EXTRAHOP

ExtraHop Global Threat Landscape Report

Manufacturing, Construction, and Utilities Edition

Table of Contents

Key Industrial Sector Findings

$2.7M
AVERAGE RANSOMWARE PAYMENT

1.60 Days
AVERAGE DOWNTIME PER INCIDENT

54.15%
CITE PUBLIC CLOUD AS TOP CYBER RISK

12.3 Days
DWELL TIME

The Shift Redefining Cybersecurity in the Industrial Sector

In the utilities and industrial sectors, safety, reliability, and operational continuity have long been foundational priorities. Historically, this commitment was secured through physical hardening, fail-safes, and rigorous safety protocols.

As these environments have become increasingly dependent on connected systems, that same mission-critical discipline has expanded into digital defense, shaped by a rapidly evolving regulatory landscape.

Government mandates from NERC CIP to Europe's NIS2 are formalizing what industry leaders already know: critical infrastructure is a primary target for cyber threats. Rather than viewing these regulations as administrative hurdles, forward-thinking organizations are utilizing them as strategic blueprints through which to establish a unified baseline for cyber resilience.

However, these frameworks do not exist in a vacuum. They are a direct response to a highly aggressive and constantly evolving adversary that has moved beyond the perimeter, and whose actions can ripple through physical supply chains and threaten public safety.

THE INDUSTRIAL RISK REALITY

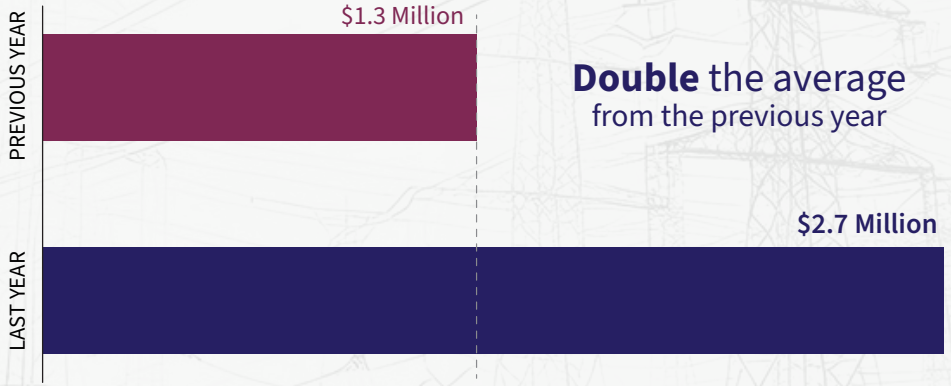
This regulatory momentum establishes a defensive baseline, yet it also exposes a gap: as perimeters evolve, the sheer volume and persistence of modern strikes have pushed industrial organizations into a cycle of continuous incident response.

Over the last 12 months, industrial organizations experienced five ransomware incidents on average.

And the costs are **catastrophic**.

When asked how much their organization paid in ransomware payments in the last year, industrial respondents reported an average of $2.7 million, almost double the average from the previous year.

Beyond the ransom itself, the true cost of these incidents is measured in the halted production and paralyzed systems that can erode margins long after the ransom payment is made.



Disruption is also measurable through incident-level downtime.

On average, organizations in this sector experienced 38 hours of downtime per incident. For high-output environments, this time can halt production, disrupt essential services, strain supply chains, and generate lasting financial and operational fallout.

Real incidents show how disruption plays out at scale.

Jaguar Land Rover

In late 2025, a ransomware attack shut down Jaguar Land Rover's global production for five weeks, halting the assembly of approximately 1,000 vehicles per day and costing an estimated $2.5 billion. The incident followed closely on the heels of a massive breach six months prior, when the threat actor HELLCAT exfiltrated 350GB of proprietary data.

Halliburton

In August 2024, the RansomHub ransomware gang breached Halliburton, a global energy services company operating in 70 countries, forcing a shutdown of IT systems that resulted in $35 million in immediate losses.

