection rules across SaaS, identity, and multi-cloud environments with sub-second latency.
- **Together:** Teams detect threats earlier and at greater scale, improving response speed and coverage.

03. Lower Costs and Greater Reliability

- **Microsoft Sentinel** retains data in Azure storage tiers, but ingestion and retrieval costs can increase rapidly.
- **Abstract** reduces data volumes by 60–80 percent before ingestion, applies checkpointing to prevent gaps, and offers cost-efficient retention options.
- **Together:** Security teams cut costs while ensuring reliable access to the data they need.

Building on Microsoft Sentinel with Abstract Security

Capability	Microsoft Sentinel	Abstract Security
Data Collection	Uses Azure Function–based connectors that require setup, debugging, and ongoing management.	Adds no-code SaaS, Syslog, and API integrations that eliminate manual scripting and maintenance.
Complexity	Supports Data Collection Rules (DCRs) for detailed configuration and control.	Simplifies management with global policies that apply across data sources, reducing setup overhead.
Detection Rules	Includes 512 scheduled rules and 50 near real-time rules for Microsoft environments.	Adds unlimited streaming rules with sub-second latency to cover SaaS, identity, and multi-cloud telemetry.
Threat Intelligence	Delivers Microsoft-native intelligence with optional manual third-party integrations.	Complements this with out-of-the-box support for additional feeds that enrich detections in real time.
Query Flexibility	Offers KQL and natural-language query builder for powerful analytics.	Provides a visual rule builder to complement KQL, making complex detections easier to design.
Data Retention	Stores data in Azure Blob tiers with flexible retention and compliance options.	Offers cost-efficient retention choices that complement Sentinel tiers and optimize storage costs.

Ideal Use Case:

Microsoft Sentinel is best for organizations with a strong Microsoft footprint, providing deep visibility into Microsoft 365, Azure, and Windows with powerful KQL analytics. Abstract Security expands this reach with SaaS and multi-cloud integrations, real-time streaming detections, and cost-efficient pipelines. Together, they give teams broader coverage, faster insights, and more predictable costs.

Introducing Data Filtering Capabilities

- Microsoft Sentinel provides options like Azure Monitor Agent or Logstash for basic filtering to manage costs, but these often require custom setup and tuning. Abstract adds advanced, vendor-agnostic filtering through a simple drag-and-drop interface, giving teams more precise control without needing KQL.

Cost-Effective Data Ingestion

- \Sentinel offers free ingestion for Microsoft cloud data, but costs increase quickly with third-party sources. Abstract reduces volumes by 60–80% before they reach Sentinel, allowing organizations to retain visibility while keeping ingestion costs under control.

True Real-Time Detection

- Sentinel supports 50 near real-time rules and 512 scheduled rules, which deliver strong analytics but with some latency. Abstract brings in thousands of streaming rules across SaaS, identity, and multi-cloud telemetry, giving teams real-time detections at scale.

Complementary Detection Focus

- Sentinel is strongest in Microsoft cloud and Windows endpoint environments. Abstract extends coverage across SaaS, identity, and multi-cloud data, so teams can protect both Microsoft and non-Microsoft assets in a single workflow.

Seamless Migration & Detection Portability

- Sentinel includes partial automation for migrating detection content, like translating Splunk queries into KQL. Abstract simplifies this further by making detection content portable with no scripting required, easing the transition for teams moving from legacy SIEMs.

Streamlined Threat Intelligence Integration

- Sentinel ships with MSTIC intelligence and supports additional feeds, though third-party integrations often take extra effort. Abstract offers out-of-the-box connectors for providers like Flashpoint and Recorded Future, enriching detections in real time and improving triage.