WatchGuard Advanced Endpoint Security for SOCs

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard Orion	WatchGuard Orion-EPDR
Direct access to 365-day endpoint telemetry – Pre-created and custom queries	✓	✓
Behavior analytics – Pre-created and custom Threat Hunting rules	✓	✓
Investigation console and attack graphs	✓	✓
Pre-created and custom Notebooks (automatic investigation) and playbooks	✓	✓
OSQuery and remote shell for deeper investigation	✓	✓
Response: isolate, restart and remote shell to kill processes, run scripts, etc	✓	✓
Orion APIs - IoCs search 365-day retrospectively, OSQuery, queries, etc	✓	✓
STIX IOC and YARA rules search in real time at the endpoints		✓
Threat Hunting Service: High fidelity, deterministic and non-deterministic IOA detection with contextual telemetry		✓
Advanced security policies to reduce the attack surface		✓
Remote Shell to manage processes, files, services, command line, dumps, pcap, etc.		✓
Lightweight Cloud-based agent		✓
Collective Intelligence lookups in real time		✓
Zero-Trust Application Service: Pre-execution, execution and post-execution		✓
In-memory behavioral anti-exploit technology		✓
Decoy Files and shadow copies		✓
Persistent malware detections. Collective Intelligence lookups in real time		✓
IDS, firewall and device control		✓
Web browsing and email protection		✓
Category-based URL filtering		✓
Endpoint access enforcement. Ability to deny connections		✓

ENDPOINT SECURITY AND MANAGEMENT	WatchGuard EPDR	WatchGuard Advanced EPDR
Direct access 7-day endpoint telemetry – Pre-created and custom queries		✓
Investigation console and attack graphs		✓
IoAs and events mapped to MITRE ATT&CK tactics and techniques		✓
CAPA tool information for files (behaviors, strings, imports, exports)		✓
STIX IOC and YARA rules search in real time at the endpoints		✓
Advanced security policies to reduce the attack surface		✓
Remote Shell to manage processes, files, services, command line, dumps, pcap, etc.		✓
Threat Hunting Service: Non-deterministic IOA detection with contextual telemetry		✓
Endpoint access enforcement. Ability to deny connections		✓
Lightweight Cloud-based agent	✓	✓
Collective Intelligence lookups in real time	✓	✓
Zero-Trust Application Service: pre-execution, execution and post-execution	✓	✓
In-memory behavioral anti-exploit technology	✓	✓
Decoy Files and Shadow Copy	✓	✓
Protection of systems when files are created	✓	✓
Threat Hunting Service: High fidelity, deterministic IOA detection	✓	✓
IDS, firewall and device control	✓	✓
Web browsing and email protection	✓	✓
Category-based URL filtering	✓	✓
WatchGuard Unified Security Platform features: WatchGuard Cloud, ThreatSync – XDR	✓	✓

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com