The attack's full cost remains an open question: with data confirmed stolen, Halliburton faces additional financial exposure should client data be sold or leaked, potentially triggering litigation and further regulatory scrutiny.

The Industrial Cybersecurity Landscape

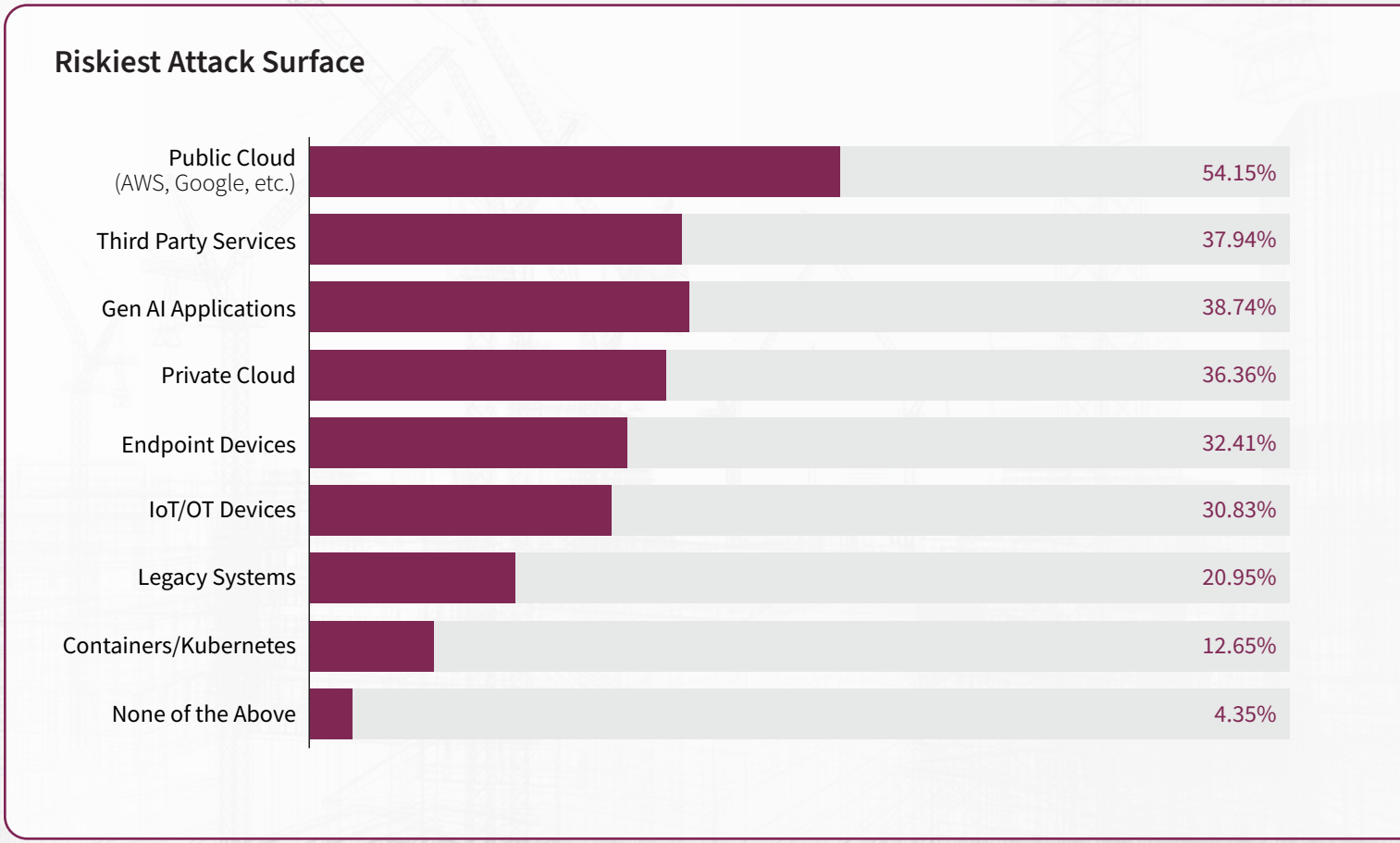
AN EXPANDING ATTACK SURFACE

The attack surface is expanding, making defense even more difficult for industrial organizations, especially as they increasingly move critical data and OT management to the cloud.

