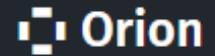


WatchGuard Orion

Proactive Cybersecurity. Efficient Security Operations



Modern SOC Challenges

Modern SOC's face several challenges, including the rapid evolution of threats, the high volume of security alerts, and a significant shortage of skilled cybersecurity professionals. The gap¹ will grow by 35% by 2031. SOC professionals need to address these issues by providing scalable and flexible solutions that enhance threat detection with AI and machine-learning capabilities, automate complex processes, and offer real-time visibility, enabling more efficient threat hunting, detection, incident investigation, and response, ultimately improving SOC efficiency, managing the growing scale and sophistication of cyber threats.



Too Many Alerts
To Manage



Cyber Analysts
Shortage



Shortage of
Expertise and
Collaboration Tools



Tracing
Sophisticated
Techniques

What is WatchGuard Orion?

WatchGuard Orion is a multi-tenant threat hunting and incident detection, investigation, and response Cloud-native solution for SOC's that leverages security analytics, machine learning, and automation to proactively and efficiently uncover and respond to unknown, sophisticated threats.

Benefits

WatchGuard Orion aims to boost SOC analyst productivity, reduce time-to-detection, and enhance overall customer cybersecurity resilience. This is on top of WatchGuard EDR, EPDR, Advanced EPDR, and the Zero-Trust Application Service, augmenting their capabilities with the following:

- **Alert Noise Reduction:** an 80% decrease in alert noise through automated IoA prioritization.
- **Collaboration:** tools to effectively coordinate alert and incident case management, investigations, and response efforts across teams.
- **Automation:** alleviates repetitive tasks such as activity monitoring to detect suspicious behaviors, intelligence-driven and analytics-driven hunting, and investigating repetitive incident cases. It frees analysts for higher-level investigations and proactive threat hunting.
- **Custom proactive threat hunting:** Includes intelligence-driven, analytics-driven, and hypothesis-based hunting to uncover sophisticated threats or unwanted behaviors. The result can be automated through threat-hunting rules.
- **Consolidated SOC tools in just one console:** Streamlined integration with SOC tools out-of-the-box that enables swift triage, investigation, and response.

Flexibility vs Pre-built, Out-Of-The-Box

WatchGuard Orion brings flexibility and efficiency to all SOC members, integrating into a single console powerful tools that enable expert analysts and hunters to configure threat hunting rules, freely investigate incidents by accessing the 365-day enriched telemetry, share their investigations, and extend to others through Jupyter Notebooks. The over-400 pre-built and automated detection analytics rules, created and managed by WatchGuard SOC, investigation console features, and assisted investigations increase analyst efficiency. The combination of Orion's flexibility with automation makes it a perfect fit for SOC teams at any security maturity stage.

Robust APIs and Plugins: WatchGuard Orion offers cloud console and API access for easy SecOps integration. It enables actions on endpoints, real-time and retrospective IoC searches, access to WatchGuard's data lake, retrieval of IoCs, IoAs, and OSQuery data, and more. It supports SIEM (ArcSight, QRadar), ticketing (ServiceNow), and TIPS (MISP) plugins.

1. [Bureau of Labor Statistics](#)

