ExtraHop

ExtraHop Reveal(x) vs. Vectra Cognito

Don't Let Threats to Your Enterprise Operate Incognito

Noise is everywhere in enterprise security. It starts with incomplete data sources, leading to missed detections or false alerts, and ends with an insecure attack surface vulnerable to attacks. Because of its limited application layer visibility, lack of decryption, and weak investigation capabilities, Vectra Cognito struggles to help SecOps teams separate signal from noise. With complete visibility, real-time behavioral detection, and guided investigation workflows, Reveal(x) empowers your team to rise above the noise and secure your enterprise from core to edge to cloud.

	REVEAL(X)	VECTRA COGNITO
Sustained Throughput*	**100 Gbps**	**20 Gbps**
Enterprise Application Protocols	**50+**	**10**
Machine Learning	Behavioral Anomaly Detection	Behavioral Anomaly Detection
Decryption	**SSL/TLS** Including TLS 1.3	—
Automatic Critical Asset Classification and Prioritization	✓	—
Investigation	Full Investigations and Threat Hunting	Limited Investigative Data
Transaction Indexing	No Volume Pricing	Priced on Volume
Forensics	Continuous Packet Capture	Limited Packet Capture
Cloud Integrations (Azure, AWS)	✓	✓
Extensibility (Custom Dashboards, Universal Payload Analysis)	✓	—

* Full-stream reassembly, decryption, and full payload analysis before writing to disk.

EXTRAHOP VECTRA

DECRYPTION CAPABILITIES

Encrypted traffic offers great hiding spots for attackers. Reveal(x) decrypts traffic at line rate — even with Perfect Forward Secrecy enabled. This allows Reveal(x) to detect threats such as SQL injection and cross-site scripting where the key features may be encrypted in the transaction payload. Vectra Cognito offers no decryption, forcing the product to rely on information contained in headers rather than the transaction payload to detect threats, which results in lower-quality detections and also makes that rich transaction payload data unavailable for investigations or forensics.

Can you afford to be blind to the 70% of threats lurking behind encryption?

100Gbps EXTRAHOP

20Gbps VECTRA

SECURITY AT SCALE

Keeping up with the scale of the enterprise is a challenge for most network security products. A single Reveal(x) appliance analyzes a sustained 100 Gbps of traffic in real time, extracting 4,800+ points of metadata about observed communications. With just 20 Gbps of analysis per appliance, Vectra Cognito requires five times the hardware to reach the same scale, adding complexity and cost.

Reveal(x) provides 500% more throughput in a single appliance than Vectra Cognito.

EXTRAHOP VECTRA

DEPTH & BREADTH OF DATA

If you can only access surface-level insight, you can only provide surface-level security. Reveal(x) performs full-stream reassembly and protocol analysis for complete, contextual visibility into all transaction payloads from Layer 2 to Layer 7 for more than 50 enterprise protocols. Continuous full packet capture is available as an add-on. Vectra Cognito misses key protocols such as MS-SQL, MySQL, Postgres, and TDS for databases, and offers minimal packet capture and storage.

Vectra Cognito will tell you that two systems spoke. Reveal(x) tells you what they said.

EXTRAHOP VECTRA

INVESTIGATION AUTOMATION

Providing visibility is only the first step for an enterprise security solution. Detecting, scoring, and accurately alerting about potential threats in real time is step two. Step three is enabling a full investigation with the option of forensic reference to packets. Vectra Cognito stops short, and investigations usually require analysts to request additional data from their IT counterparts. Reveal(x) enables Tier 1 analysts to take on more of the investigative workload with automated collection and correlation of transactions and packets in real time, suggested next steps, and enhanced detection cards (including attack TTP education).

How much time can you afford to spend investigating incidents?

SEE EXTRAHOP IN ACTION

Try our fully interactive online demo to see how the ExtraHop platform applies the power of machine learning.

www.extrahop.com/demo

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

ExtraHop
520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com