EXTRAHOP

Agriculture and Food: Protecting the Global Flow from Farm to Fork

Keep Critical Food Supply Chains and Agricultural Networks Free from Threats with ExtraHop RevealX™

Industry Challenges: Protecting the Flow from Farm to Fork

The global agriculture and food industry operates at the vital intersection of national security and economic stability. By 2026, the sector will have fully embraced Industry 4.0, transforming into a hyper-connected web of autonomous harvesters, IoT-enabled silos, and AI-driven processing facilities. While this digital evolution maximizes yield, it creates a vast, fragmented attack surface where a single compromised sensor can trigger a regional food shortage. Industry leaders face several critical friction points:

- **The Escalation of Nation-State Sabotage and Kinetic Risk:** Geopolitically motivated adversaries have shifted focus from data theft to the functional destruction of food production. These actors target the integrity of automated irrigation systems and livestock climate controls to induce long-term yield failures. Protecting the global food supply requires internal visibility to stop lateral movement before destructive commands can execute on critical field controllers or processing PLCs.
- **The Crisis of Interconnected AgTech and API Sprawl:** Modern agriculture relies on thousands of API integrations between growers, distributors, and retailers. Attackers exploit these trusted connections as a backdoor to move from a partner's environment into the core of a food processing network. Using hijacked service tokens, they can manipulate batch recipes or alter cold-chain temperature logs, creating safety risks that remain undetected by traditional perimeters.
- **The Visibility Gap in Smart Farming and OT Environments:** Processing plants and smart farms run on thousands of unmanaged endpoints, including robotic sorters, smart tractors, and chemical mixers, that cannot host security agents. These agent blind spots allow attackers to move laterally while disabling traditional IT security tools. Organizations must have off-the-box visibility to detect anomalies directly on the wire before they escalate into systemic outages or food safety incidents.
- **Regulatory Rigor and the Mandate for Rapid Disclosure:** 2026 mandates like the FDA's FSMA Rule 204 and the EU NIS2 Directive have compressed the timeline for incident reporting and traceability. Agricultural leaders must now provide an immutable source of truth that proves the integrity of every network interaction. Meeting these standards requires definitive record-keeping to ensure food safety while maintaining the precision required for just-in-time delivery.

KEY CAPABILITIES

Depth and Breadth of NDR Performance: Monitors all network interactions by decrypting and decoding 90+ protocols at speeds up to 100 Gbps to protect high-velocity food processing and automated sortation.

The Definitive Data Source for the AI-Enabled SOC: Provides high-fidelity wire data to power next-generation agriculture SOC automation, eliminating investigative friction and accelerating the path from detection to remediation.

AI-Powered Cyber Threat Detection: Identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting critical AgTech services and supply chain systems using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility: Automatically discovers every asset, including unmanaged IoT devices like smart silos, tractors, and processing robots, along with hybrid cloud workloads, without installing software.

Strategic Line-Rate Decryption: Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats and unauthorized data staging without adding latency to time-sensitive food production operations.

High-Fidelity Performance Metrics: Troubleshoots disruptions using 5,000+ wire data metrics for deep operational insight into network latency and automated production performance.

Continuous Forensic Recording: Maintains an unalterable record of all network transactions to satisfy audit requirements for FSMA, CIRCIA, and NIS2, accelerating root-cause analysis and incident reconstruction.

