EXTRAHOP

Protecting the Silicon Lifecycle and Securing Global Innovation from Design to Fabrication

Keep Critical Semiconductor Design and Manufacturing Processes Free from Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: Securing the Architecture of Global Innovation

In 2026, the semiconductor industry represents the foundation of global technology and national security. Spanning the entire silicon lifecycle from proprietary architecture design to automated 2nm fabrication, this sector is the primary battleground for geopolitical supremacy. As manufacturing and digital design converge, leaders face four critical friction points.

- **Nation-State Sabotage and Industrial Espionage:** Geopolitically motivated actors have moved beyond data theft to the functional disruption of global supply chains. Using living-off-the-land tactics, adversaries infiltrate networks to steal process recipes or stage designs for exfiltration. Protecting these assets requires absolute internal visibility to stop lateral movement before an actor can sabotage lithography systems or compromise the engineering core.
- **The Intellectual Property and Design Pipeline Crisis:** The shift toward distributed design and electronic design automation tools has expanded the attack surface into engineering workstations and compute clusters. These environments often lack traditional endpoint coverage due to extreme performance requirements, creating a significant agent blind spot. Identifying threats to RTL designs requires a network-centric approach to spot the anomalous data transfers that signify an IP breach in progress.
- **The Visibility Gap in Automated Fabs and Clean Rooms:** Fabrication relies on thousands of unmanaged OT devices communicating via specialized protocols like SECS/GEM. These dark assets cannot host security agents, leaving the fab floor vulnerable to silent entry and production manipulation. A single unauthorized command to a robotic handler or a subtle change to a chemical delivery system can result in catastrophic yield defects or ruined wafers.
- **Strict Compliance and the 2026 Export Control Mandate:** Regulatory scrutiny has reached a peak with the 2026 implementation of U.S. export control frameworks for high-end AI processors. Manufacturers must provide verifiable, unalterable proof that sensitive technology is not accessed by restricted entities. Meeting NIST 800-171 and CMMC mandates requires a definitive source of truth that can reconstruct all network transactions and data flows to maintain government incentives.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all interactions by decrypting and decoding 90+ protocols at 100 Gbps to protect high-value chip design pipelines and automated wafer fabrication environments.

The Definitive Data Source for the AI-Enabled SOC

Provides high-fidelity wire data to power the next generation of semiconductor SOC automation and defenses. This delivers unalterable ground truth to eliminate investigative friction across complex engineering zones.

AI-Powered Cyber Threat Detection

Identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting proprietary IP and manufacturing control systems using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers every asset, from EDA tool clusters to lithography systems and robotic handlers, without installing software or impacting high-precision system performance.

Strategic Line-Rate Decryption

Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats within secure design transfers and proprietary manufacturing APIs.

High-Fidelity Performance Metrics

Troubleshoots production disruptions using 5,000+ wire data metrics for deep operational insight into network latency and automated manufacturing application performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy audit requirements for the CHIPS Act, NIST 800-171, and global export controls.

