EXTRAHOP

Protecting the Modern Property Technology Ecosystem

Keep Critical Property Technology and Smart Building Applications Free from Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: From Physical Foundations to Digital Vulnerability

Property technology (PropTech) serves as the digital orchestration of the built environment, bridging physical real estate assets and cloud-integrated management systems. This infrastructure spans cloud-native management software and the IoT sensor arrays that define modern smart buildings. By 2026, the sector will have reached a critical pivot where cybersecurity is one of the direct foundations of asset valuation and operational continuity.

Property leaders face several critical friction points:

- **Nation-State Sabotage and Kinetic Risk:** Geopolitically motivated actors have shifted from simple data theft to functional destruction. In early 2024, attackers used AI-generated deepfakes to trick a finance worker at a global engineering firm into transferring $25.6 million. Physical building systems are also primary targets for siegeware, which is a specialized form of extortion where attackers seize control of building automation systems (BAS) to hold the physical environment hostage. By hijacking HVAC, lighting, or elevator controls, attackers can render a building uninhabitable until a ransom is paid. Unlike traditional ransomware that only locks data, siegeware targets the kinetic or physical functions of a property to render it uninhabitable or dangerous. A prominent example occurred recently when a major building automation provider suffered a ransomware attack that disrupted building automation and security platforms across its global portfolio. Visibility is required to contain movement before malicious commands reach life safety systems.
- **The Identity and Post-Compromise Crisis:** Advanced actors prioritize the exploitation of tenant data and high-value identities using generative AI and deepfake impersonation. They bypass traditional authentication to navigate undetected toward sensitive financial records and building access databases. PropTech firms must identify this living off the land behavior on the wire to prevent mass exfiltration of sensitive information or the abuse of service accounts.
- **The IoT and Surveillance Blind Spot:** Modern properties run thousands of unmanaged endpoints, including smart locks and 4K cameras, that cannot host security agents. This agent blind spot leaves specialized traffic invisible to traditional IT tools. Attackers use these nodes as a foothold to pivot into core business systems, creating a visibility gap that violates zero trust principles. Proactive discovery of these assets is critical for grid and building stability.
- **Regulatory Rigor and the IT Visibility Mandate:** The rollout of PCI DSS 4.0.1 requires institutions to prove real-time behavioral monitoring across IT environments. Simultaneously, NYC Local Law 97 mandates buildings over 25,000 square feet meet emission limits or face annual penalties. Proving digital integrity relies on network ground truth to confirm compliance data remains unmodified. Proving system integrity requires an unalterable record of transactions to satisfy audit requirements.

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-density property portfolios.

The Definitive Data Source for the AI-Enabled SOC

Provides the high-fidelity wire data required to power the next generation of PropTech SOC automation applications and defenses.

AI-Powered Cyber Threat Detection

Identifies sophisticated attacks and early-stage ransomware targeting property management systems using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers every asset, including unmanaged IoT sensors and building controllers, without installing software or impacting system performance.

Strategic Line-Rate Decryption

Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats in payment and building access APIs without adding latency.

High-Fidelity Performance Metrics

Troubleshoots complex disruptions using over 5,000 wire data metrics for deep operational insight into smart building application and database performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy audit requirements for PCI DSS 4.0.1 and other reporting mandates.

The Solution: RevealX Network Intelligence

ExtraHop RevealX delivers the comprehensive network intelligence required to secure the complex digital supply chain of modern real estate. By providing a unified, real-time view across converged IT and building management system (BMS) environments, RevealX enables security teams to detect and neutralize sophisticated threats across expansive property portfolios. Whether managing high-rise residential complexes, automated fulfillment centers, or luxury commercial spaces, the platform provides the visibility needed to maintain operational continuity and protect high-value physical assets from digital exploitation.