Public cloud (AWS, Google, Azure, etc.) represents the most significant cybersecurity risk for this sector (54.15%).

Gen AI applications represent the second-most significant risk (38.74%), as rapid adoption introduces unmanaged data flows that attackers exploit for exfiltration.

Third-party services and integrations follow at 37.94%, where each integration point represents a potential entry vector that bypasses primary defenses.



PROLIFERATING THREATS

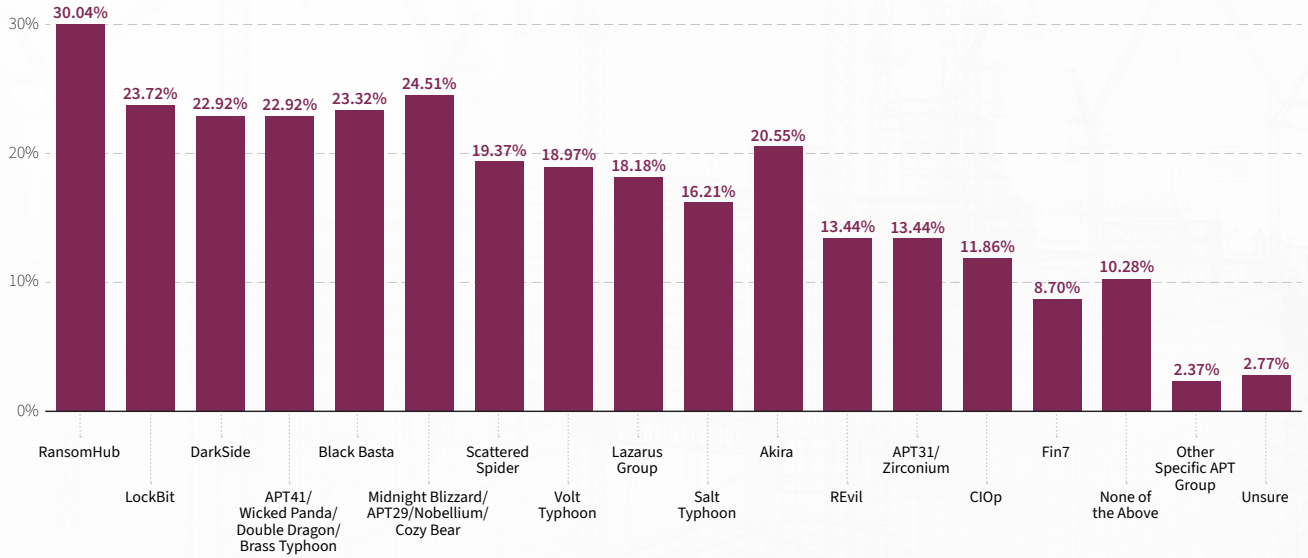
The expanding attack surface is being exploited by a growing range of threat actors, including RansomHub, Midnight Blizzard (APT29), LockBit, DarkSide, and APT41.

Among these, **RansomHub** was the most widely observed, detected in nearly a third of industrial networks. The group targets manufacturing, construction, engineering, and utilities via vulnerabilities in public-facing services or spearphishing. Upon entry, it uses custom tools and Living-off-the-Land (LotL) techniques to steal privileged service account credentials and move laterally across systems.

Midnight Blizzard was detected in a quarter of industrial networks. It typically gains access through password spraying, dormant accounts without MFA, or spearphishing. It then uses identity and cloud infrastructure to maintain access while blending in as legitimate users. The result is long-term, low-visibility access to industrial environments, often to steal blueprints and intellectual property over time.

LockBit was detected nearly as frequently. The group commonly gains entry through public-facing services, phishing, or stolen credentials. After initial access, it uses tools like PsExec and Cobalt Strike to move laterally and escalate privileges across the environment. The attackers then typically encrypt systems, steal data, and leak it on the dark web, triggering regulatory scrutiny and litigation.