The Solution: RevealX Network Intelligence

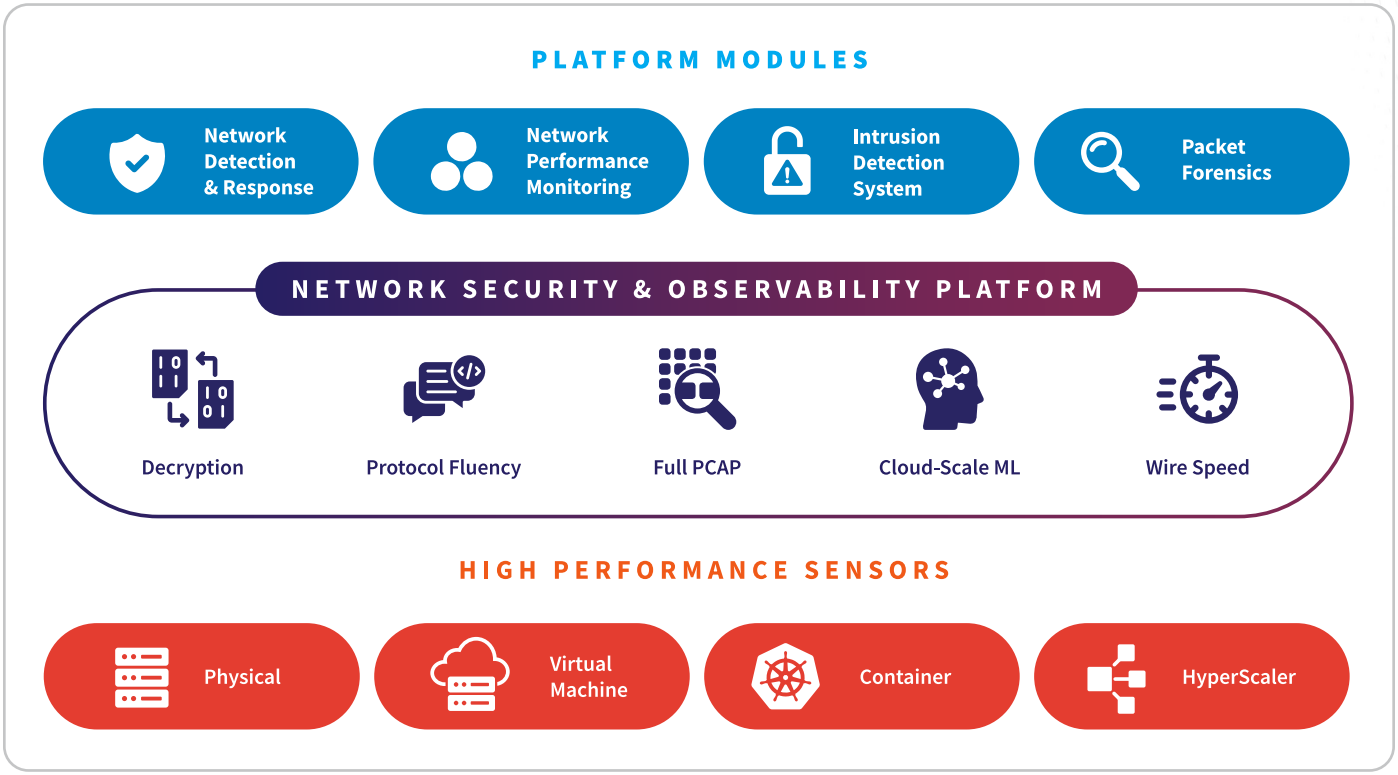
ExtraHop RevealX provides the unalterable ground truth required to secure the semiconductor lifecycle. By analyzing every packet at line rate up to 100 Gbps, RevealX eliminates the visibility gaps in both advanced design environments and automated fabrication facilities. In an industry where intellectual property is the primary asset and a single minute of fab downtime can cost tens of thousands of dollars, RevealX delivers the real-time insights needed to maintain production yield and protect brand integrity.

The platform solves the agent blind spot by providing decryption and decoding of over 90+ protocols. This agentless passive monitoring of critical assets like lithography machines, chemical delivery systems, and robotic handling units is fully visible without risking system stability or introducing performance overhead. By baselining normal behavior across these unmanaged devices and specialized SECS/GEM communications, security teams can instantly detect anomalies that indicate an adversary is attempting to manipulate a process recipe or has established a foothold on the factory floor.

To counter nation-state industrial espionage, RevealX identifies subtle shifts in network behavior that signify the staging of sensitive chip designs for exfiltration. By exposing hidden threats within encrypted traffic using strategic decryption, the platform stops attackers before they can move from corporate IT into high-security design zones hosting electronic design automation (EDA) tools. This visibility extends to the global supply chain, where RevealX monitors the integrity of connections to OSAT partners and equipment vendors to prevent supply-chain-borne attacks from reaching the core manufacturing network.

Beyond threat detection, RevealX accelerates incident response to meet the rigorous reporting requirements of the CHIPS Act and NIST 800-171. It provides a definitive forensic record of all network transactions, which eliminates the guesswork during investigations and allows for rapid root-cause analysis. This unified approach bridges the gap between the SOC and the fab operations teams by combining security detection with deep performance metrics. By monitoring the health of critical data paths, RevealX ensures that security measures do not introduce latency, protecting the precision and speed of advanced semiconductor manufacturing.

