EXTRAHOP

Securing the Architecture, Engineering, & Construction Digital Lifecycle: Protecting Design IP and Project Continuity

Protect Project Timelines and Infrastructure Integrity with Real-Time Network Intelligence

SOLUTION BRIEF

Industry Challenges: Securing the Architecture, Engineering, and Construction Lifecycle

In 2026, architecture, engineering, and construction (AEC) firms operate under constant operational friction where digital vulnerabilities cause physical project delays. As the industry integrates digital lifecycles, the attack surface expands to every job site and subcontractor connection. A single breach can compromise proprietary design work or halt multi-billion-dollar infrastructure projects. AEC leaders face several critical friction points:

- **Persistent Non-Kinetic Warfare and State Actors:** The industry faces continuous undeclared conflict where state-sponsored actors target critical infrastructure blueprints. By gaining engineering network footholds, adversaries map structural vulnerabilities in utility hubs and transport networks during the design phase to enable strategic leverage long before construction begins.
- **Intellectual Property and Design Theft:** Proprietary blueprints and engineering specifications are high-value targets. Threat actors exfiltrate BIM files and CAD designs containing a project's "digital DNA." This espionage allows competitors to avoid R&D costs and undermines the competitive advantage of engineering innovators.
- **Ransomware and Project Continuity:** Ransomware uses recovery denial tactics to target production lines. By locking project management and logistics systems, attackers force work stoppages, triggering massive penalties and reputational damage that jeopardize future contract awards.
- **The Subcontractor and Supply Chain Gap:** Fragmented third-party networks often lack robust security, serving as preferred entry points. Attackers compromise these smaller vendors to move laterally into sensitive design repositories, making extended enterprise risk a significant burden.
- **Regulatory and Compliance Pressure:** Public and private projects face stringent requirements. Defense contractors must satisfy CMMC 2.0 and NIST 800-171, while the commercial sector follows ISO 19650-5. Additionally, insurers increasingly demand real-time behavioral telemetry for liability coverage.
- **Unmanaged IoT and Job Site Connectivity:** High-density job sites utilize connected machinery and access controllers on temporary networks. These unmanaged devices cannot support security agents, creating significant blind spots that attackers exploit as launchpads for broader corporate attacks.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all network interactions by decrypting and decoding over 90 protocols at line rate to protect high-density design studios and globally distributed job site operations.

The Definitive Data Source for the AI-Enabled SOC

ExtraHop RevealX provides high-fidelity wire data for AEC SOC automation. This unalterable ground truth accelerates the path from detection to remediation.

AI-Powered Cyber Threat Detection

Identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting proprietary design IP and infrastructure using cloud-scale machine learning.

Unified Agentless Visibility

Automatically discovers all assets, including unmanaged IoT and hybrid cloud workloads, without installing software or risking project stability.

Strategic Line-Rate Decryption

Analyzes TLS 1.3 and PFS traffic to expose hidden threats and unauthorized data staging without adding latency to BIM synchronization.

High-Fidelity Performance Metrics

Troubleshoots disruptions and verifies SLAs using 5,000+ wire data metrics for insight into network latency and AEC application performance.

Continuous Forensic Capture

Maintains unalterable network records to satisfy CMMC 2.0, NIST 800-171, and ISO 19650-5 audit requirements while accelerating incident reconstruction.

