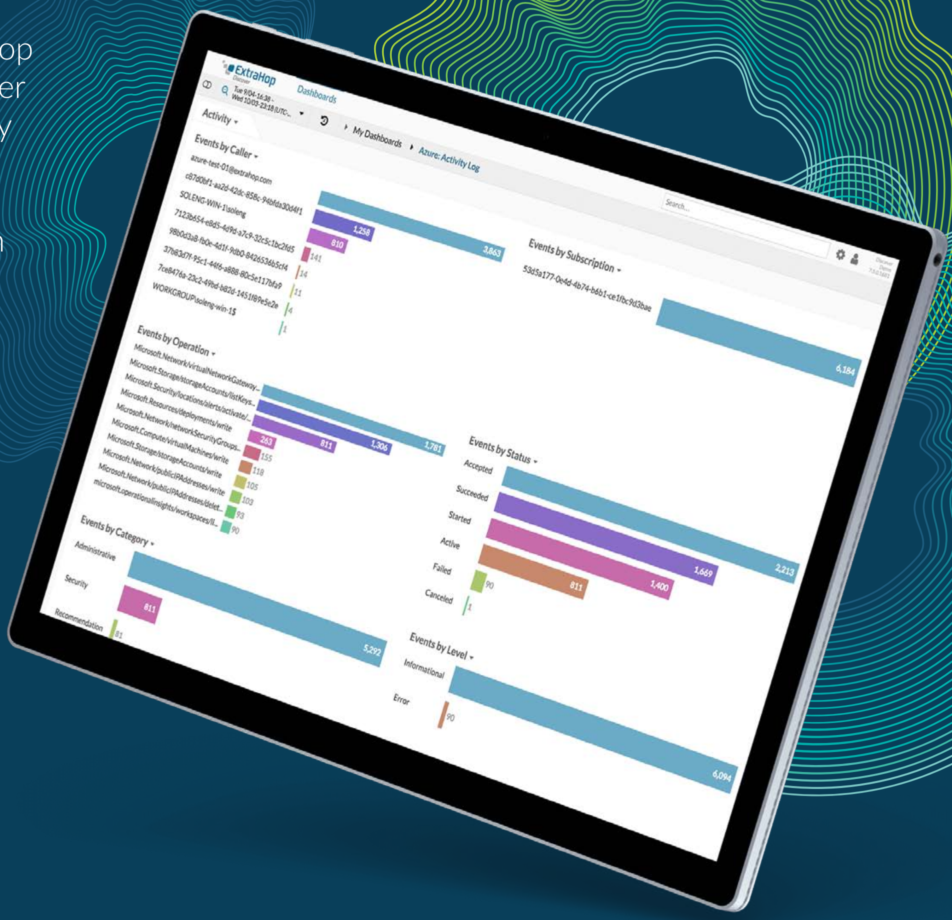
ExtraHop Cloud Platform

In the cloud, clarity is key. The ExtraHop Cloud Platform illuminates every corner of your hybrid environment, backed by advanced machine learning and a simplified workflow for incident investigation and response so you can embrace the cloud with confidence.


ExtraHop
Discover
Tue 9/04-16:38 - Wed 10/03-23:18 (UTC...
Dashboards
Activity
My Dashboards
Azure: Activity Log
Search...
Events by Caller
azure-test-01@extrahop.com
c87d0bf1-aa2d-42dc-858c-94bfda30d4f1
SOLENG-WIN-1\soleng
7123b654-e8d5-4d9d-a7c9-32c5c1bc2fd5
98b0d3a8-fb0e-4d1f-9db0-8426536b5cf4
37b83d7f-95c1-44f6-a888-80c5e117bfa9
7ce8476a-23c2-49bd-b82d-1451f89e5e2e
WORKGROUP\soleng-win-1$
3,863
1,258
810
141
14
11
4
1
Events by Subscription
53d5a177-0e4d-4b74-b6b1-ce1fbc9d3bae
6,184
Events by Operation
Microsoft.Network/virtualNetworkGateway...
Microsoft.Storage/storageAccounts/listKeys...
Microsoft.Security/locations/alerts/activate/...
Microsoft.Resources/deployments/write
Microsoft.Network/networkSecurityGroups...
Microsoft.Compute/virtualMachines/write
Microsoft.Storage/storageAccounts/write
Microsoft.Network/publicIPAddresses/write
Microsoft.Network/publicIPAddresses/delet...
microsoft.operationalinsights/workspaces/li...
1,781
1,306
811
263
155
118
105
103
93
90
Events by Status
Accepted
Succeeded
Started
Active
Failed
Canceled
2,213
1,669
1,400
811
90
1
Events by Category
Administrative
Security
Recommendation
5,292
811
81
Events by Level
Informational
Error
6,094
90

COMPLETE VISIBILITY

ExtraHop pulls in data from anywhere the enterprise network exists to transform unstructured network packets into the only observed source of information about the security and performance of your hybrid enterprise. With the introduction of the first vTAPs for cloud from Azure and AWS, ExtraHop makes it easy to gather virtual packets from every cloud instance.