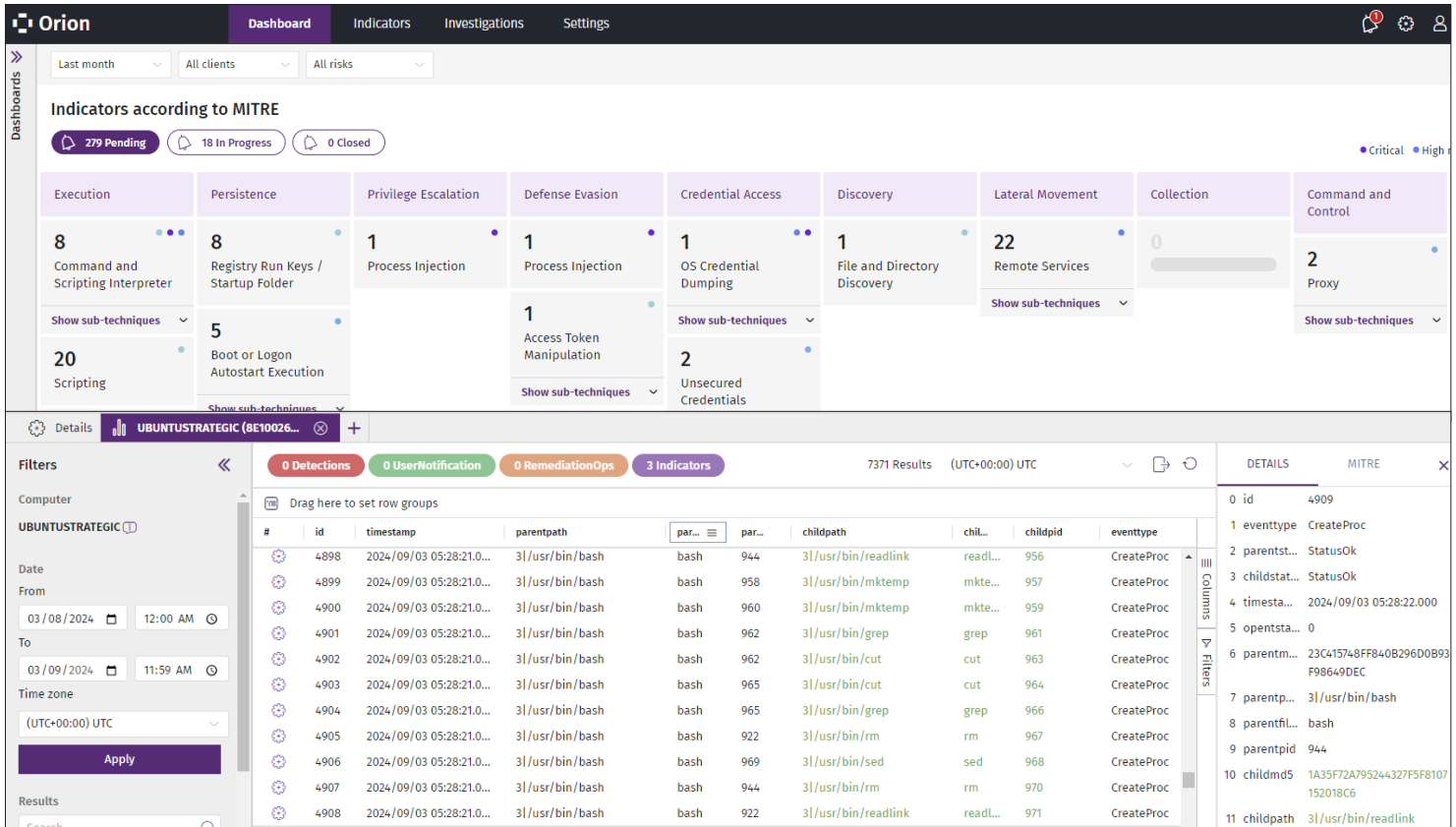


Figure 1. WatchGuard Orion and its features boost efficiency for analysts and threat hunters across WatchGuard's SOC, and partner, and customer SOCs.

WatchGuard Orion Features

WatchGuard Orion is designed to enhance the efficiency of SOC analysts, expedite the detection process, and improve the cybersecurity resilience of customers, building upon the foundation of WatchGuard EDR, EPDR, and Advanced EPDR. It achieves this by augmenting their capabilities with the following features:

- **Cloud-Native Architecture:** A flexible, scalable, and resilient infrastructure ensuring comprehensive visibility.
- **Multi-Tenant Management:** Allows for centralized administration of multiple customers or "tenants" while maintaining separate, secure environments for each tenant's data, configuration, and management.
- **Flexible Views for Role-Based SOC Members Access:** Provides customizable user interfaces tailored to the specific SOC role and ensures they see only the relevant customer data and functions according to their permissions.
- **Real-Time Activity Monitoring:** Monitors and analyzes the endpoint activity and the behavior of all programs in real time.
- **Zero-Trust Application Service:** Classifies 100% of running processes on endpoints, ensuring that only safe applications execute. It employs AI/ML and deep learning to boost the automatic classification of unknown processes.
- **365-Day Data Lake:** Stores enriched events to aid retrospective activity analyses from the first threat movement at the endpoints. The Data Lake can be accessed through queries via the threat hunting API from Jupyter Notebooks, assisted investigations, and the investigation console.
- **Threat Intelligence:** Access to global threat intelligence for informed detection and response strategies.
- **Advanced Security Analytics:** Over 400 pre-built advanced hunting rules mapped to MITRE ATT&CK to instantly uncover sophisticated, hidden threats on the stream of events to reduce detection engineering time significantly.
- **Custom Threat Hunting Rules:** Enable SOC teams to detect abnormal or suspicious behaviors in addition to the pre-built threat hunting rules.
- **Behavior Analytics Engine:** Detects unusual system behavior, triggers prioritized and contextualized indicators of attack (IoAs), and correlates behaviors based on hunting rules.

WatchGuard Orion Features (Cont.)