The Solution: RevealX Network Intelligence

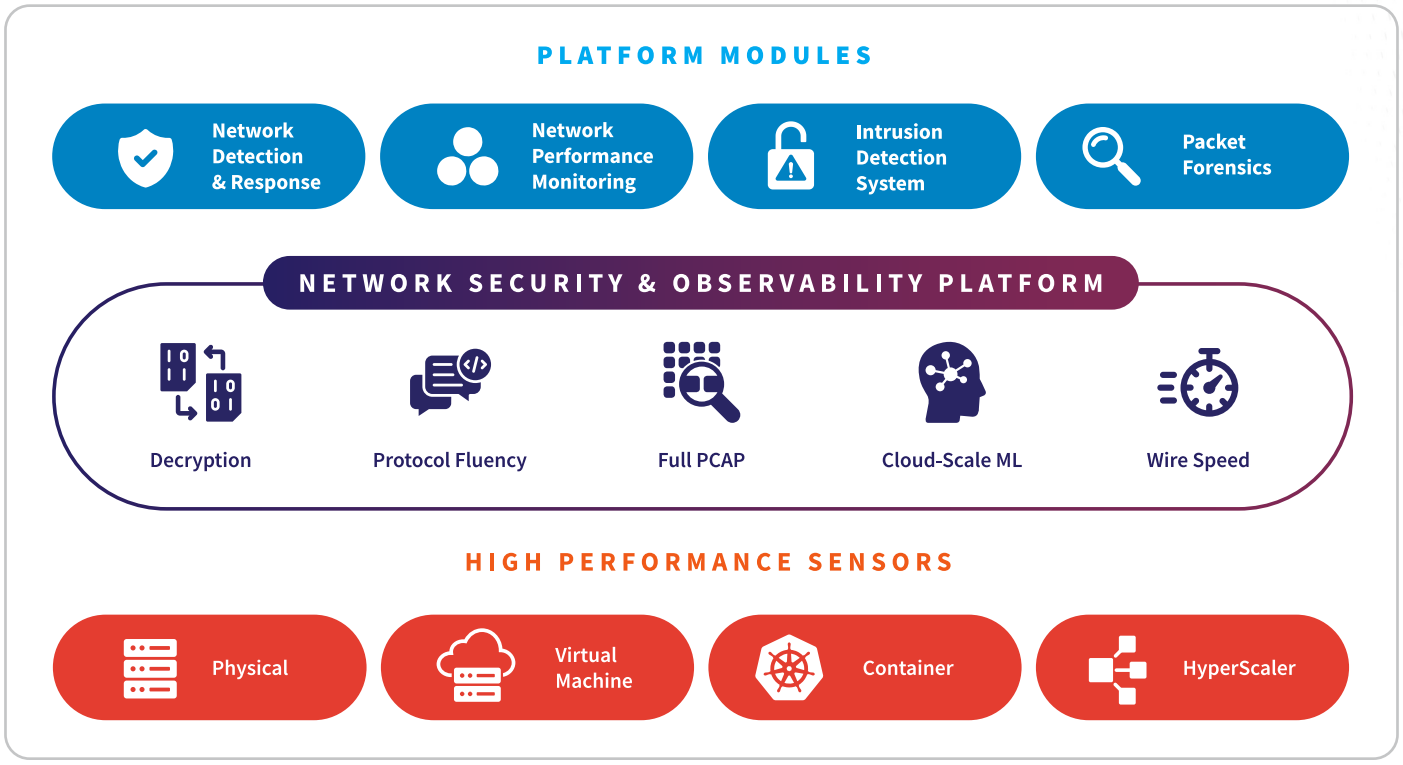
ExtraHop RevealX provides the unalterable ground truth required to secure the modern agriculture and food ecosystem. By analyzing every packet at line rate, RevealX eliminates the visibility gaps that traditional security tools ignore. In a sector where a single hour of downtime can result in the loss of entire perishable batches, RevealX delivers the real-time insights needed to maintain production uptime and global food security.

The platform solves the agent blind spot by providing agentless, passive monitoring of over 90 protocols. This ensures that critical assets like automated irrigation systems, warehouse robots, and cold-chain sensors are fully visible without risking system stability. By baselining normal behavior across these unmanaged IoT and OT devices, security teams can instantly detect anomalies that indicate an adversary has established a foothold on the processing floor or within a remote smart silo.

To counter geopolitically motivated sabotage, RevealX identifies subtle shifts in network behavior that signify lateral movement from corporate IT into the operational heart of the production network. By exposing hidden threats within encrypted traffic using strategic decryption, the platform stops attackers before they can manipulate chemical mixing ratios or freeze automated fulfillment lines. This visibility extends to the sprawling AgTech ecosystem, where RevealX monitors the integrity of third-party integrations to prevent partner-borne contagion from reaching core systems.

Beyond threat detection, RevealX accelerates incident response to meet the compressed disclosure windows of 2026 mandates like CIRCIA and NIS2. It provides a definitive forensic record of all network transactions, eliminating the guesswork during investigations and allowing for rapid root-cause analysis. This unified approach bridges the gap between the SOC and the NOC by combining security detection with performance metrics. By monitoring the health of critical transaction paths, RevealX ensures that security measures do not introduce latency, protecting the precision of farm-to-fork logistics.