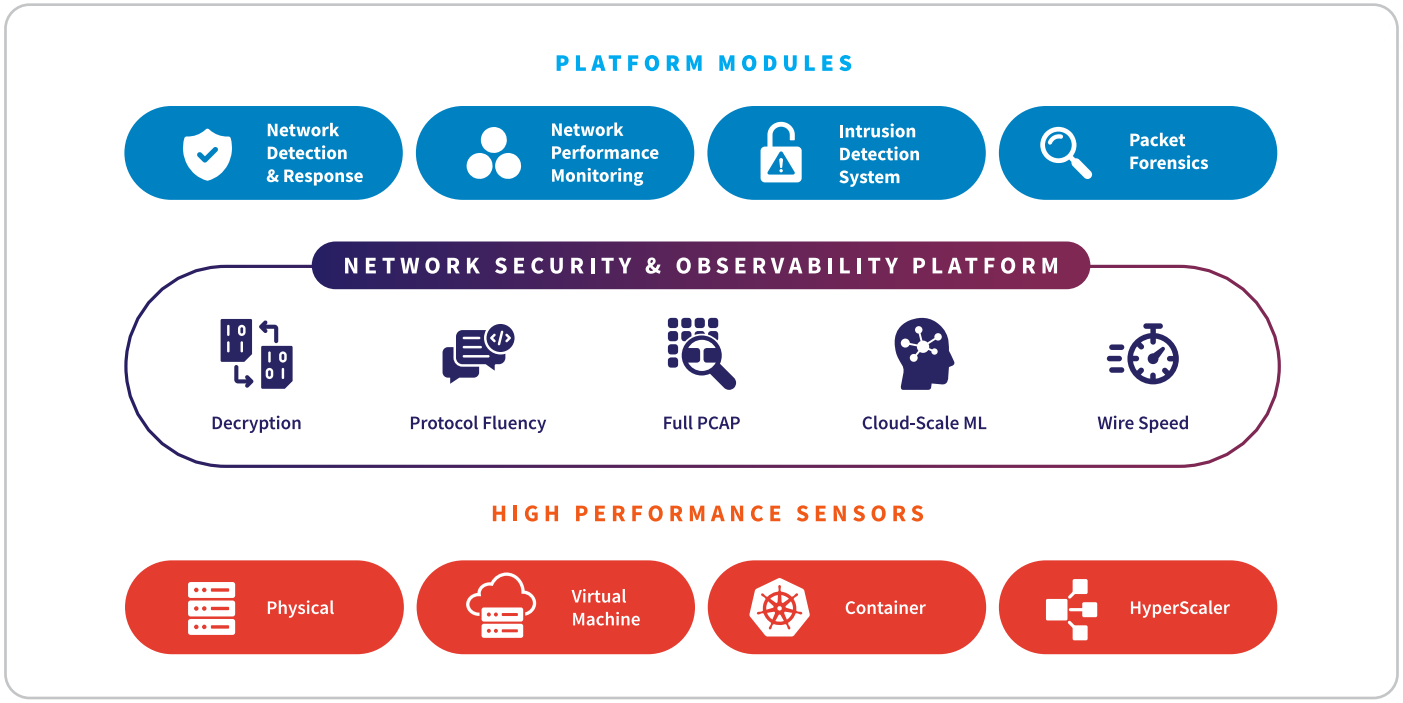
Neutralizing destructive kinetic attacks or AI-driven financial fraud requires stopping malicious actors before they can execute damaging commands. Because RevealX monitors the wire directly rather than relying on vulnerable endpoint agents, it identifies the subtle lateral movement and credential abuse used to pivot from corporate office environments into sensitive building control zones. This agentless approach is particularly critical in PropTech environments where thousands of unmanaged IoT devices, such as smart locks and environmental sensors, cannot support traditional security software without risking system crashes or operational instability.

When a threat is detected, RevealX provides the forensic detail necessary to understand the scope and intent of the intrusion. Security teams can rapidly isolate affected segments, preserving the integrity of property management systems (PMS) and protecting building infrastructure from systemic disruption or ransomware-induced shutdowns. This high-fidelity wire data ensures that critical property services, such as vertical transport, climate control, and life safety systems, remain uninterrupted even during an active security incident. By analyzing traffic at the protocol level, RevealX exposes hidden commands that traditional tools miss.

Beyond immediate threat detection, RevealX satisfies the rigorous auditing requirements of modern regulations like PCI DSS 4.0.1 and localized mandates such as NYC Local Law 97. By maintaining an unalterable record of all network transactions, the platform provides the ground truth required to prove that energy management data and tenant financial records have not been tampered with or modified by unauthorized entities. This level of transparency is essential for maintaining asset valuation and long-term tenant trust in an increasingly connected and regulated global market.

RevealX transforms the network into a source of truth for property leaders. It closes the visibility gap between the digital and physical worlds, providing the resilience needed to scale smart building operations without increasing organizational risk. Property technology firms use the platform to validate that their sensors and third-party maintenance connections are not compromised. By shifting the focus to behavioral analysis on the wire, organizations maintain a robust defense against evolving tactics that target the intersection of property and technology.

