securonix

Security Orchestration, Automation, and Response
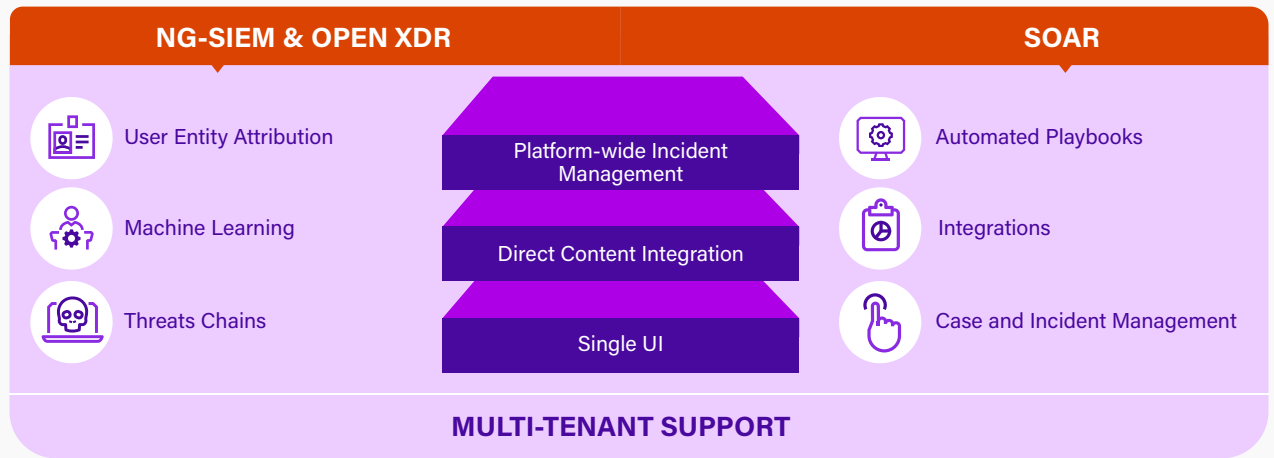
Streamline Investigation and Response with Embedded SIEM + SOAR

Why Securonix?

Rapid response is essential to mitigate the risks of cybersecurity threats. However, many security teams leverage poorly integrated SIEM and SOAR solutions, adding unnecessary complexity and delays to threat detection and response.

Securonix SOAR helps SOCs accelerate incident response by bringing all the details from their IT environments into a single pane of glass. By simplifying investigations with a converged view for detection and response, we help security teams drive efficiency and reduce complexity for a faster MTTR.

NG-SIEM & OPEN XDR | **SOAR**

- User Entity Attribution
- Machine Learning
- Threats Chains

Platform-wide Incident Management
Direct Content Integration
Single UI

- Automated Playbooks
- Integrations
- Case and Incident Management

MULTI-TENANT SUPPORT

The Benefits of SOAR

Accelerate Incident Response

Securonix helps your team work smarter, not harder. Our integrated SOAR offering simplifies the analyst experience and streamlines the end-to-end incident response cycle with a seamless workflow for threat detection, investigation, and response.

Respond to Threats at Scale

Securonix SOAR was built in the SIEM, not bolted on, so you have zero infrastructure to manage, and unlimited scalability. Our unified platform consolidates data sharing and delivers threat detection and response in a cloud-native architecture that evolves with you as you grow.
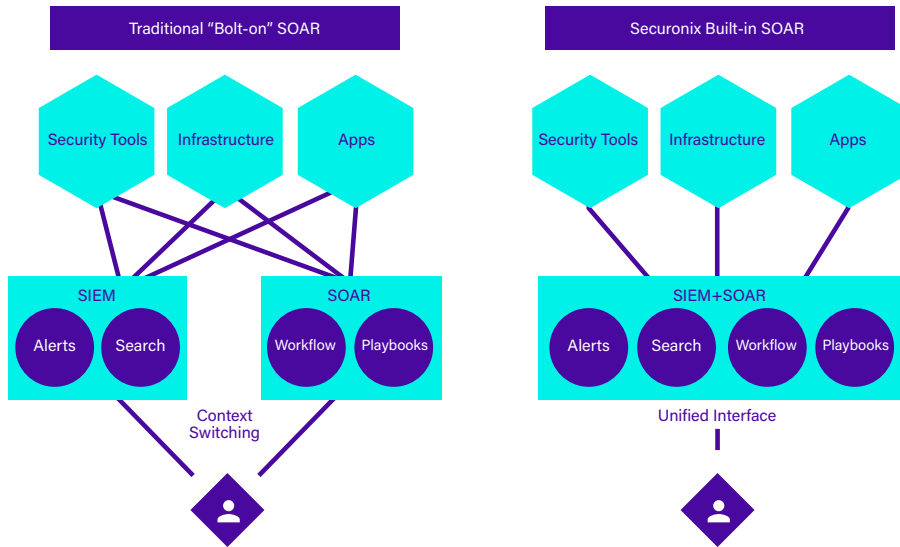
Maximize Security Operations Investment

In combination with Securonix SIEM or Open XDR, our SOAR offers unified detection and response reporting to help you identify and address constraints in your security operations process. SOAR also offers simple add-on licensing in line with our SIEM, with no hidden costs or additional variables.

Experience a Built-In, Not Bolted on, Embedded SOAR

In synergy with Securonix Next-Gen SIEM and Open XDR, Securonix SOAR creates the industry's first true end-to-end cybersecurity operations fabric for threat detection, response, automation, and orchestration across endpoints, networks, and the cloud.

Simplified Licensing and Operations

Flat Pricing: Securonix is simplifying licensing by providing a flat pricing model that allows for unlimited analyst usage at no extra costs.

Content as a Service: SOAR customers gain free access to consistently updated threat content through a one-click opt-in process. This enables new integration and playbook content to be updated regularly to meet the demands of evolving SIEM and XDR detection content.

Seamless Playbook Management

OOTB and Custom Playbook Actions: Leverage pre-built playbooks that cover the most common use cases out-of-the-box, or create your own with our flexible, user-friendly Playbook Designer.

Cloud-Native SOAR: Built with a pure, SaaS architecture, security teams can easily incorporate response playbook actions into the SIEM policies without having to switch screens or tools.

Integrations: Scale playbook actions with the orchestration of best-in-breed tools like EPP, EDR, next-gen firewalls, and more.

Multi-Tenant Response for MSSPs

Securonix supports response actions in a multi-tenant environment, enabling your analysts to take actions across multiple tenants from a centralized console. This capability is beneficial for managed service providers using Securonix to support multiple diverse customers.

For more information about the Securonix SOAR, schedule a demo at: **www.securonix.com/request-a-demo**

securoni**x**