Reveal(x) vs. Darktrace

IT’S THE DATA, NOT THE MATH.

SECURITY AT SCALE
Reveal(x) gathers and analyzes 100Gbps of data in real time, providing context-rich insights within 15 minutes of being plugged in. Darktrace provides 6Gbps of analysis per appliance, requiring sixteen times as much hardware to achieve the same scale, and adding management and correlation overhead.

ExtraHop provides 16 times greater throughput in a single appliance, with deeper line-rate analysis than Darktrace at any scale.

DECRIPTION CAPABILITIES
Reveal(x) is the only security analytics solution that can decrypt traffic at line rate, including current SSL/TLS versions, even with Perfect Forward Secrecy enabled. Darktrace offers no decryption capabilities, leaving the majority of traffic - including malicious activity - completely opaque.

Are you okay with zero visibility into 70% of modern attacks?

DEPTH & BREADTH OF DATA
Reveal(x) uses wire data to give you complete, contextual visibility into all assets and payloads from L2 to L7, including 40 enterprise protocols. Darktrace analyzes packet headers, which means they mostly see from L2 to L4 with limited contextual insight.

Darktrace will tell you two systems spoke. Reveal(x) will tell you what they said.

INVESTIGATION AUTOMATION
Detection is step one for any modern security solution. Step two is confirming the validity of a potential threat to eliminate false positives before sending an alert. Providing relevant forensic data for real-time investigation and remediation should be the ultimate goal, but Darktrace stops at detection. Reveal(x) detects threats, automates the collection and correlation of transactions and packets in real time, and integrates with SIEM to provide an optimized, efficient workflow.

SecOps needs more efficiency, not more alerts.
TIMELINE OF A BREACH

ExtraHop Reveal(x) goes beyond detection to provide deep visibility and automated investigation at every step of an attack, so you can quarantine malicious devices before damage is done, and get conclusive forensic evidence in just clicks.

Experience the Power of ExtraHop Reveal(x)

EXTRAHOP.COM/DEMO

"We don’t have better algorithms than anyone else; we just have more data."

PETER NORVIG, DIRECTOR OF ENGINEERING, GOOGLE