ExtraHop NDR Platform



NDR Technology Use Cases for the Semiconductor Industry

Nation-State Attacks	Detects lateral movement and staging of proprietary chip designs (GDSII files) or process recipes by persistent actors targeting advanced technology nodes.
Threat Detection & Response	Investigates hidden threats across converged design (IT) and fab (OT) environments, filling visibility gaps where agents cannot be deployed on lithography or metrology tools.
Threat Hunting	Leverages behavioral baselining to find signature-less threats targeting EDA pipelines or automated material handling systems (AMHS) before they impact wafer yield.
SOC Modernization	Unifies SOC and fab operations workflows with AI prioritization to manage high-velocity telemetry, accelerating response times for critical manufacturing infrastructure.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of SECS/GEM and HSMS protocol commands for one-click root-cause analysis of fab outages or process manipulation.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots from corporate office networks toward secure engineering zones and restricted fab control segments.
Cloud Workload Security	Provides agentless visibility for cloud-hosted design simulations and supply chain portals, discovering shadow IT and unmanaged assets across multi-cloud environments.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value engineering workstations, jump hosts, and fab management servers.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of proprietary IP or total paralysis of a multi-billion-dollar wafer fab.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including clean room sensors, chemical delivery systems, and robotic controllers that cannot support traditional agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled or missing on legacy fab hardware and specialized engineering high-performance clusters.
AI Security	Monitors generative AI and autonomous agents used for photolithography optimization and predictive yield maintenance in containerized cloud workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that micro-segmentation between production zones and third-party vendor "air-gaps" is being monitored.

NPM Technology Use Cases for the Semiconductor Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for time-critical HSMS messaging between fab hosts and equipment.
Operational Resilience	Resolves infrastructure degradation before it hits wafer continuity, ensuring availability for mission-critical manufacturing execution systems (MES) and design storage.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between fab operations (OT) and IT network teams during production "stalls."
Migrate Workloads to the Cloud	Maintains performance during EDA tool or ERP migration by auto-mapping dependencies and using network baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for fab management gateways and supply chain traceability APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past fab downtime or telemetry drops in the clean room.
Application Performance Monitoring	Fills network gaps by decrypting and decoding 90+ protocols, providing real-time insights into SECS-II transaction time vs. network latency in high-volume fabs.

Semiconductor Industry Compliance & Regulatory Use Cases

Incentive Security	US	CHIPS Act	Grant Verification: Provides the continuous monitoring and unalterable forensic records required to prove the security of facilities receiving federal funding.
IP Safeguarding	Global	NIST 800-171 / CMMC	CUI Protection: Monitors and audits access to controlled unclassified information (CUI), ensuring the protection of sensitive chip designs and technical specifications.
Export Control	Global	ITAR / EAR	Access Auditing: Audits data transfers and remote access to ensure sensitive semiconductor technology is not accessed by restricted entities or regions.
Industrial Resilience	EU	NIS2 Directive	Manufacturing Continuity: Identifies unauthorized pivots and sabotage attempts. RevealX satisfies mandates for continuous monitoring of essential manufacturing.
Incident Reporting	US	CIRCIA	Response Verification: Powers the ability to identify, scope, and report covered incidents within the mandatory 72-hour window using definitive wire-data evidence.

Ensuring Innovation Resilience and Production Continuity Across the Silicon Lifecycle

ExtraHop RevealX delivers tangible business outcomes for semiconductor leaders by transforming complex network data into actionable intelligence. Organizations achieve immediate ROI through the consolidation of security and performance monitoring into a single platform. This reduces operational overhead and improves collaboration between the SOC and the fab operations teams responsible for maintaining high-yield manufacturing.

A primary benefit is the protection of the industry's most valuable asset: intellectual property. By providing unalterable ground truth across design and manufacturing environments, RevealX ensures that security teams can identify industrial espionage attempts before sensitive designs are exfiltrated. This proactive stance protects global market leadership and prevents the massive financial losses associated with the theft of process secrets or the sabotage of advanced fabrication equipment.

Furthermore, RevealX simplifies the complexity of 2026 regulatory compliance. The platform automates the data collection required for CHIPS Act, NIST 800-171, and export control reporting, allowing organizations to meet strict audit requirements with confidence. By maintaining continuous visibility into unmanaged OT and IoT assets, manufacturers can prove the integrity of their digital perimeters to government agencies and partners. Ultimately, RevealX secures the global flow of silicon by ensuring that the digital infrastructure supporting chip innovation remains resilient and visible.

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments in the semiconductor industry: Global Semiconductor Manufacturing Leader

Or contact us to schedule your personalized demo and security assessment.

> "We use ExtraHop every day. When we see a potential problem, it's the first place we go to check it out. With RevealX, we're constantly aware of patterns so we can quickly identify actual issues that need mitigation."

CHIEF INFORMATION OFFICER AND VICE PRESIDENT OF INFORMATION TECHNOLOGY
Leading Manufacturer

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com