

# WatchGuard Orion

Proactive Cybersecurity. Efficient Security Operations

## Modern SOC Challenges

Modern SOCs face several challenges, including the rapid evolution of threats, the high volume of security alerts, and a significant shortage of skilled cybersecurity professionals. The gap<sup>1</sup> 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.

## What is WatchGuard Orion?

WatchGuard Orion is a multi-tenant threat hunting and incident detection, investigation, and response Cloud-native solution for SOCs 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 timeto-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

# • Orion



## DATASHEET

•	Orion	D	ashboar	d I	ndicators Investigation	ons Settings											ے 🕫 🗘
Dashboards	Last month V All clients V All risks																
	Indicators according to MITRE																
	Critical • High																
	Execution	ecution Persistence			Privilege Escalation	Defense Evasion	Credential Access			Discovery		Lateral Movement		Collection			Command and Control
	8 Command and Scripting Interpreter	<b>8</b> Registry Run Keys /		• rs /	1 Process Injection	<b>1</b> Process Injection	<b>1</b> OS Credential Dumping			<b>1</b> File and Directory Discovery	٠	• Remote Services		0			2 Proxy
	Show sub-techniques		•			1 •	Show sub-	Show sub-techniques 🗸				Show sub-technic	how sub-techniques 🛛 🗸				Show sub-techniques 🗸
	20 • Scripting	<ul> <li>5</li> <li>Boot or Logon Autostart Execution</li> <li>Show sub-techniques</li> </ul>				Access Token Manipulation Show sub-techniques	<b>2</b> Unsecure Credentia		•								
C	} Details ₀∬ UBUNTUSTR																
Filte	ers	«	0 De	tections	0 UserNotification	0 RemediationOps 3	ndicators			7371 Results	(UTC+C	0:00) UTC		₿ €		DETAILS	MITRE ×
Com	puter	*	🕅 Dra	ng here to	set row groups											0 id	4909
UBU	UBUNTUSTRATEGIC 🕕			id	timestamp	parentpath	par ≡	par	childpa	th	chil.	. childpid	event	type		1 eventtype	
Date			۲	4898	2024/09/03 05:28:21.0	3]/usr/bin/bash	bash	944	3 /usr	/bin/readlink	read	il 956	Crea	teProc 🔺	ш	2 parentst	
Fron			$\odot$	4899	2024/09/03 05:28:21.0	3 /usr/bin/bash	bash	958	21/mer	/bin/mktemp	mkt				8	3 childstat	StatusOk
03	/08/2024 🗖 12:00 AM	Q							51/usi	ion / macinp	тк	e 957	Crea	teProc	Ē		
		$\odot$	$\odot$	4900	2024/09/03 05:28:21.0	3]/usr/bin/bash	bash	960		/bin/mktemp	mkt			teProc teProc	Columns	4 timesta	2024/09/03 05:28:22.000
То		0	۲	4900 4901	2024/09/03 05:28:21.0 2024/09/03 05:28:21.0	3 /usr/bin/bash	bash bash	962	3 /usr 3 /usr	/bin/mktemp /bin/grep		e 959	Crea		7	5 opentsta	0
	/09/2024 📋 11:59 AM		⊕ ⊕					962	3 /usr 3 /usr	/bin/mktemp	mkt	e 959	Crea Crea	teProc	7	5 opentsta	
03	/09/2024 📋 11:59 AM e zone		⊕ ⊕	4901 4902 4903	2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0	3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash	bash bash bash	962 962 965	3 /usr 3 /usr 3 /usr 3 /usr	/bin/mktemp /bin/grep /bin/cut /bin/cut	mkt grep	e 959 961 963 964	Crea Crea Crea Crea	teProc teProc teProc teProc	H	5 opentsta	0 23C415748FF840B296D0B93
03 Time			0 0 0	4901 4902 4903 4904	2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0	3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash	bash bash bash bash	962 962 965 965	3 /usr 3 /usr 3 /usr 3 /usr 3 /usr	/bin/mktemp /bin/grep /bin/cut /bin/cut /bin/grep	mkt grep cut	e 959 961 963 964 966	Crea Crea Crea Crea Crea	teProc teProc teProc teProc teProc	7	5 opentsta 6 parentm	0 23C415748FF840B296D0B93 F98649DEC
03 Time	e zone TC+00:00) UTC		00 00 00 00	4901 4902 4903 4904 4905	2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0	3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash	bash bash bash bash bash	962 962 965 965 922	3 /usr 3 /usr 3 /usr 3 /usr 3 /usr 3 /usr	/bin/mktemp /bin/grep /bin/cut /bin/cut /bin/grep /bin/rm	mkt grep cut cut grep rm	e 959 961 963 964 966 966	Crea Crea Crea Crea Crea Crea	teProc teProc teProc teProc teProc teProc	7	5 opentsta 6 parentm 7 parentp	0 23C415748FF840B296D0B93 F98649DEC 3]/usr/bin/bash bash
03 Time	e zone		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	4901 4902 4903 4904 4905 4906	2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0	3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash	bash bash bash bash bash bash	962 965 965 922 969	3 /usr 3 /usr 3 /usr 3 /usr 3 /usr 3 /usr 3 /usr	/bin/mktemp /bin/grep /bin/cut /bin/cut /bin/grep /bin/rm /bin/sed	mkt grep cut cut grep rm sed	e 959 961 963 964 966 966 967 968	Crea Crea Crea Crea Crea Crea	teProc teProc teProc teProc teProc teProc teProc	7	5 opentsta 6 parentm 7 parentp 8 parentfil	0 23C415748FF840B296D0B93 F98649DEC 3]/usr/bin/bash bash
03 Time	e zone rc+00:00) UTC Apply		00 00 00 00	4901 4902 4903 4904 4905	2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0 2024/09/03 05:28:21.0	3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash 3 /usr/bin/bash	bash bash bash bash bash	962 965 965 922 969 944	3 /usr 3 /usr 3 /usr 3 /usr 3 /usr 3 /usr 3 /usr 3 /usr	/bin/mktemp /bin/grep /bin/cut /bin/cut /bin/grep /bin/rm	mkt grep cut cut grep rm	e 959 961 963 964 966 966 967 968 970	Crea Crea Crea Crea Crea Crea Crea	teProc teProc teProc teProc teProc teProc	7	5 opentsta 6 parentm 7 parentp 8 parentfil 9 parentpid	0 23C415748FF840B296D0B93 F98649DEC 3]/usr/bin/bash bash 944

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.
- Al-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.

U.S. Sales 1.800.734.9905 International Sales +1.206.613.0895 Web www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2024 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67762\_041224