- **Incident Case Management:** Streamlined SOC member collaboration and workflows to rapidly detect threats and manage incidents efficiently.
- **Investigation with Jupyter Notebook:** Provides a centralized environment for sharing investigation practices and playbooks. Allows in-depth investigations and leverages third-party libraries.
- **AI-Driven Threat Investigation:** Notebooks enable analytics and machine-learning algorithms to instantly uncover and respond to sophisticated, hidden threats.
- **OSquery Integration:** Powerful tool for endpoint monitoring and analytics, allowing SQL-based queries on system data.
- **Investigation Console:** Enables deep investigation of computers, processes, and more with various tools for an in-depth look at activity over time.
- **Investigation Graphs:** Offers visual context and entity relationship mapping from data lake events for clearer understanding and analysis. SOC analysts can interact with the graph by extending the timeline or investigating more in depth.
- **Containment and Remediation Tools:** These include isolating, rebooting, managing processes and services, transferring files, and performing command line operations through remote access to endpoints.
- **APIs and Connectors:** Facilitates integration with other systems for streamlined operations.
- **Assisted Incident Investigations:** Helps analysts investigate cybersecurity incidents without writing and testing code by providing guided steps, relevant questions, and actionable insights, enabling faster investigation, decision-making, and response times.

By combining attack surface reduction, prevention, and effective detection and response strategies, WatchGuard EDR, EPDR, or Advanced EPDR and WatchGuard Orion empower SOC with a robust cybersecurity framework.

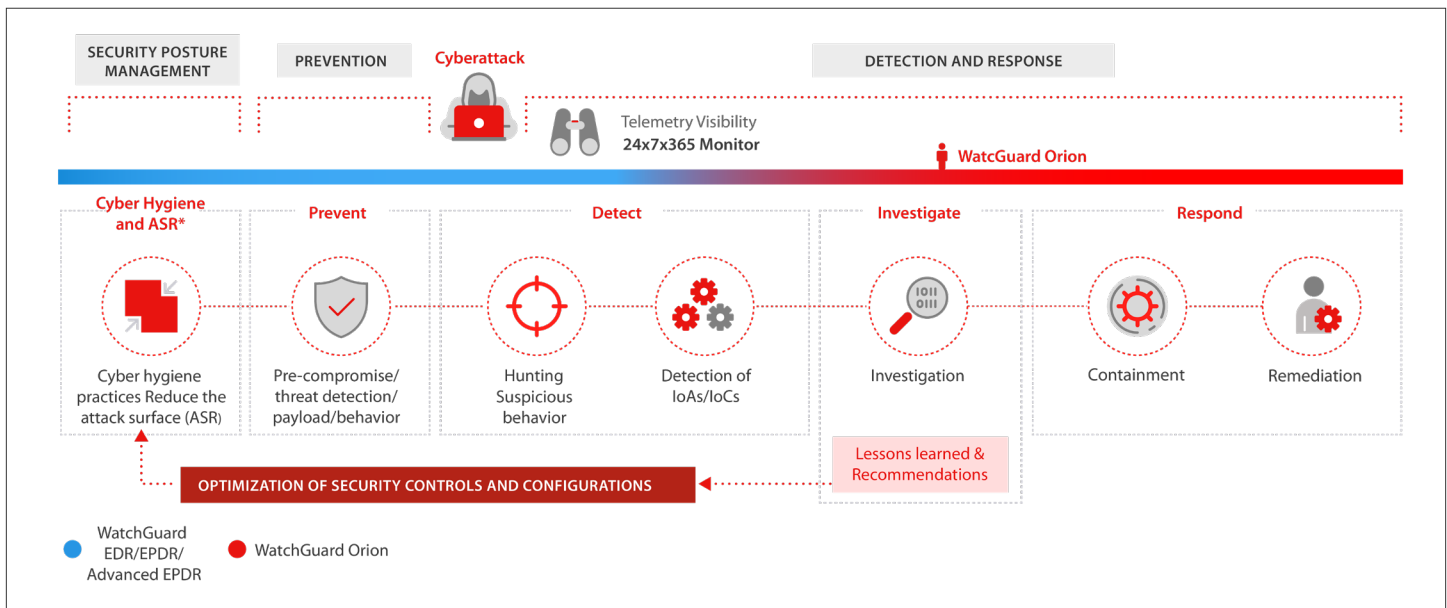


Figure 2. WatchGuard Endpoint Security solutions and modules collaborate with each other to reinforce the entire threat lifecycle, from attack surface reduction and prevention to its detection, response, and investigation for improving defense for future attacks.