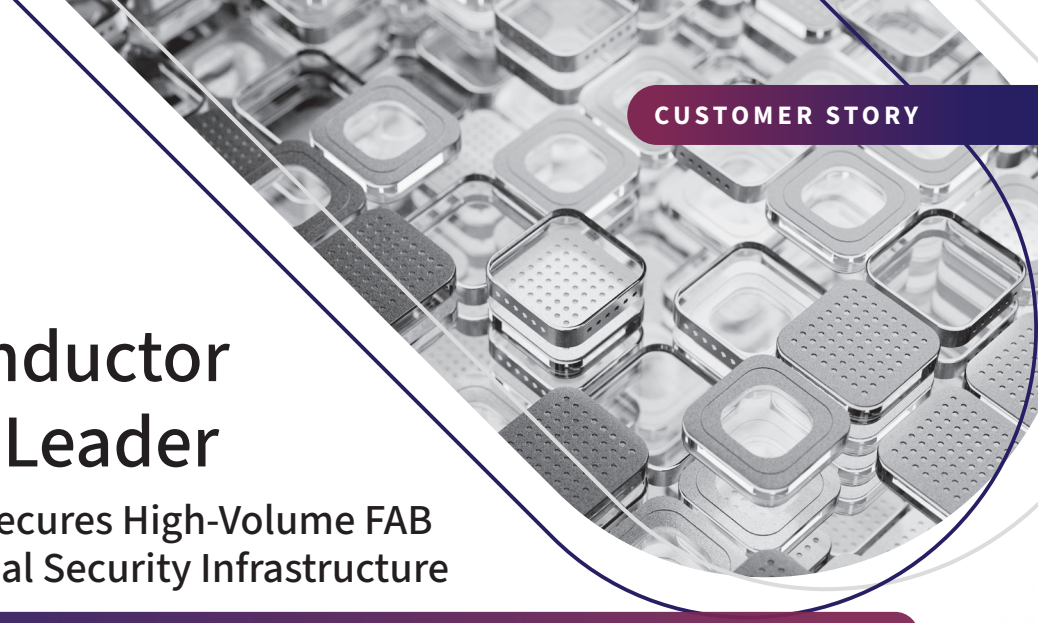
EXTRAHOP

CUSTOMER STORY



Global Semiconductor Manufacturing Leader

Semiconductor Foundry Secures High-Volume FAB Sites and Modernizes Global Security Infrastructure

A global semiconductor leader managing complex manufacturing traffic faced visibility gaps that threatened its critical intellectual property. Relying on legacy tools, the organization suffered from limited insight into sensitive data movements. To modernize its security posture, the foundry deployed ExtraHop RevealX NDR. By providing real-time network intelligence and automated analysis, RevealX replaced inefficient legacy solutions. This transition enabled security teams to manage massive traffic volumes and close critical detection gaps, helping to ensure the continuous protection of the advanced chip manufacturing operations.

The company selected the ExtraHop RevealX platform after an extensive proof of concept (POC) involving a red team demonstration, achieving the following strategic outcomes:

- **Platform replacement and visibility:** The company displaced legacy solutions to gain unmatched network visibility and 100 Gbps performance across global manufacturing sites.
- **Protocol and IP protection:** The deployment eliminates weak protocols while using IOC intelligence to prevent unauthorized intellectual property exfiltration.
- **Strategic ecosystem integration:** The platform leverages a critical CrowdStrike relationship for a unified defensive posture, feeding high-value data to existing security investments.
- **Modernized database and asset tracing:** ExtraHop provides deep database access tracing and detailed records without physical hardware, delivering transformative efficiency to the security team.

The Challenge: Safeguarding Intellectual Property Across Global FAB Operations

As a global leader in semiconductor manufacturing operating high-volume FAB sites, this company manages an incredibly complex technical landscape, where protecting intellectual property is a matter of national and economic security. However, the existing architecture presented several core challenges:

Inadequate Legacy Visibility

The company struggled with legacy tools that failed to handle complex traffic. These systems left the team blind to sophisticated threats in specialized manufacturing environments where intellectual property is most vulnerable.

Skeptical Detection Requirements

Previous experiences led the team to doubt network-based machine learning. They required a solution that proved its strength against real-world attack scenarios and rigorous red team testing before committing to a global rollout.

Protocol and Compliance Risks

The company maintained weak protocols serving as potential exfiltration paths. The team established a mandate to eliminate these worldwide to meet compliance goals and harden the network against IP theft.

Hardware and Scaling Constraints

Global business required NDR that scales across geographic locations. The team prioritized a deployment providing detailed forensics and records without the burden of managing extensive on-premise hardware.

