WHITE PAPER

Top Security Trends for Houston Leaders in 2026

A Houston-First Look at Energy, Healthcare, and Critical Infrastructure

MIGGO

Executive Summary

Houston's position as a hub for energy, healthcare, shipping, and technology makes it both an economic powerhouse and a prime target for cyber adversaries. In 2025, attackers advanced beyond traditional tactics, exploiting vulnerabilities, abusing APIs, and targeting live systems that are increasingly complex, containerized, and AI-driven.

This report highlights five security trends Houston leaders must watch:

The first two to discuss are the targeted infrastructures for security threats.

1. **Oil & Gas:** Vulnerability exploitation is rising, with attackers targeting operational technology and supply chains that underpin global energy.
2. **Healthcare:** Intrusions through vulnerabilities and vendor systems disrupt patient care and highlight the risks of third-party dependencies.

The following trends dive into the evolution of the technological infrastructure paving the way for today and tomorrow's cyber threats.

3. **AI Systems:** Artificial intelligence accelerates both attack and defense, with prompt injection, poisoned models, and runtime manipulation creating new risks.
4. **Supply Chain:** Partner and vendor compromise has doubled, showing how weaknesses in trusted software and services ripple across industries.
5. **Cloud & Hybrid:** Misconfigurations, shadow AI, and runtime exploitation are becoming the dominant risks in multi-environment operations.

Across all five trends, one theme stands out: critical risks are surfacing at runtime. Pre-deployment testing and perimeter defenses remain necessary but are no longer sufficient. Houston organizations must invest in visibility, detection, and response that operate while applications, AI models, and workloads are live.

This report provides a Houston-first view of these national and global threats, translating them into local impact with actionable steps. For business and security leaders preparing for 2026, the path forward requires a blend of industry-specific readiness, vendor vigilance, and continuous runtime protection.

Table of Contents

Houston at the Crossroads of Risk and Resilience

Houston is more than an energy capital. It is also home to the Texas Medical Center, Port Houston, and a rapidly growing technology sector. This concentration of critical infrastructure makes the city a focal point for cyber attackers.

In 2025, attackers refined their techniques across industries. Exploited vulnerabilities, code injection, and API abuse grew as common entry points. Privilege escalation, misuse of credentials, and malicious activity in containerized and serverless environments showed how fast-changing workloads can be compromised before traditional defenses react.

Recent incidents such as the exploitation of SharePoint[1] apps and the compromise of popular open-source NPM[2] packages illustrate this shift. These attacks demonstrate how adversaries are exploiting runtime behaviors in trusted platforms and third-party code, risks that Houston's critical sectors must prepare to confront.

At the same time, AI expanded the stakes on both sides, giving adversaries more speed while helping defenders modernize detection.

Houston's leaders cannot afford to view these as distant risks. They are local, immediate, and growing. This report highlights five key trends shaping Houston's security landscape in 2026. Each section draws from leading industry reports and translates national data into local impact, with actionable steps for organizations on the front lines.

$600B+
Economic output from Houston's energy sector

Texas Medical Center
The largest medical complex in the world

Port Houston
#1 in the U.S. for foreign waterborne tonnage

[1] Miggo Security. SharePoint Apps Under Attack: What You Need to Know About the Latest Vulnerabilities. Miggo Blog, 2025.

[2] Miggo Security. Pwned Debrief: NPM's Debug/Chalk Package Attack Explained. Miggo Blog, 2025.

TREND 1

Oil and Gas: Vulnerabilities as Attackers' Gateway

Energy companies remain a prime target for attackers who exploit weaknesses in live systems. Verizon's DBIR 2025[3] highlights that breaches initiated through vulnerability exploitation are increasing, and that third-party involvement in breaches has doubled year over year. These weaknesses are particularly dangerous in operational technology environments where downtime can have cascading effects.

