ExtraHop

Reveal(x) vs. Darktrace

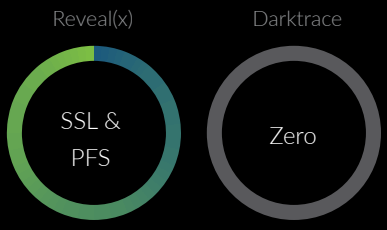
IT'S THE DATA, NOT THE MATH.

THROUGHPUT

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.

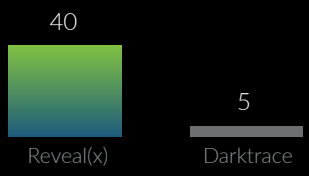


DECRYPTION

DECRYPTION 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?



L7 PROTOCOL DECODERS

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.

WORKFLOW

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.

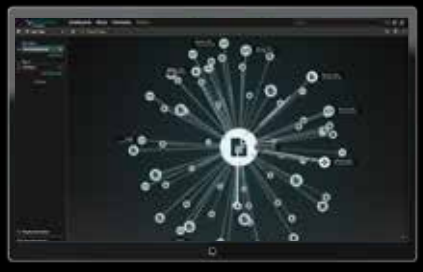
TIMELINE OF A BREACH

REVEAL(X) SEES EVERY DETAIL OF AN ATTACK. NO DARKSPACE.

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.

Reveal(x)		Darktrace
CLIENT ATTEMPTS AND FAILS DB LOGIN SEVERAL TIMES		Unusual amount of SQL traffic between a DB and rare client
CLIENT SUCCESSFULLY LOGS INTO DB		
CLIENT REQUESTS INFO FROM DB USING "SELECT" COMMAND		
DB RESPONDS IN THE AFFIRMATIVE & BEGINS DELIVERING DATA		ZERO NETWORK VISIBILITY
CLIENT ISSUES "DROP" COMMAND AGAINST DB AUDIT TABLE		
DB RESPONDS IN THE AFFIRMATIVE		
CLIENT INITIATES LARGE DATA TRANSFER TO EXTERNAL HOST		Unusual volume of data transfer between client and rare external host

> "We don't have better algorithms than anyone else; we just have more data."
>
> **PETER NORVIG**, DIRECTOR OF ENGINEERING, GOOGLE



Experience the Power of ExtraHop Reveal(x)

EXTRAHOP.COM/DEMO

ExtraHop

520 Pike Street, Suite 1700
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com