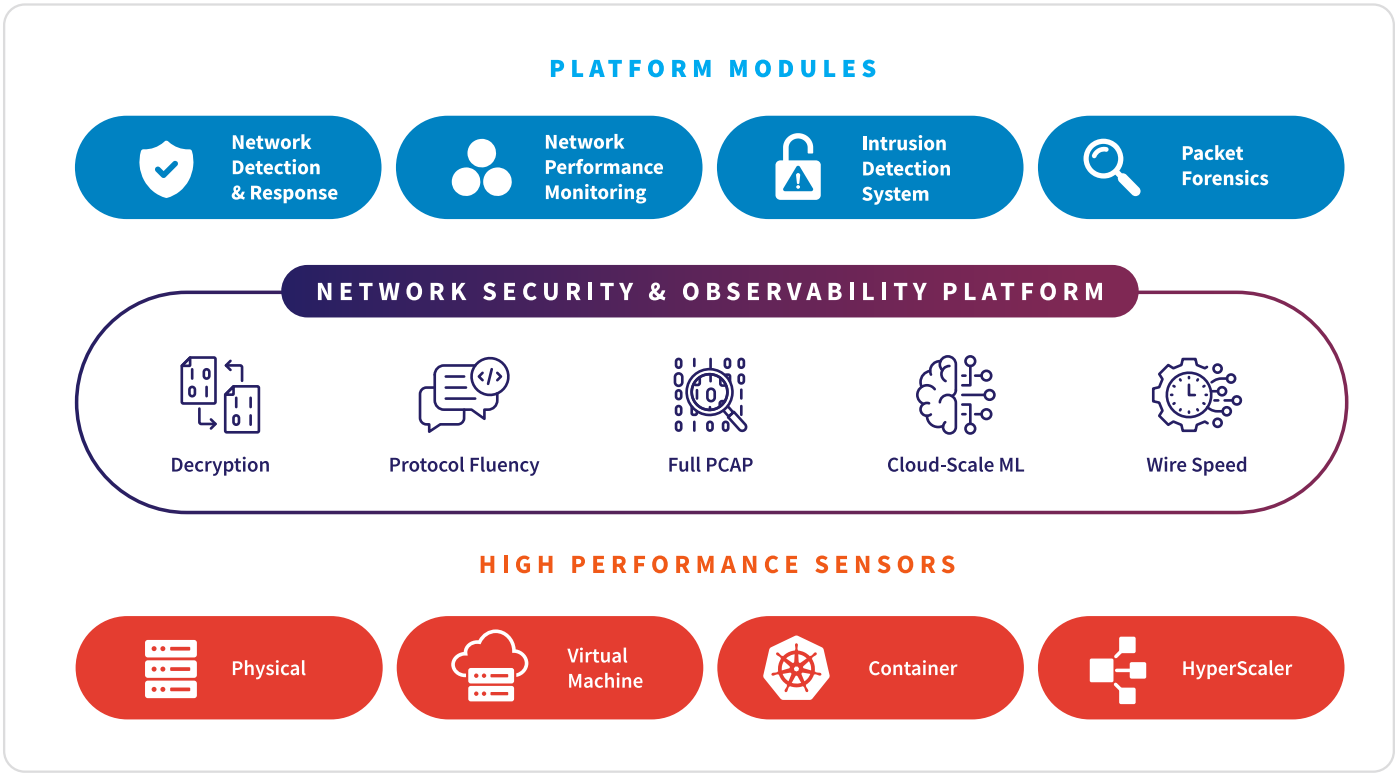
The Solution: Unified Detection with ExtraHop NDR

The successful POC proved that ExtraHop could handle the high-stakes requirements of a global semiconductor manufacturing leader. The modern NDR platform enabled the security team to transition from reactive monitoring to a proactive defense of their core manufacturing blueprints across their high-speed network.

The key outcomes and advantages delivered to the company include:

- **Unrestricted visibility and decryption:** The semiconductor manufacturing leader secured the required forensic depth and network control when it deployed ExtraHop, which analyzes 100 Gbps of east-west traffic and uses high-speed decryption to immediately find threats previously hidden within encrypted flows.
- **Reduced alert fatigue via high-fidelity detection:** The cloud-scale machine learning built into the ExtraHop platform reduced the SOC's operational burden by providing high-fidelity, low-noise detections. This shift allowed analysts to move their focus from low-value false positives to highly reliable network activity, signaling true post-compromise threats and endpoint detection and response (EDR) evasion tactics.
- **Actionable context and identity:** The security team achieved comprehensive insight by using identity-based investigation, which links malicious network activity directly to user and service accounts, finally enabling the detection of all missed AD and lateral movement attacks.
- **Streamlined incident response via ecosystem integration:** ExtraHop fundamentally simplified incident response workflows because it established itself as the definitive source of network truth, automatically feeding high-value contextual data to the customer's existing SIEM and EDR platforms.
- **Unified security platform:** The company gained efficiency and reduced complexity by consolidating NDR, NPM, and IDS capabilities into one unified, integrated solution for comprehensive network security and observability.
- **Deep protocol coverage for core assets:** The semiconductor manufacturing leader mitigated major risk by gaining deep fluency (parsing over 90 protocols) that allowed for accurate decoding of all traffic, including sensitive database communications, without introducing performance risk. This was critical for detecting hidden AD attacks and lateral movement.

ExtraHop NDR Platform



The Results: Performance and Protection

The global semiconductor manufacturing leader achieved immediate, transformative security improvements and operational stability following the deployment of the ExtraHop NDR platform.

Verified Detection Strength

The platform's machine learning capabilities successfully passed a rigorous red team demonstration. This validation gave the company confidence in the platform's ability to detect sophisticated post-compromise threats targeting intellectual property that previous solutions had missed.

Accelerated Global Rollout

The company successfully implemented the platform across multiple locations worldwide, securing critical FAB sites. This rollout provided the first-ever unified view of the global manufacturing network and simplified the management of complex traffic flows.

Enhanced Threat Intelligence

By integrating file hashing with internal IOC intelligence, the security team now identifies and neutralizes threats with greater precision. This integration, combined with the CrowdStrike partnership, ensures a rapid and coordinated response to attempts at intellectual property theft.

Modernized Infrastructure and Compliance

The company is on track to eliminate all targeted weak protocols. By utilizing a solution that provides detailed records without requiring on-premise physical hardware, the company simplified its technical environment and reduced management overhead.

Optimized Intellectual Property Security

The introduction of deep database access tracing has significantly reduced the time required for forensic investigations. Analysts now possess the granular visibility needed to secure sensitive manufacturing data and proprietary chip designs against both internal and external threats.

ABOUT EXTRAHOP

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response (NDR).

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance monitoring (NPM), intrusion detection (IDS), and packet forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com