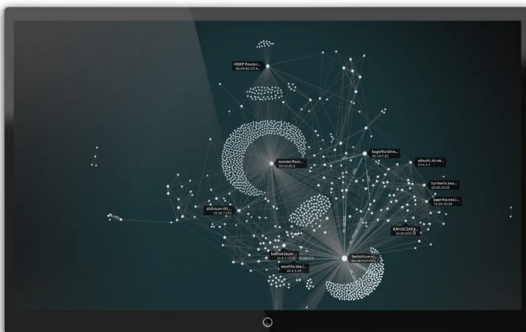# ExtraHop

SECURITY

# Detect Everything. Automate Investigations. Reduce Dwell Time. Evolve Security Talent.

At ExtraHop, we've created a fundamentally new way to analyze every digital transaction occurring on the network, turning that insight into actionable intelligence for security teams. We call this wire data, which is the definitive source for real-time analytics.

UNSTRUCTURED PACKETS → REAL-TIME STREAM PROCESSOR → STRUCTURED WIRE DATA → MACHINE LEARNING → ACTIONABLE INSIGHT

UNMATCHED ENTERPRISE VISIBILITY

ExtraHop gives Security teams comprehensive visibility into communications across on-premises, public cloud and hybrid environments, even those that are encrypted.

‣ Auto-discovery and classification of corporate assets for a complete view of all connected devices

‣ Depth and Breadth of full payload analysis for over 50 enterprise protocols

‣ Cross-tier visibility with application fluency for context and dependency mapping
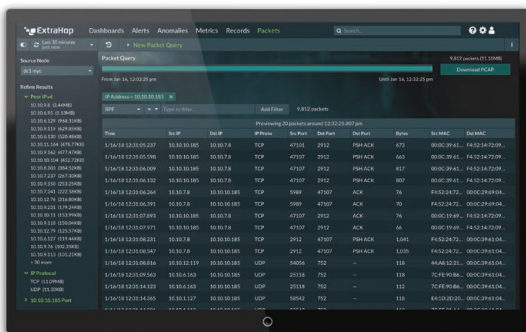
ADVANCED BEHAVIORAL ANALYTICS

With ExtraHop's real-time analytics and wire data-driven anomaly detection, you can spot abnormal behavioral patterns as they occur anywhere across your enterprise.

‣ Advanced threat detection with east-west network traffic analysis

‣ Ready-to-go solutions for ransomware, authentication, and more

‣ Integration with Splunk, Phantom, Palo Alto, ServiceNow and others
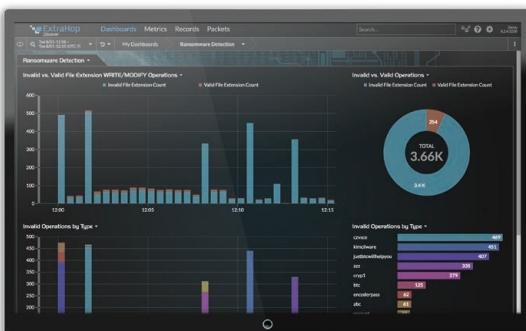
AUTOMATED INVESTIGATION

ExtraHop's analytics-first workflow takes you from issue to associated packet in a matter of clicks, saving hours of troubleshooting time and enabling real-time insights and rapid threat

‣ Always-on machine learning automatically surfaces anomalies the moment they hit the wire

‣ Open and extensible platform so you can automate workflows

‣ Seamless drill-down from detected event to details needed

SECURITY ANALYTICS
‣ East-West Traffic Analysis
‣ Ransomware Detection
‣ Automated Threat Hunting
‣ Custom metrics for real-time adaptation

COMPLIANCE
‣ PII and clear text transmission
‣ Encryption and Cipher Strength
‣ Enabling GDPR Compliance
‣ Continuous Packet Capture

INTEGRATIONS
‣ SIEMs and NGFWs
‣ Automation/Orchestration with Phantom, Ansible, Cisco Tetration, Moogsoft
‣ Incident response with ServiceNow or Slack.

CLOUD
‣ Hybrid Security Monitoring
‣ Public and Private cloud usage
‣ AWS API integration

REAL-TIME SECURITY ANALYTICS

ExtraHop gives Security teams comprehensive visibility across all transactions occurring in their hybrid environment, in context. This turns the network into the most comprehensive and high-fidelity data source available, all in real-time.

MACHINE LEARNING

ExtraHop unsupervised machine learning powered by wire data surfaces precise anomalies and threats in your environment before they impact your business. Always on and learning, our machine learning service evolves as threats emerge and new variants are released.

AUTO DISCOVERY & CLASSIFICATION

ExtraHop discovers and classifies all endpoints communicating in your environment. Eliminate the opaque network by identifying rogue nodes, IoT devices, and BYOD systems the moment they communicate on the network. The opaque network is a segment in every environment that agents and logs simply can't address.

DECRYPTION

ExtraHop decrypts SSL and PFS traffic enhancing visibility and context across the enterprise while maintaining your security posture.

SMART FORENSICS

ExtraHop Global Search and Indexing provides immediate access to security insights, including live metrics, transaction records, and packets for forensic lookback. Investigate anomalies with automated workflows and live activity maps that take you from issue to root cause in two clicks.
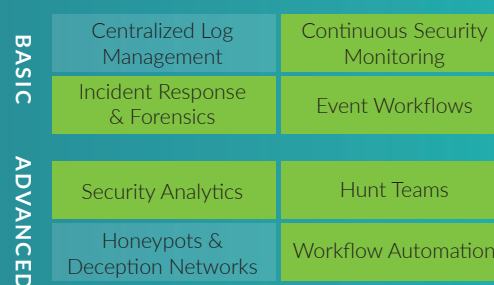
INTEGRATION & AUTOMATION

ExtraHop integrates with your existing security infrastructure, streaming wire data to your SIEM for correlation and automated incident response to streamline your security workflows.

DATA SOURCES

AGENTS	Difficult to deploy and scale Introduces new attack vectors	
LOGS	Self-reported, past activity Costly data tax	
WIRE DATA	Instant, Emperical & Definitive Complete Context	

NEXT-GEN SOC

BASIC	Centralized Log Management	Continuous Security Monitoring
	Incident Response & Forensics	Event Workflows
ADVANCED	Security Analytics	Hunt Teams
	Honeypots & Deception Networks	Workflow Automation

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.

ExtraHop

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