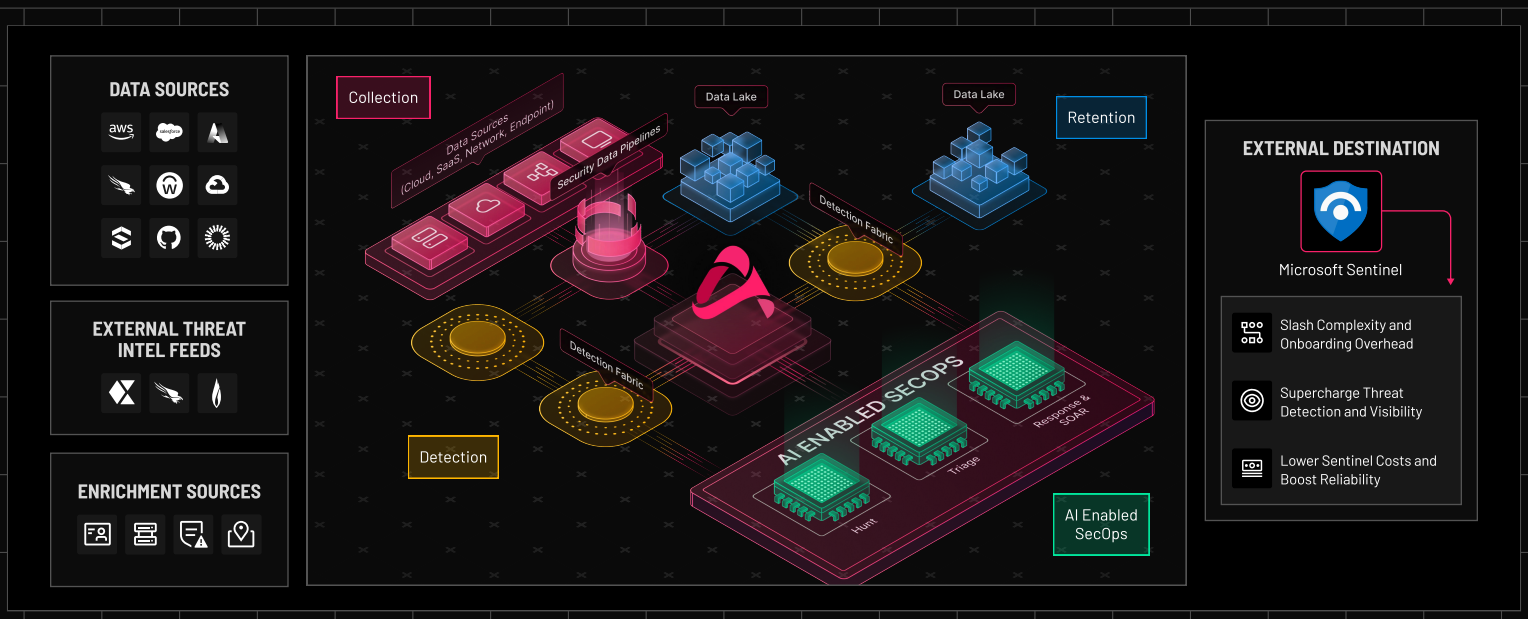
ABSTRACT + MICROSOFT SENTINEL

UNLOCK UNLIMITED REAL-TIME DETECTIONS IN SENTINEL

Microsoft Sentinel delivers native visibility and analytics across the Microsoft cloud and Windows ecosystem, backed by powerful KQL and built-in threat intelligence. Abstract 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 AND 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. SUPERCHARGE THREAT DETECTION AND VISIBILITY

- **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 SENTINEL COSTS AND BOOST 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

CAPABILITY	MICROSOFT SENTINEL	ABSTRACT
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 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 recommends customers filter out irrelevant data before ingestion to reduce costs (Refr: Best practices for data collection – Microsoft), using Azure Monitor Agent or Logstash that support basic filtering capabilities.

Abstract's Security Data Pipelines offer advanced, out-of-the-box, vendor-agnostic filtering capabilities through a simple drag-and-drop interface, with no KQL required.

COMPLEMENTARY DETECTION FOCUS

Sentinel excels at Microsoft cloud and Windows endpoint detections.

Abstract enhances this with robust coverage of SaaS software, enabling broader, cross-platform coverage — ideal for the modern enterprise.

COST-EFFECTIVE DATA INGESTION

Optimized for non-Microsoft sources: Sentinel provides free ingestion for Microsoft Cloud data sources ingesting third-party data can get expensive. Abstract reduces data volume of popular integrations by as much as 60-80% before it hits Sentinel, lowering costs.

SEAMLESS MIGRATION & DETECTION PORTABILITY

Sentinel offers rule translation (e.g., Splunk to KQL) with partial automation.

SIEM Migration experience from Sentinel Abstract provides no tooling/scripts required experience for SIEM migration easing transition from any SIEM to Sentinel without complex manual mapping.

TRUE REAL-TIME DETECTION

Abstract supports thousands of true real-time streaming rules, allowing teams to augment their Azure Sentinel detections for more flexible and immediate responses without eating into Azure Sentinel's Detection rule limits.

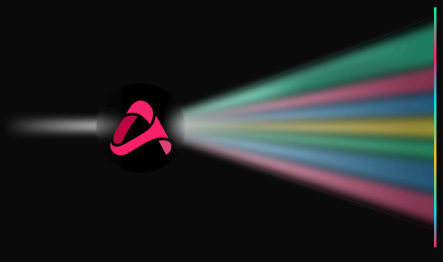
Sentinel supports 50 near real-time (NRT) rules and 512 total detection rules (ref: Service limits for Sentinel.) Batch processing can add minutes of delay due to indexing.

STREAMLINED THREAT INTELLIGENCE INTEGRATION

Sentinel includes MSTIC threat intel out-of-box, but bringing in 3rd-party intel (e.g., Flashpoint, Recorded Future) requires uploading content Refr: Bring your threat intel.

Abstract provides OOTB integrations for third party threat intel, match against real-time data, and send results into Sentinel or other destinations.

SEE IT FOR YOURSELF.



Most teams are up and running with real security outcomes on day one. We'll work with your data, your sources, and your environment — no generic demo.

BOOK A DEMO →