ExtraHop + Keysight Technologies

Promoting Alignment Between NetOps and SecOps

JOINT SOLUTION HIGHLIGHTS

- Complete, realtime visibility for performance and security monitoring
- Streamline sharing of data by NetOps and SecOps
- Reduce costs by leveraging tools across teams
- Rise above the network noise

Features and Benefits

COMPLETE VISIBILITY
- Edge to core to cloud
- Real-time access to relevant data
- SSL decryption
- Complete context

REAL-TIME DETECTION
- Scalable cloud-based ML
- Transaction-level detail
- Fewer false positives

GUIDED INVESTIGATION
- Automated investigation and response
- Continuous packet capture
- Integrated workflow
- Integration with Splunk, Palo Alto, ServiceNow, etc.

Things used to be simple. Information technology (IT) and network operations focused on performance and availability while Security Operations (SecOps) worked to secure the business. Each played a vital role in keeping end-users happy while basically staying in their own swim lanes.

But more and more, your NetOps and SecOps teams must interact and collaborate to achieve desired business outcomes. For example, it may not be clear at first whether a user issue is truly a performance problem or the result of a security breach. A recent survey by Enterprise Management Associates (EMA) found that security-related issues such as infected hosts or distributed denial of service (DDoS) attacks play a role in nearly 40 percent of complex IT service issues and outages.

In drilling down to troubleshoot, the same data might be used by IT to source congestion or latency and by security teams to hunt for exploits. Both efforts are fundamentally data-driven and both teams increasingly need deeper understanding of the network from the inside out.

ExtraHop and Ixia have teamed to deliver complete visibility solutions that promote better alignment and return on investments (ROI) in performance and security.

The Growing Need for Alignment

Several technology trends are making it more important and difficult than ever for NetOps and SecOps teams to work together. Increased complexity, the explosive growth of cloud migration and "Everything-as-a-Service" are all prompting IT to modernize operations and further digitize transactions. For example, virtualized servers and containerized apps explode the number and diversity of connecting endpoints making it harder to control underlying networks and maintain perimeter security.

These trends give rise to new management issues that impact both sides. For example, a failure or successful attack upon a centralized controller in a software defined data center (SDDC) can now bring down entire data centers and bring both efforts to a halt. To make matters worse, it is increasingly difficult for NetOps and SecOps teams to access the network traffic required as the single source of truth as network speeds continue to soar toward 100/400Gbs and encrypted traffic volumes rise exponentially. Troubleshooting, threat detection and future-proofing all require real-time monitoring and historical data leaving NetOps and SecOps asking different questions while looking at the same surface area within an organizations network:

Data	NetOps	SecOps
Users	How good is the user experience?	How are people logging in and are their credentials compromised?
Applications	How well are applications performing?	What is the dause of unusual activity?
Web	Which servers are responding slowly?	Does encrypted internet traffic contain malware?
Storage	How much capacity do we need?	Are we seeing unusual access to sensitive fields?
Monitoring	Troubleshooting	Incident Response

Hybrid environments, tool sprawl, competing priorities, knowledge silos, and skillset deficiencies all contribute to noise that in turn leads to chaos that gets in way of sharing knowledge. Uptime and security become competing efforts with each team focused on narrower, more immediate mandates instead of pooling valuable expertise and resources.

Lack of alignment also causes tremendous waste—duplicated instrumentation and training, redundant procurement, increased overhead on the network — causing precious time and money to be lost. Last but not least, operating in silos results in missed opportunities to share information that can benefit cross-functional teams.

So how do we shift toward better alignment? By making things easier.

