Cytomic is now WatchGuard for SOCs

FAQ for WatchGuard Cytomic customers, partners, and prospects

Q. What does it mean that WatchGuard Cytomic is now WatchGuard for SOCs?
A. When WatchGuard acquired Panda Security in June 2020, Panda Security was marketing and selling endpoint cybersecurity products and services under the Cytomic brand.

These solutions offered specific features and capabilities for companies with a security operations center (SOC), to serve internally in the organization or to serve their customers. Following the acquisition, a co-brand, WatchGuard Cytomic, was implemented and a dedicated sales team continues to support these specialized customers and partners.

Now that the entire Panda Security portfolio and its security services are integrated into WatchGuard Unified Security Platform^{TM}, the next step, already underway, is the integration of the proactive hunting, detection, and response capabilities of WatchGuard Cytomic.

Q. What does it mean from the point of view of products and services?
A. With this consolidation, the solutions previously marketed under the WatchGuard Cytomic brand become WatchGuard-branded and integrated into the portfolio of **Endpoint Solutions for SOCs.**

- **WatchGuard Orion** (formerly Cytomic Orion) is the comprehensive, multi-tenant Cloud platform that enables SOCs to speed up and be more efficient in their proactive hunting, detection, and response operations for unknown and sophisticated cyber threats.
- **WatchGuard Advanced EDR/EPDR** (formerly Cytomic EDR/EPDR) are the endpoint prevention and/or detection and response solutions that, in addition to the Zero-Trust Application Service and the Threat Hunting Service, include advanced security capabilities on top of WatchGuard EDR/EPDR products. These capabilities allow analysts to search for indicators of compromise (IoCs and YARA rules) and set of advanced security policies to reduce the attack surface at the endpoints.
- WatchGuard Cytomic Patch, Encryption, Insights, SIEM Connect and Data Watch **modules** are renamed to their corresponding WatchGuard Endpoint Security Modules.
- **Premium Threat Hunting service** (formerly Bronze Threat Hunting service) - Managed threat hunting service created for our partners to proactively identify and respond to sophisticated threats that have evaded other security controls, but without the hassle of hiring specialized and scarce profiles, such as threat hunters. With the Premium Threat Hunting service, the partner delegates threat hunting activities to WatchGuard's team of hunters.

Q. What are the implications for me that Cytomic is now WatchGuard for SOCs?
A. First of all, these changes do not affect WatchGuard Cytomic customers and partners in the short term. It is a product name change to be consistent with the WatchGuard portfolio and WatchGuard Unified Security Platform, with no functional, security or other implications.

In the medium term, there are exciting plans to evolve the WatchGuard Unified Security Platform by integrating the proactive hunting, detection, and response capabilities of products and services previously marketed as WatchGuard Cytomic. This will enable customers and partners to immediately access the unified security and management capabilities that WatchGuard Unified Security Platform offers as platform features and the broad WatchGuard portfolio of multi-factor authentication, endpoint, secure Wi-Fi, and network security products, managed from a single Cloud-based management console, WatchGuard Cloud.

The branding on the products will change throughout the releases during 2022 and 2023. In the meantime, you will see WatchGuard branding on marketing materials and continue to see Cytomic branding on certain product areas until we complete the integration into WatchGuard systems.

This won't mean any negative changes for customers and partners — on the contrary, they will benefit from many new and enhanced features as their products will be part of the WatchGuard Unified Security Platform.

In fact, as SOCs play a critical role in protecting organizations against the ever-evolving threats and expanding attack surface we are experiencing now and, in the future, the WatchGuard Unified Security Platform will accelerate the modernization, automation, and optimization of the security operations across the network, endpoint, identity and other security environments and controls, anticipating unknown and sophisticated threats before damage is done.

Q. What is the WatchGuard Unified Security Platform?

A. WatchGuard Unified Security Platform elevates the practice of modern security services by offering a **comprehensive portfolio** of multi-factor authentication, endpoint, secure Wi-Fi, and network security products in a fully integrated **security platform.**

It enables the deployment, management, and automation of a true zero-trust security approach and XDR-based security services to accelerate unknown and sophisticated threat detection and remediation at scale. Meanwhile it boosts operational efficiencies to spend more time on what matters most, delivering more value to their customers.

WatchGuard's Unified Security Platform provides:

- **Comprehensive Security**: A complete portfolio of enterprise-grade network security, advanced endpoint security, multi-factor authentication, and secure Wi-Fi services that scale to meet the needs of any organization, regardless of size.
- **Clarity and Control**: WatchGuard Cloud™ enables the delivery and management of hardware, software and subscription cybersecurity services using one, intuitive interface for consolidated administration, visibility, and reporting.
- **Operational Alignment**: We take the complexity out of business operations by offering direct API access, a rich ecosystem of out-of-the-box integrations, and tools for fast, efficient deployment.
- **Shared Knowledge**: Our fully integrated platform makes it easier to adopt a true zero-trust security posture. WatchGuard's Identity Framework and ThreatSync™ correlation engine enable an XDR-based approach to accelerate threat detection and remediation.
- **Automation**: A binding fabric through the entire platform, WatchGuard's Automation Core brings simplicity and scalability to every aspect of security consumption, delivery, and management.

Q. Where do I find WatchGuard Endpoint for SOC information on the WatchGuard website?

A. WatchGuard for SOCs (formerly WatchGuard Cytomic or Cytomic) information can be found on the WatchGuard corporate website as of April 21, 2022, at www.watchguard.com/wgrd-products/security-operations- center-soc

Q. How are WatchGuard Orion and the Premium Threat Hunting service different from the existing WatchGuard Endpoint Security products and services?

A. WatchGuard Endpoint for SOC offers solutions with specific functionality to enhance the capabilities of security operations centers (dedicated in-house SOCs, virtual SOCs or SOC-as-a-service delegated to our partners and hybrid client/partner SOCs) that are staffed to hunt, detect, investigate, and respond to unknown sophisticated threats as soon as possible to mitigate the damage. These advanced threats are able to evade other security controls and are lurking the organization.

WatchGuard Orion provides specialized tools for threat hunters and cybersecurity analysts that enable them to detect, investigate and respond to advanced threats rapidly, leveraging comprehensive 365-day visibility, automated behavioral analysis, and incident case management tools to accelerate root cause analysis and mitigation of those threats.

The Premium Threat Hunting service extends the Threat Hunting Service provided with WatchGuard EDR/EPDR and the advanced version. Qualified WatchGuard personnel continuously monitor the activity on each customer's endpoints and provide actionable information and recommendations, in the event of an incident.

Q. What is the difference between WatchGuard EDR/EPDR and WatchGuard Advanced EDR/EPDR?
A. WatchGuard Advanced EDR/EPDR allows you to import third-party indicators of compromise (IoCs) in STIX 2.0 format (hash, file names, path, domain, IP addresses and Yara rules) and implement a more advanced and proactive set of security policies required by customers with a more mature cybersecurity program.

Q. Does WatchGuard have any plans to expand the Premium Threat Hunting service from 8/5 to 24/7 coverage?
A. Yes, WatchGuard is actively working to have a full 24/7 service coverage for customers and partners in the coming months.