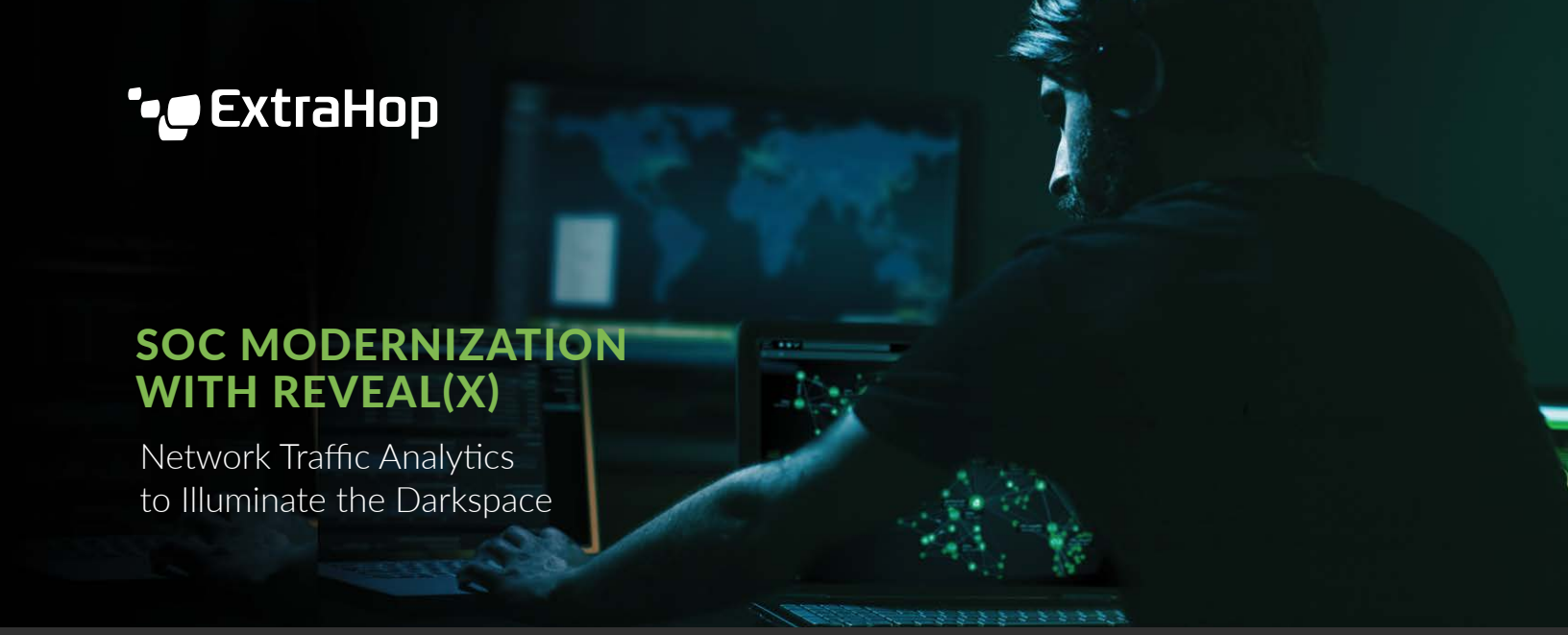
ExtraHop



SOC MODERNIZATION WITH REVEAL(X)

Network Traffic Analytics to Illuminate the Darkspace

- EVOLVE FROM REACTIVE TO PROACTIVE
- CONSOLIDATE YOUR TOOLSET
- AUTOMATE INVESTIGATION WORKFLOWS
- ORCHESTRATE RAPID THREAT RESPONSES

THE PATH OF THE MATURING SOC

Security teams often start out by trying to detect hackers and malware at the perimeter of their network, and prevent them from entering. As the business and the security practice evolves, they need to move toward real-time monitoring, detection, and proactive threat hunting inside the network.

Reveal(x) auto-discovers and classifies every device on the network, then analyzes every transaction, decoding over 50 enterprise protocols and decrypting SSL/TLS traffic, even with PFS enabled, at up to 100Gbps to provide unprecedented visibility, definitive insights, and immediate answers for SecOps teams.