ExtraHop + Ixia: Seamless Visibility for Rising Above the Noise

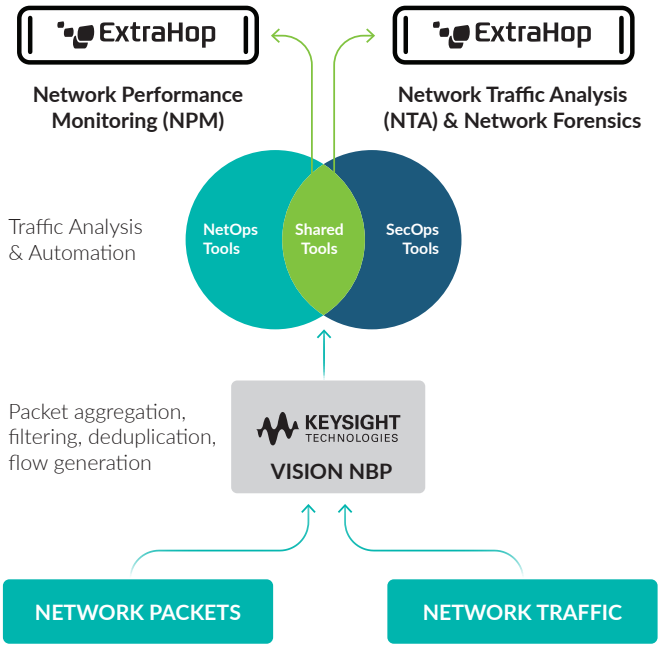
Along with intent, collaboration hinges on two things: Real data and rich context. Though they operate in silos, both teams need access to the same monitoring data from the network to do their jobs. This can be viewed as a visibility challenge that can be overcome with better, faster sharing of information through:

- Real-time access to deep, packet-level insight from networks and cloud environments
- Pre-processing of traffic that makes it easier to share and streamline data
- Monitoring and visibility tools that can be easily shared across multiple teams
- Working together at the beginning, not just the end

How it Works

Fast, reliable access to data can be achieved using Ixia's physical and virtual "taps" to extract and forward packets to intelligent network packet brokers (NPBs). Ixia's Vision NPBs handle the pre-processing of data by aggregating, deduplicating, filtering, and grooming traffic for use by performance and security monitoring tools such as ExtraHop's analytics solutions.

BRIDGING THE GAP WITH VISIBILITY INTELLIGENCE



ExtraHop has created a way to explore every digital interaction taking place on the network using real-time analytics and machine learning (ML) to transform data into an objective source of truth. The ExtraHop Performance Platform and Reveal(x) security solutions take in data provided by Ixia's visibility architecture and perform line-rate decryption, decoding, and full-stream reassembly for every transaction in real time. This results in complete coverage from the core to the edge to the cloud, and better intelligence for investigation.

Structured wire data from ExtraHop allows both NetOps and SecOps professionals to analyze, explore and fully leverage insight for response and remediation. It is even possible to search and query transactions at scale to see what happened and why in a matter of clicks.

Better alignment — and results — require complete visibility, real-time detections, and guided investigations. ExtraHop and Ixia combine to provide NetOps and SecOps teams real-time access to exactly the data they need in a format that makes their job easier, whether that means threat detection or troubleshooting slow videoconferencing in the conference room.

A Lasting Advantage Through Better Processes

Cooperation must be embraced by experts themselves through a combination of:

- Breaking down silos
- Formalizing collaborative processes
- Automating interaction
- Tool consolidation

Start by identifying common handoff and escalation points. For example, NetOps and SecOps should both be aware and prepared before making significant changes to the network. As issues get resolved, documentation equips both sides to hone and update processes. Create SLAs that ensure teams pass along details in formats used by other teams.

Cross-training on tools is another excellent way of breaking down barriers, and actually sharing them will save significant time and money (many companies spend double or triple what they need to on tools). Cross-training promotes faster communication and better understanding of problems by letting both teams leverage a shared dashboard for shared understanding.

Where possible, automate. Make things simpler with integrated, streamlined GUIs and informative dashboards.

Keep It Simple

Collaboration can best be approached as an evolution versus a revolution. Start simple and keep expanding. Whenever possible, involve both teams in procurement processes, new architecture designs, and application rollouts. Demonstrate value while recognizing each team must operate independently at times.

Above all, stick with it. Better cross-functional alignment may seem like a valuable "nice to have" now, but it will soon prove essential to running your business effectively. To learn more, watch the webinar and or contact ExtraHop or Ixia to arrange a demonstration.

LEARN MORE

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