The Solution: Unified Network Intelligence for the AEC Lifecycle

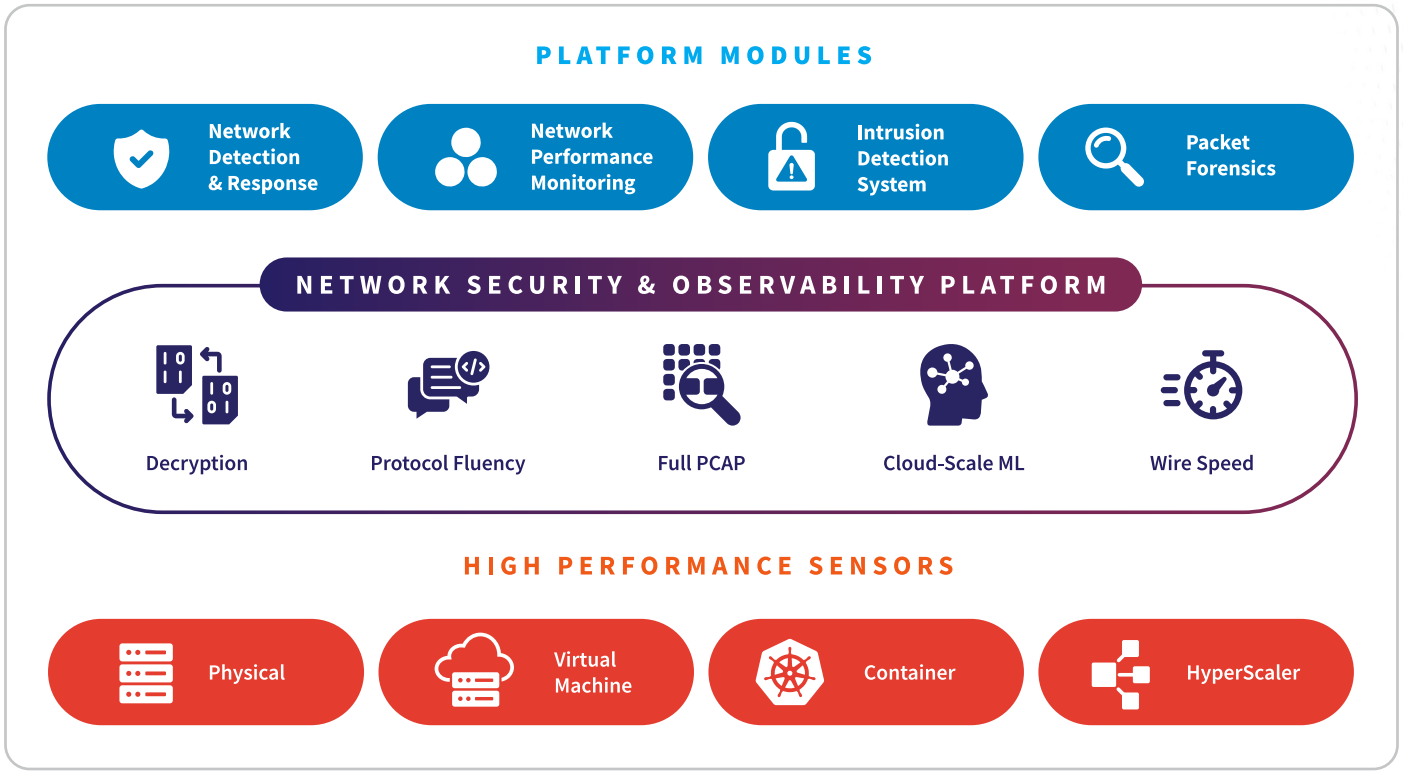
ExtraHop RevealX™ provides the real-time visibility and behavioral analytics required to secure the integrated digital workflows of modern construction and engineering firms. By turning the network into a source of ground truth, RevealX allows security teams to identify and contain threats that bypass traditional perimeter and agent-based defenses. This approach helps to ensure that the digital DNA of a project remains protected from the initial design phase through the final physical handover.

RevealX eliminates the visibility gaps created by a fragmented supply chain and the proliferation of unmanaged IoT at the jobsite edge. The platform automatically discovers and classifies every asset on the network, including connected heavy machinery, site access controllers, and subcontractor devices. This agentless monitoring provides a continuous audit of all internal and external connections, allowing firms to detect lateral movement or credential abuse before an attacker can access sensitive engineering repositories.

To protect high-value intellectual property, RevealX decrypts and analyzes network traffic at line rate to expose hidden threats within encrypted BIM and CAD synchronization. Behavioral machine learning baselines normal data movement to identify anomalous exfiltration patterns or unauthorized access to proprietary blueprints. By stopping the theft of design innovations, AEC firms can maintain their competitive advantage and prevent the long-term strategic risks associated with state-sponsored espionage.

Operationally, RevealX helps to ensure project continuity by detecting the early indicators of ransomware and recovery denial tactics that threaten to halt construction schedules. The platform provides the high-fidelity telemetry needed to accelerate incident response and minimize the risk of costly contractual delays. Additionally, RevealX serves as the definitive record of network activity to satisfy the stringent requirements of ISO 19650-5 and CMMC 2.0, providing the empirical proof of security posture required by regulators and insurance carriers.