REAL-TIME DETECTION

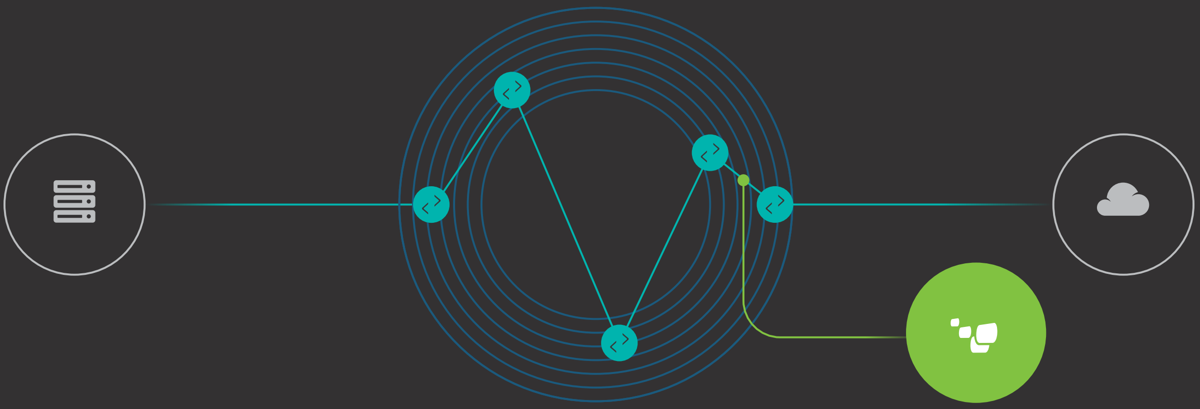
A completely passive solution that turns raw packets into metadata, the ExtraHop Cloud Platform makes everything searchable. Combining automated discovery and asset classification with full payload analysis and machine learning for high-fidelity threat detection, The ExtraHop Cloud Platform gives cloud-focused SecOps teams the power to proactively monitor and respond to threats.

GUIDED INVESTIGATION

The ExtraHop Cloud Platform is the only solution that converts all wire data to a fully indexed record of every element of every transaction. It's an exponential gain in empirical data that has never before been available. We deliver the largest and richest set of factual and contextualized data to answer the most important questions coming from the Security and Operational teams.

RISE ABOVE CLOUDY INSIGHTS.

Complete Visibility into Virtual Environments



ExtraHop Reveal(x) + the Azure V-Tap

ExtraHop Reveal(x) for Azure integrates with the Microsoft Virtual Network TAP to provide the first complete network traffic analysis (NTA) solution in the Azure cloud. ExtraHop Reveal(x), Network Traffic Analysis for the enterprise, natively integrates with Microsoft Azure via the Azure Virtual Network TAP to provide unified security analytics in the cloud. By combining automated discovery and asset classification with full payload analysis and machine learning for high-fidelity threat detection, Reveal(x) for Azure gives cloud-focused SecOps teams the power to proactively monitor and respond to threats. ExtraHop also partners with Amazon Web Services for powerful security analytics and investigation automation.

BUILT FOR SHARED RESPONSIBILITY

For enterprises, a critical first step in the cloud is knowing what, exactly, you are responsible for. Based on the Shared Responsibility model, security of data and applications, along with organizational/regulatory compliance, rests on IT/cloud and security architects within the enterprise.

APPLICATIONS & CONTENT

Insecure APIs	Enumeration attacks	Unknown Threats

NETWORK SECURITY

- Accountability for who accesses your systems remotely
- Accountability for the types of communications (ports and protocols) to ensure that they match as-built expectations