ExtraHop NDR Platform



NDR Technology Use Cases for the Agriculture and Food Industry

Nation-State Attacks	Detects lateral movement and exfiltration in campaigns targeting crop yield data, food processing IP, and national food reserve systems.
Threat Detection and Response	Investigates hidden threats across converged IT and OT environments, filling visibility gaps in automated warehouses and processing plants where agents fail.
Threat Hunting	Leverages behavioral baselining to find signature-less threats and protocol anomalies before they impact food safety protocols or production uptime.
SOC Modernization	Unifies SOC and NOC workflows with AI prioritization to reduce alert fatigue, accelerating response times for critical food processing and supply delivery.
Incident Response and Investigation	Delivers forensic visibility and unalterable records of Modbus, MQTT, and OPC UA commands for one-click root-cause analysis of production outages.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots from corporate IT toward critical plant controllers and automated irrigation SIS.
Cloud Workload Security	Provides agentless visibility for cloud-integrated farm management systems (FMS), discovering shadow IT across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value production workstations and silo control systems.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of proprietary recipes or paralysis of the distribution network.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including field sensors, autonomous harvesters, and smart scales that cannot host security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy processing floor hardware and PLC stations.
AI Security	Monitors generative AI and autonomous agents used for yield prediction, soil analysis, or route optimization in containerized workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that IEC 62443 zone/conduit policies and Purdue Model segmentation are effective.

NPM Technology Use Cases for the Agriculture and Food Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for automated processing and sorter control sessions.
Operational Resilience	Resolves infrastructure degradation before it hits production continuity, ensuring availability for mission-critical ERP and supply chain services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between plant operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during FMS or ERP migration by auto-mapping dependencies and using OT baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for 3PL gateways and food traceability APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past processing outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into transaction processing time versus network latency in high-volume hubs.

Agriculture and Food Industry Compliance & Regulatory Use Cases

Food Traceability	United States	FSMA Rule 204	Record Integrity: RevealX provides the unalterable network audit trail required to prove data integrity and verify the "farm-to-fork" chain of custody for safety.
Incident Disclosure	United States	CIRCIA	72-Hour Reporting: Provides the immutable forensic record and ground truth evidence required to meet mandatory CISA reporting timelines for food infrastructure.
Critical Infrastructure	European Union	NIS2 Directive	Network Continuity: Identifies unauthorized pivots and “living-off-the-land” attacks. RevealX satisfies mandates for continuous monitoring of essential food services.
Quality Management	Global	ISO 22000	Process Assurance: Audits network access to critical batching and pasteurization controls. RevealX ensures production quality records remain untampered and accurate.
Supply Chain Risk	Germany / Global	Supply Chain Act (LkSG)	Vendor Auditing: Monitors third-party maintenance and 3PL connections for unauthorized pivots to the processing floor, ensuring production integrity is not compromised.

Customer Benefits: Ensuring Supply Chain Resilience and Operational Continuity Across the Food Ecosystem

ExtraHop RevealX delivers tangible business outcomes for agriculture and food leaders by transforming network data into actionable intelligence. Organizations achieve immediate ROI through the consolidation of security and performance monitoring tools, which reduces operational overhead while improving cross-team collaboration between the SOC and NOC.

A primary benefit is the significant reduction in mean time to detect and respond to systemic threats. By providing unalterable ground truth across the entire supply chain, RevealX ensures that security teams can identify lateral movement before it impacts food processing or cold-chain logistics. This proactive stance protects brand reputation and prevents the massive financial losses associated with batch contamination or distribution standstills.

Furthermore, RevealX simplifies the complexity of 2026 regulatory compliance. The platform automates the data collection required for FSMA 204, CIRCIA, and NIS2 reporting, allowing organizations to meet strict disclosure windows with confidence. By maintaining continuous visibility into unmanaged IoT and OT assets, food producers can prove the integrity of their digital perimeters to partners and insurers. Ultimately, RevealX secures the global flow of nutrition by ensuring that the digital infrastructure supporting the physical world remains resilient, visible, and under control.

> "ExtraHop has fundamentally changed the way that we monitor and manage our business."
>
> Director of IT
> US-Based Application Provider

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:
Home Depot | Ulta Beauty | Seattle Children's Hospital

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

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