ExtraHop NDR Platform



NDR Technology Use Cases for the PropTech Industry

Nation-State Attacks	Detects lateral movement and exfiltration in campaigns targeting high-value real estate portfolios, critical building infrastructure, and sensitive tenant data.
Threat Detection and Response	Investigates hidden threats across converged IT and building management system (BMS) environments where traditional agents cannot be installed.
Threat Hunting	Uses behavioral baselining to find signature-less threats in IoT sensor arrays before they impact building safety, climate controls, or physical security.
SOC Modernization	Unifies building facilities and IT security workflows, using AI prioritization to reduce alert fatigue and accelerate response for smart building services.
Incident Response and Investigation	Delivers forensic visibility and unalterable records of building protocols like BACnet and Modbus for rapid root-cause analysis of system disruptions.
Lateral Movement	Detects pivots from guest Wi-Fi or unmanaged IoT nodes toward sensitive property management systems (PMS) and critical building controllers.
Cloud Workload Security	Provides agentless visibility for cloud-integrated PropTech applications, identifying shadow IT and unmanaged assets across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse and deepfake impersonation targeting property managers and high-value identities.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before attackers can lock down building access or exfiltrate tenant financial records.
Unmanaged Devices	Monitors network traffic for unmanaged smart locks, 4K surveillance cameras, and environmental sensors that cannot support traditional security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled or missing on legacy elevator controllers and HVAC workstations.
AI Security	Monitors generative AI and autonomous agents used for building energy optimization and tenant experience management in containerized workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that micro-segmentation between tenant zones and management networks is effective.

NPM Technology Use Cases for the PropTech Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for smart building sensors and IoT-to-cloud sessions.
Operational Resilience	Resolves infrastructure degradation before it hits tenant experience, ensuring the availability of mission-critical life safety and climate services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a unified workflow, eliminating friction between facilities operations and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during PMS or tenant portal migration by auto-mapping dependencies and using baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for building access APIs and payment gateways.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past building outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into building automation system (BAS) command processing time.

PropTech Industry Compliance & Regulatory Use Cases

Asset Integrity	US (NYC)	Local Law 97	Data Validation: Ensures energy management data for carbon compliance has not been tampered with by providing an unalterable network record.
Cybersecurity Maturity	Global	UL/TIA SPIRE	Cyber Audit: Powers the cybersecurity criterion by using wire data to audit network security and building system isolation.
Life Safety Systems	Global	UL 2900-2-3	Software Security: Evaluates the digital integrity of network-connectable life safety and security signaling systems.
Smart Building Best Practice	US	NIST Digital Building Profile	Detect & Protect: Automates the identification of anomalies within HVAC, lighting, and vertical transport systems to meet NIST security profiles.
Financial Data Security	Global	PCI DSS 4.0.1	CDE Monitoring: Safeguards sensitive cardholder data in PMS environments by monitoring for unauthorized staging or access.

Customer Benefits: Hardening the Digital Infrastructure of the Physical Asset Portfolio

In 2026, a property is no longer just steel and glass. It is a converged network where a single vulnerability in a smart lock or HVAC controller can directly impact net operating income. ExtraHop RevealX provides real-time visibility across every system, allowing property leaders to contain lateral movement before a malicious actor can jeopardize tenant safety or asset integrity.

To counter generative AI-driven fraud and deepfake impersonation, RevealX establishes behavioral baselines for every device and user. The platform detects post-compromise activity that traditional authentication tools miss, including unauthorized access to tenant databases and fraudulent attempts to reach property management systems.

RevealX also eliminates the visibility gap created by thousands of unmanaged IoT endpoints. Using an agentless approach, it discovers and monitors PropTech devices automatically, identifying when they are used as a foothold into core business systems.

Finally, RevealX transforms PCI DSS 4.0.1 compliance into a repeatable process. It provides the forensic evidence needed to satisfy auditors and protect tenant trust at scale.

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.
Global Telco Provider
City of Dallas
Financial Organization

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

> "The network is the ground truth. It's what attackers can't avoid. You give yourself the ability to see everything on the network. You deploy ExtraHop, now you have the ability to see everything. Without that data, you're operating partially or completely blind. There is no other technology outside of NDR that can give you that, and in my professional opinion, ExtraHop is the best NDR."
>
> **TECHNICAL DIRECTOR**

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