INVENTORY & CONFIG

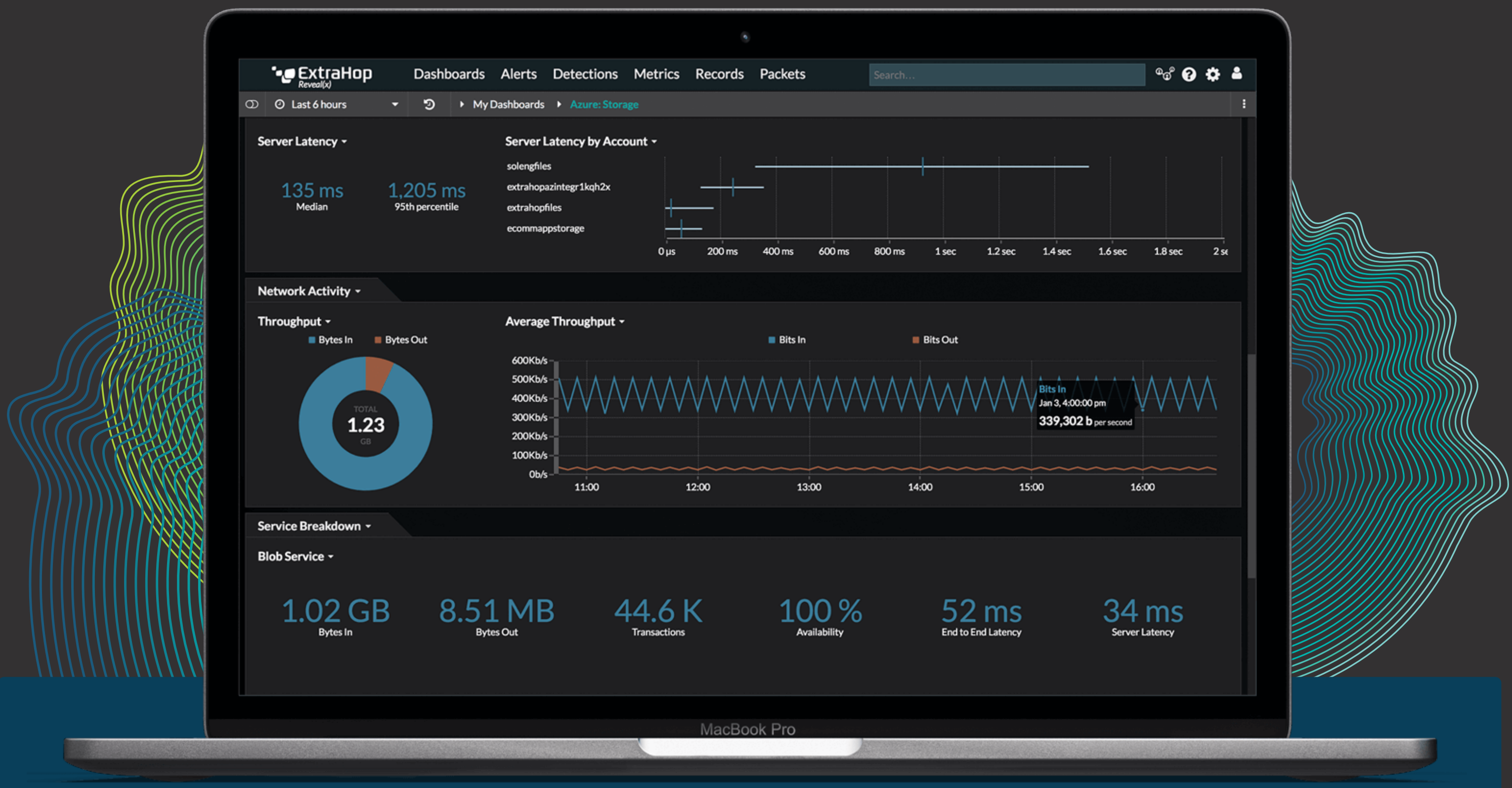
- Access misconfiguration
- Privilege escalation
- Rogue instances

DATA SECURITY

- Transaction-level visibility
  - Non-standard user-agents
  - Malformed DB queries
  - L7 exfiltration

ACCESS CONTROL

- Insider threats
- Incomplete segmentation
- Privilege escalation



EXTRAHOP CLOUD PLATFORM FEATURES

Automated Inventory

Always know exactly what's in use across your hybrid environment, with automatic grouping of critical assets.

Unified Enterprise Visibility

See all devices, signal metrics, and behavioral analytics in a single, intuitive interface.

Real-Time Anomaly Detection

Detect cloud-specific threats and performance issues with machine learning guided on 4,700+ wire data metrics.

Confident Migrations

Monitor cloud deployments before, during, and after migration with transaction-level detail.

Simplified Investigation

Click from high-level insights to forensic evidence in seconds, with auto-correlation of threats across the attack chain.

Rapid Incident Response

Integrate with orchestration platforms like ServiceNow and Phantom for immediate, automated response workflows.

FEATURED INTEGRATIONS

Azure aws servicenow Phantom

OUR CUSTOMERS RISE ABOVE THE NOISE.