ExtraHop NDR Platform



NDR Technology Use Cases for the Construction and Engineering Industry

Nation-State Attacks	Detects lateral movement and exfiltration in long-term campaigns targeting critical infrastructure blueprints, structural engineering secrets, and utility hub designs.
Threat Detection and Response	Investigates hidden threats across integrated BIM environments and job site networks, filling visibility gaps where traditional logs and agents fail.
Threat Hunting	Leverages behavioral baselining to find signature-less threats targeting proprietary design servers before they impact project timelines or IP integrity.
SOC Modernization	Unifies workflows between corporate IT and field operations using AI prioritization to reduce alert fatigue and accelerate response for globally distributed projects.
Incident Response and Investigation	Delivers forensic visibility and unalterable records of BIM and CAD protocol interactions for root-cause analysis of data corruption or unauthorized access.
Lateral Movement	Uses peer-group clustering to detect pivots from compromised subcontractor laptops toward sensitive design repositories, engineering zones, and financial systems.
Cloud Workload Security	Provides agentless visibility for cloud-integrated AEC workloads, discovering unmanaged assets across Autodesk Construction Cloud, AWS, and Azure environments.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value BIM manager accounts, jump hosts, and engineering workstations.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of proprietary designs or the disruption of site-level logistics.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including connected heavy machinery, site access controllers, and smart sensors that cannot support security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy job site hardware and remote engineering stations.
AI Security	Monitors generative AI and autonomous agents used for generative design, structural optimization, or site-level autonomous robotics in containerized workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that ISO 19650-5 security zones and network segmentation policies remain effective across the project lifecycle.

NPM Technology Use Cases for the Construction and Engineering Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for BIM-to-server sessions and real-time design collaboration.
Operational Resilience	Resolves infrastructure degradation before it hits project continuity, ensuring availability for mission-critical site management and logistics services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between field engineers and centralized IT support teams.
Migrate Workloads to the Cloud	Maintains performance during BIM repository or ERP migration by auto-mapping dependencies and using baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value modeling applications and data synchronization tools, ensuring performance for project-critical APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past project outages or significant telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into BIM synchronization time versus underlying network latency.

Construction and Engineering Industry Compliance & Regulatory Use Cases

Information Security	Global	ISO 19650-5	Security-Minded BIM: Mandates protecting sensitive building data throughout the asset lifecycle to prevent structural exploitation or unauthorized access.
Defense Contracting	US	CMMC 2.0	Certification Readiness: Provides continuous monitoring and incident response evidence required for federal contract eligibility and audit verification.
Data Protection	US	NIST 800-171	CUI Protection: Powers the detection of anomalies targeting Controlled Unclassified Information within engineering and design networks in real time.
Liability Management	Global	Cyber Insurance Mandates	Telemetry Verification: Supplies the unalterable network records and behavioral telemetry required by carriers to maintain professional liability coverage.
Contractual Compliance	Global	Private Client Annexes	Access Auditing: Tracks the exact sequence of events for third-party access to client proprietary site data, facilitating rapid incident reporting.
Infrastructure Integrity	Global	Smart Building Codes	System Integrity: Identifies lateral movement and unauthorized remote access, bypassing traditional gates to protect integrated building systems.

Customer Benefits: Ensuring Project Resilience and Operational Continuity Across the AEC Lifecycle

Visibility into network truth is the essential foundation of modern project protection. RevealX provides the real-time insights required for high-density design collaboration and complex job site logistics. By monitoring the wire, firms can safeguard against cyber threats and protocol anomalies that jeopardize project timelines and structural data integrity. This approach allows security teams to move at the speed of the business without introducing the friction caused by intrusive security agents or complex endpoint deployments that cannot reach every subcontractor device.

The shift to fully integrated digital lifecycles creates exploitable blind spots throughout a fragmented global supply chain. RevealX secures proprietary designs and distributed job site resources by observing actual traffic, including BIM synchronization and CAD data, instead of relying on modifiable logs. This level of observation provides the definitive forensic evidence needed to satisfy ISO 19650-5, CMMC 2.0, and NIST 800-171 mandates. By identifying anomalies in how data is accessed and moved across the network, firms can provide the empirical proof of security posture required by regulators and cyber insurance carriers.

RevealX also secures the unmanaged ecosystem of connected heavy machinery and smart site sensors that traditional agent-based tools miss. It identifies lateral movement and credential abuse before they compromise sensitive engineering repositories or expose proprietary blueprints to sophisticated adversaries. Through continuous and real-time discovery and classification, RevealX ensures that critical infrastructure delivery and commercial builds remain uninterrupted. This proactive stance prevents the cascading financial impact of work stoppages and the heavy penalty clauses associated with project delays.

> "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."
>
> **CIO & VP-IT**
> Leading Manufacturer

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:
Logistics and Transportation Leader
North American Homebuilder
EMEA Industrial Leader

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