

# Unified Defense SIEM

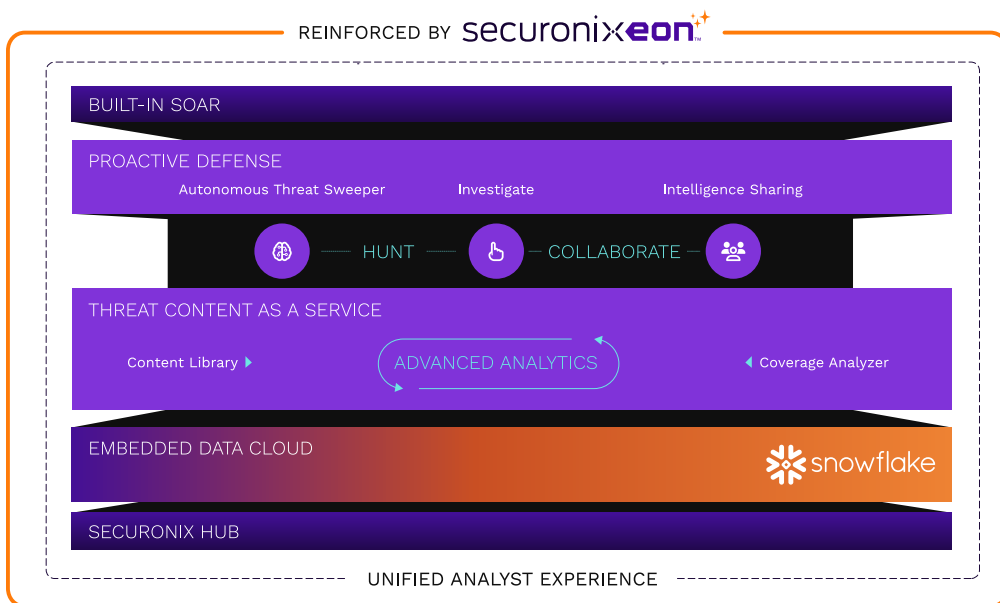
BEST-IN-CLASS THREAT DEFENSE ON THE DATA CLOUD



## Join the SIEM Evolution

As the attack surface continues to expand, many SIEMs have limitations in architecture and technology to meet the cybersecurity needs of modern enterprises. Threats can lie dormant for months without being noticed, emphasizing the need for readily available, searchable data.

To keep pace with modern sophisticated threats, up-to-date threat content is critical to understand when systems are vulnerable to new and emerging threats. The lack of skilled resources makes developing new content difficult, requiring you to depend on third parties to provide continuous content.




## Why Unified Defense SIEM?

 **Highly scalable to meet modern data demands**

Accommodate massive data demands with a highly scalable, single-tiered data storage model. Securonix offers a robust and cost-effective architecture built on Snowflake's Data Cloud that reduces complexity and delivers 365 days of 'HOT' searchable data.

 **Force multiply your SOC with curated threat content**

Unlock broad threat coverage through continuously delivered threat content as-a-service. Access extensive threat research from our world-class Threat Labs, which acts as an extension to your team.

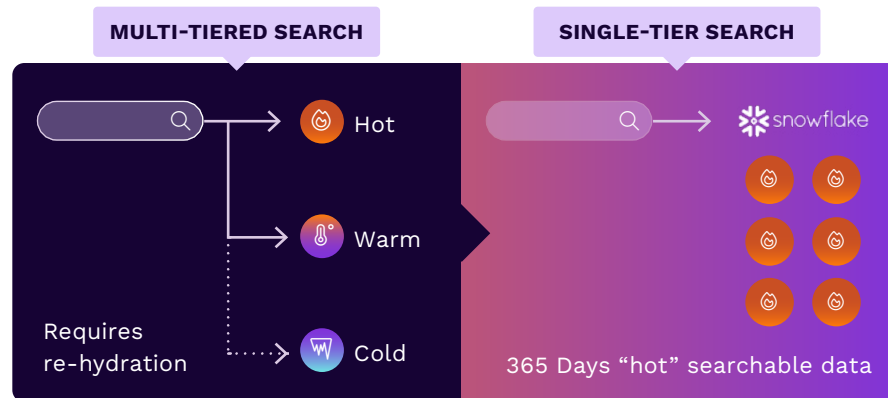
 **Better collaboration and intelligence sharing**

Take a more proactive approach to defense with tools that let you harness the power of your peers and partners. Knowledge sharing and investigations just got easier with autonomous threat sweeps and on-demand context.

## Built with the Data Cloud

Securonix offers a highly scalable architecture powered by Snowflake that can accommodate massive data demands with an easily adaptable data storage model.

- ✓ **365 Days ‘Hot’ Searchable Data:** Easily access critical details before, during, and after a breach. With 365 days of ‘HOT’ searchable data, you’ll have the visibility you need to thoroughly investigate threats.
- ✓ **Single-Tier Storage Model:** Built specifically for large-scale searches, our platform streamlines data management and eliminates performance issues found in traditional tiered-storage models.



## Threat Content-as-a-Service

Securonix takes on the burden of creating threat content for you with continuously updated and delivered cloud connectors, business applications, and content.

- ✓ **Content Library:** Our threat content service is powered by industry-leading analytics and lets you quickly add or update your system with the latest protection against emerging threats.
- ✓ **Threat Coverage Analyzer:** Understand security gaps, your level of SOC maturity, and how your cybersecurity coverage stacks up against industry frameworks such as MITRE ATT&CK with our comprehensive assessment tool.

## Proactive Defense

Unite with your peers and Securonix partners to share intelligence and threat content in the fight against threat actors.

- ✓ **Autonomous Threat Sweeper (ATS):** We codify threats found in the wild and across customer tenants to be used by ATS. This allows you to leverage shared intelligence to retroactively sweep your environment and stay ahead of emerging threats.
- ✓ **Adaptive Threat Modeling:** Securonix EON constructs clear and comprehensible threat chains by seamlessly correlating alerts across your network, facilitating a rapid understanding of potential security risks.
- ✓ **Securonix Investigate:** Securonix Investigate automatically extracts context from data sources for investigations in flight. InvestigateRX builds on Investigate and uses AI to automatically translate raw data into concise, context-aware summaries, reducing investigation times by an average of 15 minutes per incident.

## Unified TDIR Experience

Security teams that use poorly integrated security solutions may delay threat detection and response. That’s why we are streamlining the user experience to deliver detection, investigation, and response in a single interface.

- ✓ **Unified Data Storage:** Leverage consistent data across all TDIR processes. This reduces the need to move, duplicate and correlate data so you can focus on investigating and remediating threats.
- ✓ **Integrated SIEM and SOAR:** Simplify the TDIR process for analysts with seamless workflows across SIEM and SOAR, leveraging the same user interface and Data Cloud.

**For more information about the Securonix Platform, schedule a demo at:**

[WWW.SECURONIX.COM/REQUEST-A-DEMO](http://WWW.SECURONIX.COM/REQUEST-A-DEMO)