IDC

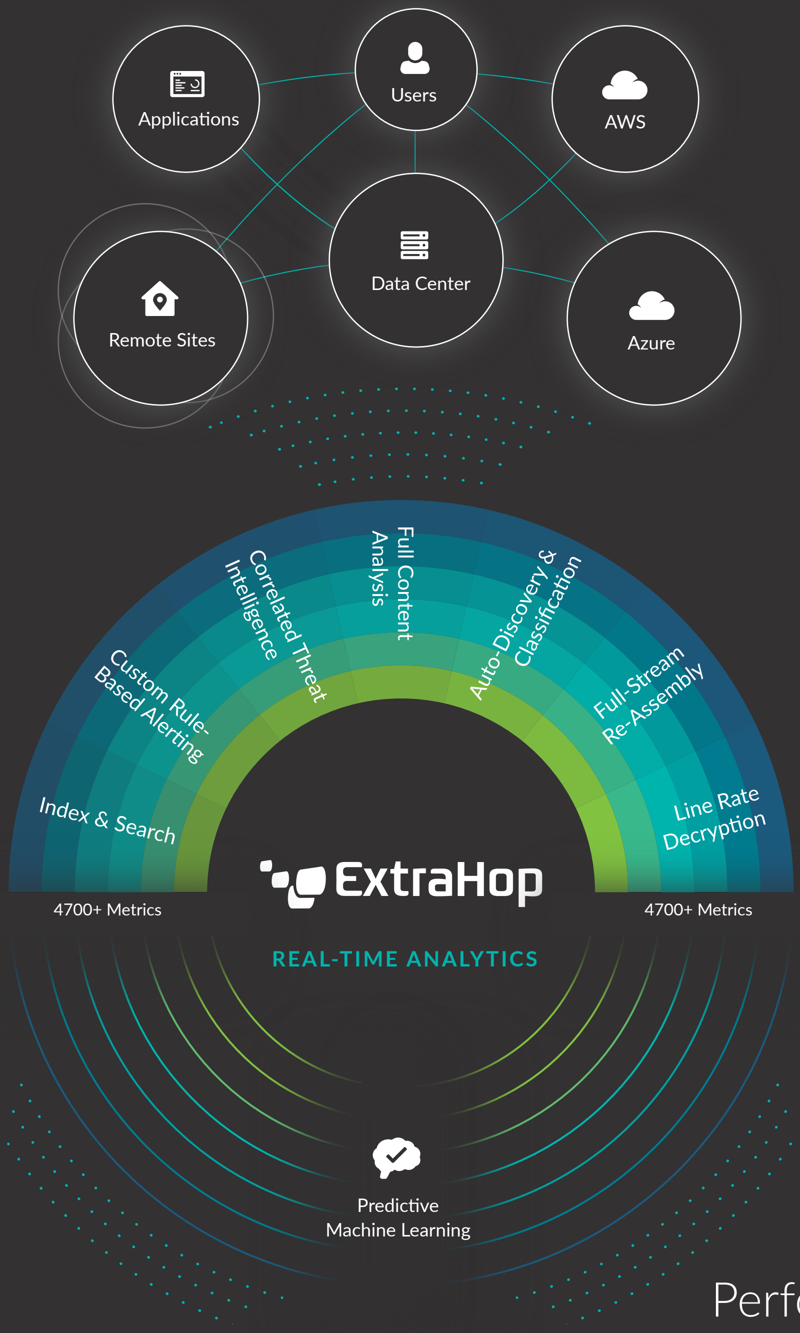
95%
REDUCTION IN AVERAGE TIME TO DETECT THREATS

59%
REDUCTION IN STAFF TIME TO RESOLVE SECURITY THREATS

78%
LESS TIME SPENT TROUBLE-SHOOTING

85%
REDUCTION IN TIME NEEDED TO REPAIR APPLICATION DEGRADATION

RAW NETWORK TRAFFIC



Applications

Users

AWS

Data Center

Remote Sites

Azure

Index & Search

Custom Rule-Based Alerting

Correlated Threat Intelligence

Full Content Analysis

Auto-Discovery & Classification

Full-Stream Re-Assembly

Line Rate Decryption

4700+ Metrics

ExtraHop

4700+ Metrics

REAL-TIME ANALYTICS

Predictive
Machine Learning

Security

High-fidelity threat detection

Hygiene and compliance

Critical asset discovery

1-click threat investigation

Automated response via SOAR

BUSINESS RESULTS

Performance

Real-time application analytics

ML-driven anomaly detection

Application dependency mapping

End-to-end visibility and hygiene

Guided investigation

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