Top Ransomware and Nation-State Actors Using Lateral Movement, Industrial Sector



In December of 2025, Luxshare, a major supplier to Apple, Nvidia, and Tesla, was hit by **RansomHub**, with attackers claiming to have stolen more than 1TB of sensitive manufacturing data, including CAD models and engineering documents.

In 2024, a **LockBit** attack on the City of Wichita disrupted municipal systems, including a water utility billing site, forcing residents to pay bills in person.

Threat Actors' Tactics

GAINING INITIAL ACCESS

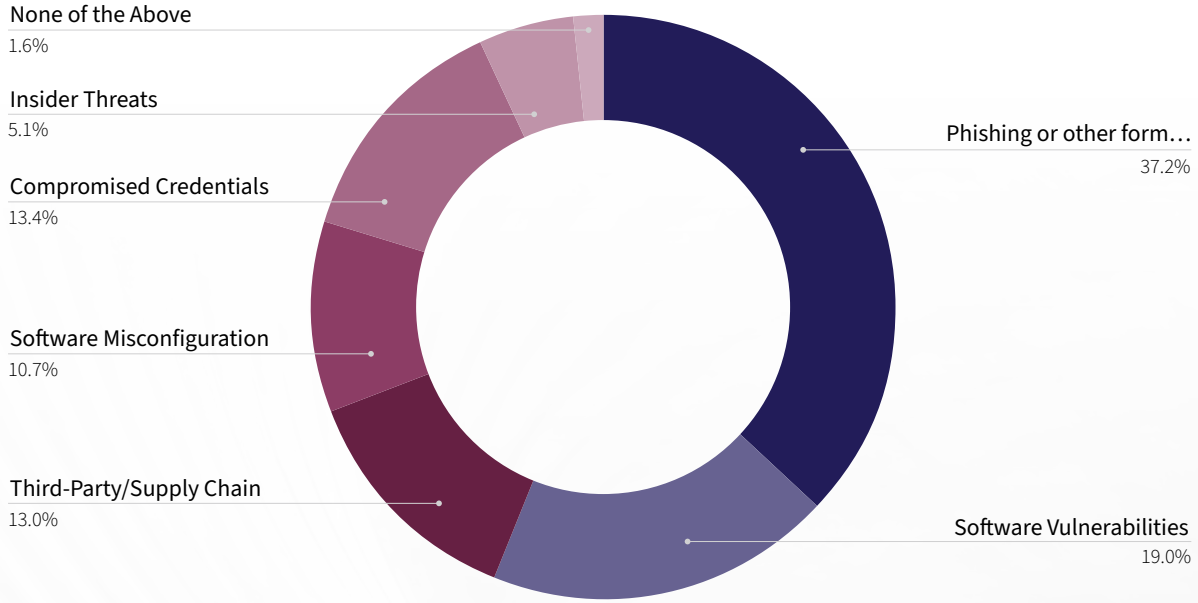
Threat actors exploit several common attack vectors to gain access in these environments. Phishing and social engineering are the most common initial points of entry (37.2%), followed by software vulnerabilities (19.0%).

Compromised credentials or brute-force attacks come in third (13.4%).

These credentials are particularly valuable because they provide immediate legitimacy within the environment, allowing attackers to bypass perimeter defenses without triggering traditional access controls.

Once inside, those same credentials can unlock broader access across the infrastructure. In cloud environments in particular, **a single set of credentials may authenticate across multiple services**, enabling attackers to move laterally and expand their reach beyond the initial point of compromise.

Most Common Initial Points of Entry for Attackers Targeting Manufacturing, Construction, and Utilities



MOVING LATERALLY

Once access is gained, the “dwell time” begins. This is the period in which attackers establish persistence and expand their reach inside the environment.

In the event of a ransomware incident, security teams believe threat actors had access to their systems for an average of 12.3 days. During this window, attackers move laterally to navigate internal systems, escalate privileges, and map high-value operational and engineering assets while remaining undetected.