TOOL BLOAT & DATA SILOS

Most SecOps teams have a suite of tools at their disposal for detecting, investigating, and responding to attacks against their assets. With the rapid increase in threat sophistication, and the proliferation of security vendors, many SecOps teams have found themselves with a fragmented toolset, limited or siloed data, and legacy platforms causing more problems than they solve. This a primary cause of several problems affecting nearly every SecOps team today:

ALERT FATIGUE & ANALYST BURNOUT

99+ DAY DWELL TIME OF THREATS IN THE NETWORK

0% JOB SATISFACTION IN CYBERSECURITY ROLES

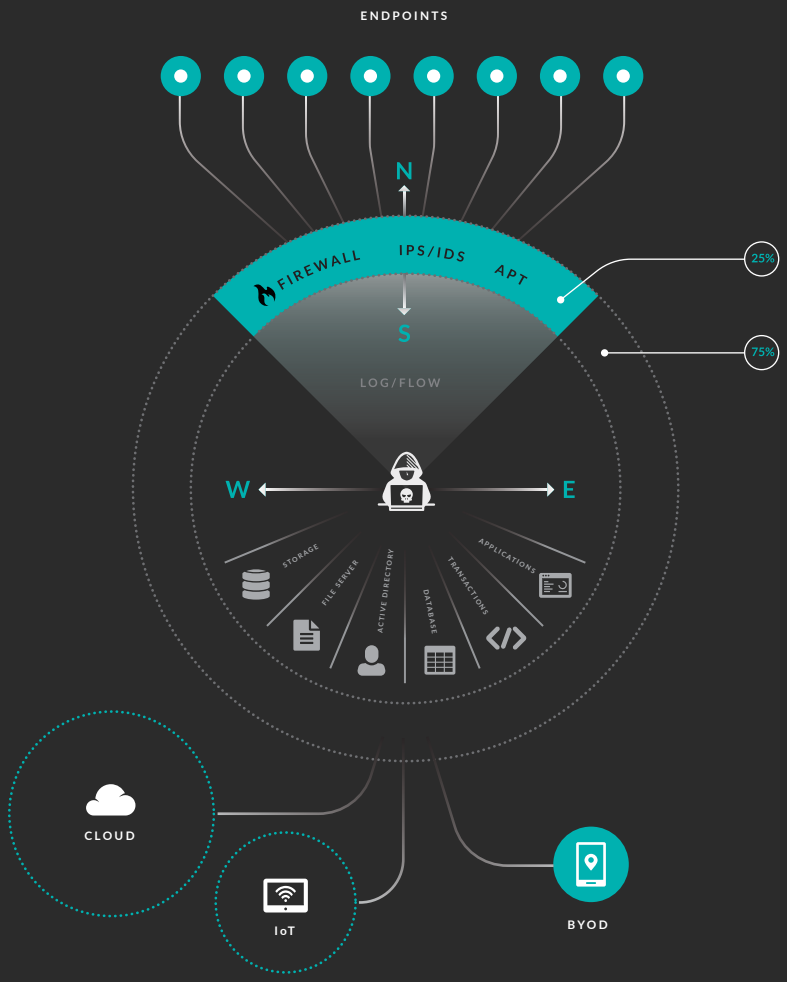
HOW REVEAL(X) ENABLES THE MATURING SOC

Reveal(x) takes the SOC from reactive to proactive by providing unprecedented visibility inside the network. Reveal(x) uses accurate, real-time, high-fidelity data and ML-driven behavioral analytics to automate investigation processes and empower Tier-1 analysts to operate at the level of Tier-3 experts.

COVERING YOUR ASSETS

A maturing SOC also needs some way to collect and analyze logs, a role usually fulfilled by a SIEM platform. They also need IDS/IPS to protect the perimeter from simpler threats, and endpoint monitoring to protect endpoints.

With Reveal(x) and a carefully selected set of best-of-breed tools, the maturing SOC can cover every necessary capability with just a few tools and data sources, eliminating the tool bloat, legacy platforms, and blind spots that plague so many teams today.



> “Our operations have really evolved since we started to use ExtraHop. Previously, we were very reactive... the use of ExtraHop allows us to move forward and proactively plan improvements.

ESTHER GO,
PRESIDENT & CEO
MEDILINK NETWORK

ABOUT EXTRAHOP NETWORKS

ExtraHop makes data-driven IT a reality. By applying real-time analytics and machine learning to all digital interactions, ExtraHop delivers instant and unbiased insights. IT leaders turn to ExtraHop first to help them make faster, better-informed decisions that improve performance, security, and digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google.

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