




# securonix **eon**™

A NEW ERA OF AI-REINFORCED SECOPS

Cybersecurity teams face an expanding attack surface, new threats, and regulations, while their resources are stretched thin:

-  **Regulatory & Compliance Pressure** is driven by these technological changes, and won't get easier to navigate.
-  **Understaffed & Outmatched** traditional, reactive SecOps will soon fall short. Security teams' resources can't match the evolving threat landscape.
-  **A Digital Tsunami** is expanding and changing the attack surface with the mass-adoption of cloud, OT/ICS, 5G, and AI technologies.
-  **Attacks Powered by AI** are changing the cybersecurity landscape, introducing new sophisticated threats to identify and defeat.

Introducing Securonix EON, a groundbreaking suite of AI-Reinforced capabilities to transform SecOps in the face of AI-powered threats.



## The Pillars of Securonix AI-Reinforced SecOps

The cornerstone of Securonix's innovative approach rests on three core pillars:

### AI-Reinforced Platform

The platform leverages AI at all layers to make precise security decisions at high speed, focusing human intervention where most valuable.

### Seamless Integration

Seamlessly and agnostically integrates with existing tools and technologies to create a unified defense architecture, maximizing the value of your security investments.

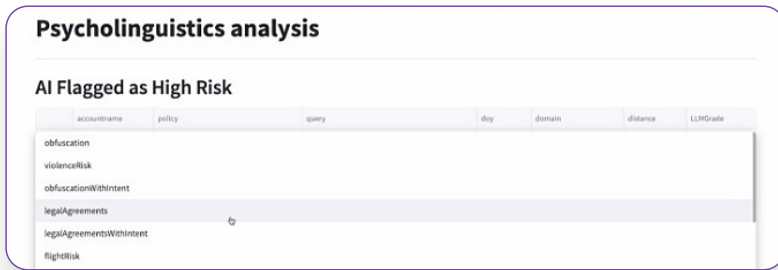
### Frictionless Security Experience

Delivers reduced noise, an intuitive user experience and targeted threat intelligence to empower teams to counter sophisticated threats.



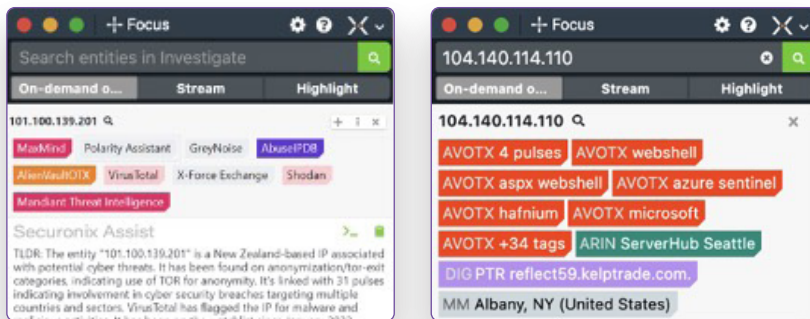
### Insider Intent Agent

Our industry first Insider Threat Psycholinguistics feature employs AWS bedrock based, Large Language Models to accurately and efficiently discern the intent behind a user's language and behavior, identifying malicious activity and giving a TLDR summary of the user's actions.



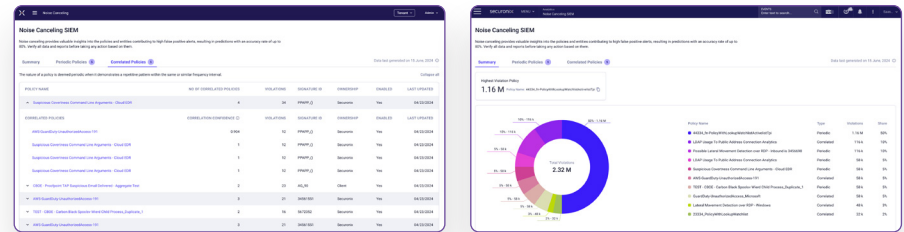
### Investigate Agent

Securonix Investigate automatically extracts context from data sources for investigations in flight. Security teams can share knowledge and collaborate within the investigation without pivoting to external tools like ticketing, email or messaging. InvestigateRX builds on this by converting retrieved personalized and objective content into a coherent and context-aware summary, analysts are empowered to make swift decisions and save approximately 15 minutes per incident.



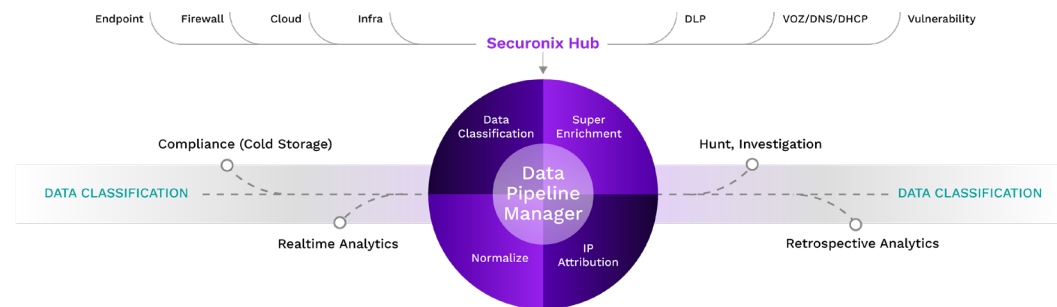
### Noise Cancellation Agent

By leveraging AI, we empower your analysts to quickly zero in on the alerts that really matter. Our innovative approach reduces duplication and irrelevant alerts and improves analyst efficiency and effectiveness. Noise Cancellation also auto picks SOAR playbooks, through our free SOAR LITE module, for auto investigations and remediations, accelerating response and reducing incident impacts.



