CORTEX XDR VS. SYMANTEC

CORTEX XDR™ BY PALO ALTO NETWORKS

Feature	Why Does This Matter?	Cortex XDR™	Symantec
Management	**Every second counts, from deployment to day-to-day use**	**Cloud-delivered** Simple management with working default policies; no reboot after single agent install; no hardware to deploy	**Difficult to use** Constant configuration tuning; need to manage multiple agents and consoles; hardware needs a lot of maintenance
Protection	**Customers need protection from more than just known and unknown malware**	**Multi-method prevention** ML-based malware prevention; stops exploits, ransomware, scripts, fileless attacks, and malicious behaviors; coordinates defenses across the enterprise	**Signature-dependent** Heavy reliance on static signatures that are resource-intensive and require constant updating
Detection	**You can't detect what you can't see**	**Market-leading visibility** No. 1 coverage in MITRE ATT&CK™ evaluations; ensures accurate detection of sophisticated attacks with behavioral analytics	**More alerts** Additional product requirements; threat intelligence and managed services; inconsistent across operating systems
Investigation & Threat Hunting	**Security teams need productivity gains for all security operations**	**Speeds all investigations** Simplify triage with alert reduction across products; speed investigations with automated root cause analysis; see everything with fast and powerful queries	**Needs experts** Reliant on multiple products with separate interfaces; requires trained personnel to use, along with managed services
Response	**Fast response is crucial to risk mitigation**	**Stops threats quickly** Contain a threat immediately with isolation; kill and block actions even on Next-Gen Firewalls while the Live Terminal allows remote access to any endpoint	**Quarantine-only** Additional EDR product or subscription required to perform anything more than just a quarantine or isolation
Network Traffic Analysis (NTA) & User and Entity Behavior Analytics (UEBA)	**Customers need detection and response for unmanaged devices as well**	**XDR** Expand detection and response from the endpoint; stop attacks even when you can't deploy an agent; leverage data from the network, users, unmanaged devices, and IoT	**Unavailable**