LEVERAGING ORGANIZATIONAL WEAKNESSES

The technical reality is that detection often occurs too late in the attack cycle to prevent impact.

Organizations in the manufacturing, construction, and utilities sectors take an average of 2.23 weeks to respond to and contain a security alert from initial detection to resolution. This lag is a window of opportunity for attackers to deepen their persistence, increasing the likelihood of operational disruptions, data exposure, and widespread business impact.

When this window extends, limited visibility into attacker movement can trigger regulatory intervention. If an organization cannot immediately account for an attacker’s internal movement, regulators often move beyond the incident to impose restrictive oversight and “red tape” that stalls business growth, leading to delayed modernization initiatives, rising compliance costs, constrained operational agility, and long-term competitive disadvantage.

FERC Order 887 mandates a level of telemetry that exposes lateral movement. It’s a shift that ensures an attacker can no longer move through the shadows of an internal network, turning what used to be a blind spot into a detectable event.

How the Industrial Sector Can Fight Back

Disrupting the attack chain early is key.

Limited visibility into the environment is the top-cited challenge (39.92%), hindering timely response to security threats in this sector.

While perimeter defenses may be hardened, limited internal transparency leaves organizations exposed to lateral movement within the network.

Comprehensive network visibility enables organizations to detect and stop compromises before high-value assets are reached. By closing these visibility gaps, organizations reduce lateral movement and dwell time, limiting financial losses and improving operational outcomes.

HOW WE GET THERE

After initial compromise of the environment, visibility is critical. The path forward requires telemetry that transforms lateral movement from a hidden liability into a definitive trigger for response, removing attackers' ability to operate undetected within the internal network. This effectively turns the network itself into a sensor.

DETECT THREATS FASTER

Most security tools exclusively focus on the "front door," monitoring only north-south traffic while offering limited visibility into internal east-west movement.

Once attackers break in, they're able to hide, often blending into normal traffic patterns, making the need for behavior analysis and monitoring more critical than ever before.

How Attackers Blend into Legitimate Activity

Compromising Hidden or Unmanaged Devices

Threat actors often exploit hidden or unmanaged devices to bypass controls and escalate privileges. Legacy PLCs, IoT sensors, SCADA systems, and shadow IT assets frequently fall outside of formal inventories, creating persistent blind spots and ideal footholds.

CIP-015-1 now mandates anomalous behavior detection across all connected assets, including those outside formal inventories. Closing the gaps requires passive network monitoring that continuously discovers and classifies devices, flagging abnormal activity.

Hiding in Encrypted Traffic

Attackers conceal lateral movement within encrypted flows, where malicious commands often ride alongside legitimate communications. Both CISA and NIST have identified these risks, and FERC Order 887 now mandates the internal telemetry required to address them.

Stealing Credentials & Tool Abuse

Adversaries exploit stolen credentials and legitimate tools like PsExec and Cobalt Strike to make malicious activity appear routine. Groups like RansomHub and Midnight Blizzard specifically target privileged service accounts to evade detection. Unmasking these tactics requires correlating identities with network behavior, helping to expose abnormal activity early.

Exploiting Siloed Tools

Attackers exploit fragmented visibility caused by poorly integrated security tools — an issue affecting nearly 36% of industrial organizations — to move across IT, OT, and cloud environments unnoticed.

Integrating network telemetry provides the contextualized data necessary to validate threats faster. When paired with EDR integrations, teams can automate detection and containment, eliminating the attacker's head start.