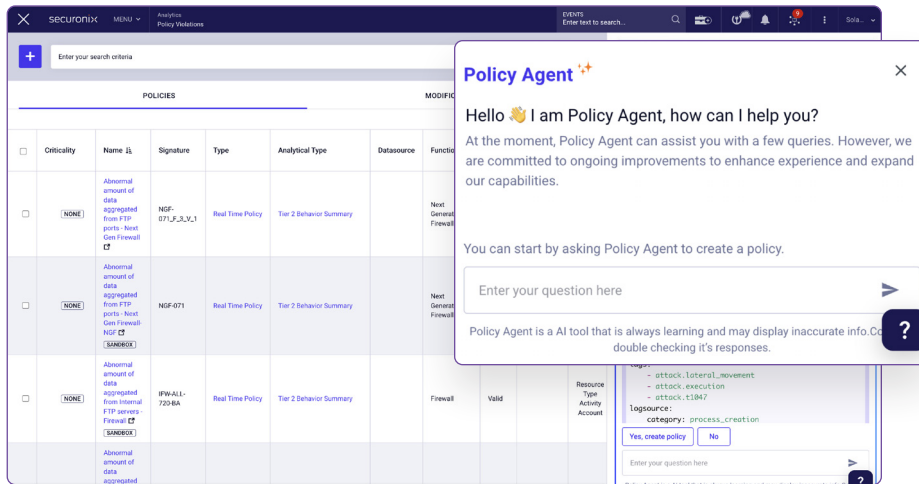
### Data Pipeline Manager (DPM)

By intelligently classifying and organizing data, Data Pipeline Manager empowers your SecOps team to focus on critical threats, increasing efficiency by up to 30%. Our modular architecture and embedded data fabric enables intelligent data classification, ensuring just the right data gets analyzed, stored and archived, controlling costs without compromising security and compliance.



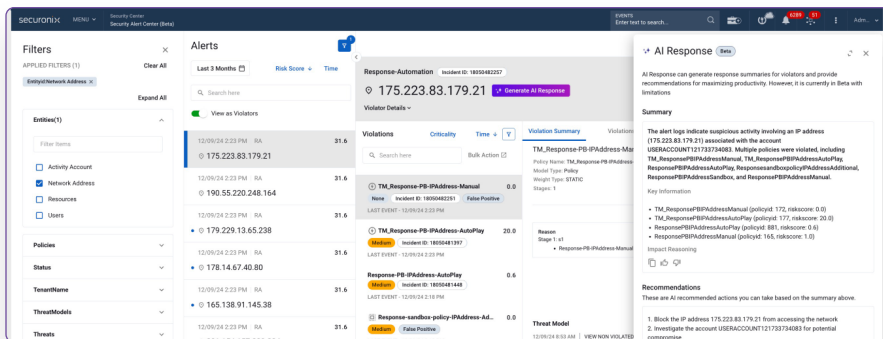
### Policy Agent

Turns analyst intent into high-precision detection content, faster. Policy Agent transforms natural language objectives into deployable detection rules. It simulates outcomes before deployment, flags issues, and enables analysts to craft and refine detection content with unprecedented speed and clarity.



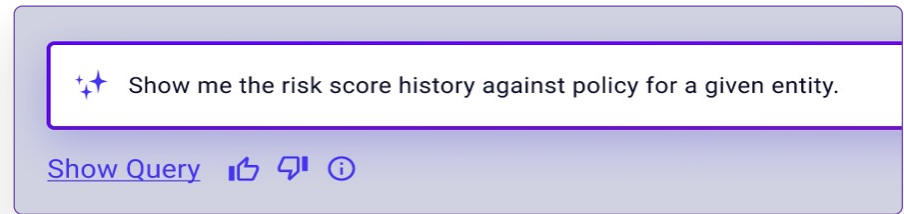
### Response Agent

Accelerates threat response by executing high-confidence containment actions without delay. When a validated threat is detected, the Response Agent initiates containment and remediation actions—like user lockouts, host isolation, or session revocation—while enforcing escalation policies.



### Spotter Agent

Helps analysts investigate faster by querying data lakes and surfacing relevant anomalies. Spotter Agent functions as an autonomous threat hunter. It translates analyst intent from natural conversational requests into optimized queries across Snowflake and other data lakes, surfacing anomalies using behavioral baselines and risk scores, and continuously learns through analyst feedback to fine-tune investigations.



### Threat Intel Agent

Summarizes and enriches investigation findings in plain language, helping analysts quickly grasp threat severity and context without wading through raw data. This accelerates response actions with less room for error.

## Your Partner in the SecOps Era

Securonix, a 5x leader in Gartner's Magic Quadrant for SIEM, offers the experience and tools to enable SecOps teams.

**Deep AI Expertise** Over a decade of experience in AI-driven security underpins our solutions (UEBA, SOAR, etc.).

**Future-Proof SIEM** The Securonix Unified Defense SIEM platform provides ultra fast 365 days of hot single-tiered search, BYO cloud, on-demand scalability and data enrichment.

**Proven Accuracy & Detection** Our solutions empower analysts with high-fidelity and targeted threat intelligence for confident decision-making.

**Continuous Innovation** We invest in threat research, advanced data science, AI capabilities, content as a service and seamless user experiences to stay ahead of threats.