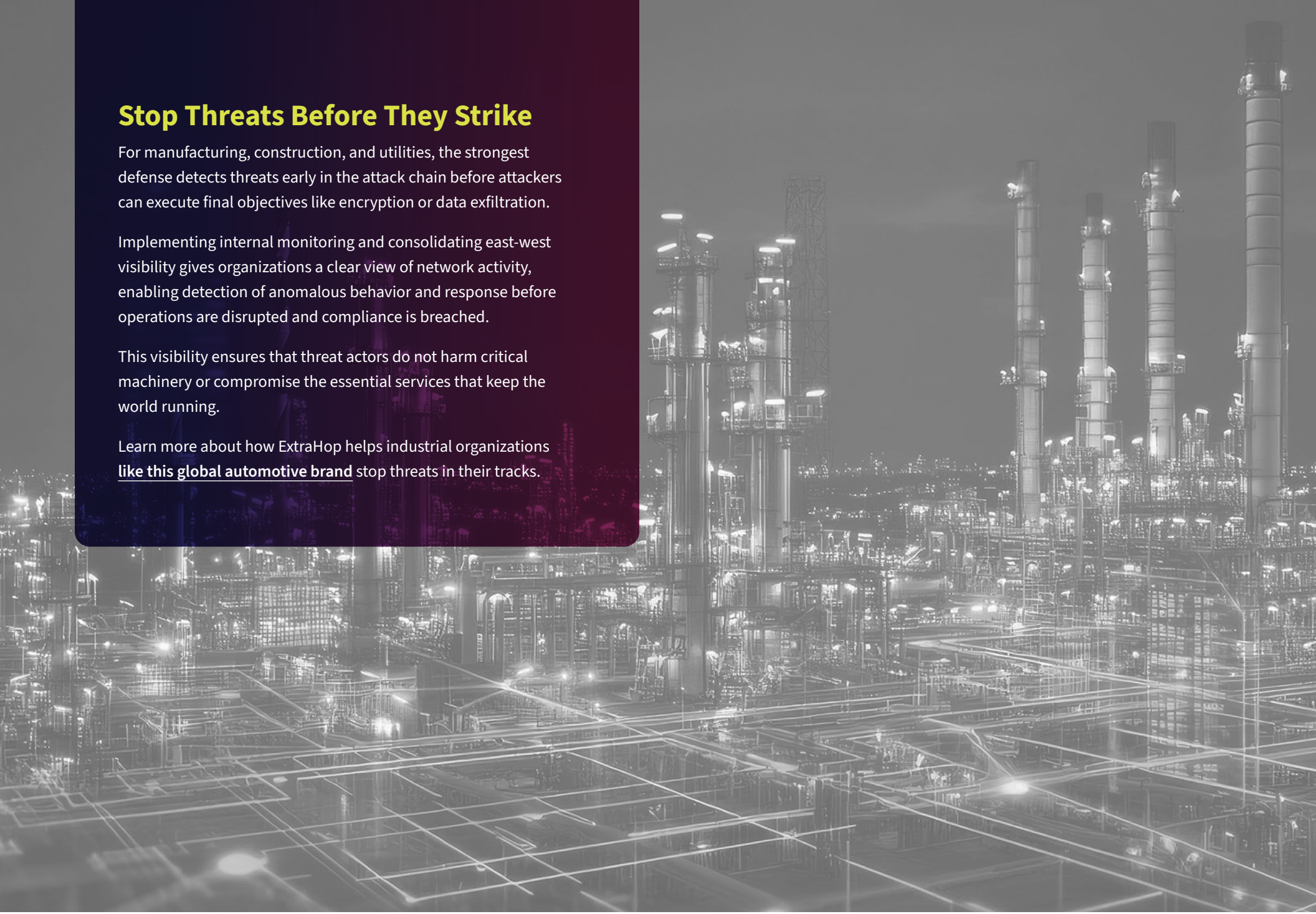
Stop Threats Before They Strike

For manufacturing, construction, and utilities, the strongest defense detects threats early in the attack chain before attackers can execute final objectives like encryption or data exfiltration.

Implementing internal monitoring and consolidating east-west visibility gives organizations a clear view of network activity, enabling detection of anomalous behavior and response before operations are disrupted and compliance is breached.

This visibility ensures that threat actors do not harm critical machinery or compromise the essential services that keep the world running.

Learn more about how ExtraHop helps industrial organizations **like this global automotive brand** stop threats in their tracks.



METHODOLOGY

Data sourced from the 2025 ExtraHop Global Threat Landscape Report.

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®