Sector-specific reporting confirms that oil and gas have become one of the hardest-hit industries. Zscaler's 2025 ThreatLabz report[4] noted some of the steepest year-over-year increases in cyberattacks, with ransomware as one of several tactics used against energy supply chains. Attackers are also focusing more on exfiltrating sensitive data and abusing APIs, rather than relying solely on file encryption.

For Houston, a city at the center of global energy, these numbers translate into operational, economic, and reputational risk. From upstream exploration apps to downstream logistics, vulnerabilities provide attackers with dangerous footholds. Even when patch cycles lag, runtime monitoring can flag exploit behavior, code injection attempts, and abnormal activity in critical systems before attackers achieve their objectives.

Checklist

- [x] Accelerate patching and vulnerability remediation cycles
- [x] Monitor runtime anomalies in your different environments
- [x] Utilize WAF to block exploitation while you patch
- [x] Leverage runtime visibility to effectively understand and prioritize real threats

Supply Chain Risk
Attacks can disrupt global production and transport supply chains

Legacy Systems
Old software and hardware create patching challenges

Data Theft
Exfiltration raises compliance and reputation costs

3. Verizon. 2025 Data Breach Investigations Report (DBIR). Verizon Business, 2025. https://www.verizon.com/business/resources/reports/dbir/

4. Zscaler. ThreatLabz 2025 Ransomware Report. Reported in TechRadar Pro: "US becomes ransomware capital of the world as attacks rise by almost 150 percent." TechRadar, 2025.

TREND 2

Healthcare Under Siege: Intrusions and Patient Impact

Healthcare continues to face sustained system intrusions that directly impact patient care. Verizon's DBIR 2025 shows that nearly half of breaches in healthcare involve system intrusion patterns, with vulnerability exploitation accounting for about 20% of initial access across all industries. This trend is especially concerning due to the prevalence of IoMT devices and reliance on third-party systems. In addition, many hospitals still rely on brownfield systems which create persistent blind spots and slow down remediation efforts. Health-ISAC[5] adds that supply chain compromise is now a top-five healthcare threat, underscoring how dependent the sector is on external vendors and IoMT devices.

High-profile incidents, including Change Healthcare and Ascension, disrupted scheduling, billing, and hospital operations nationwide. These events illustrate that attackers are not limited to one tactic: they exploit vulnerabilities, steal credentials, and misuse vendor access, with data theft and extortion among the most common outcomes.

For Houston, home to the Texas Medical Center, the stakes are especially high. Disruption here could affect not just local hospitals but the broader healthcare ecosystem. Runtime visibility across IoMT devices and third-party vendor systems is essential to spot unusual behavior, including malicious code execution, unauthorized access attempts, or data exfiltration, before care delivery is interrupted.

> **Vulnerability exploitation accounts for 20% of breach entry points**

Checklist

- [ ] Deploy runtime monitoring on IoMT and vendor-connected systems
- [ ] Patch and monitor edge devices for exploit activity
- [ ] Encrypt sensitive data and monitor for unusual outbound traffic

Patient Safety
Intrusions can disrupt scheduling, imaging, and critical workflows

Financial Losses
Billing and payment systems are high-value targets

Vendor Exposure
IoMT and third-party vendors expand the attack surface

[5] Health-ISAC. 2025 Annual Threat Report. Health Information Sharing and Analysis Center, 2025

TREND 3

AI Factor: Faster Attacks and Faster Defense

AI is reshaping cybersecurity. Deloitte[6] reports that AI is making phishing campaigns more persuasive and accelerating exploit discovery. Arctic Wolf[7] data shows 73% of organizations already deploy AI in security, and 99% of leaders say it will influence budget and purchasing decisions in the year ahead.

While AI strengthens defenses, it also introduces runtime risks: poisoned models, prompt injection attacks, and AI-generated code that behaves unpredictably once deployed. For Houston's hospitals, energy operators, and logistics hubs, AI adoption means new attack surfaces as well as new opportunities. Because many AI failures and manipulations only emerge during live use, runtime controls are essential to keep models, pipelines, and outputs safe in production.

> **99% of leaders say AI will influence cyber budgets**

Checklist

- [x] Monitor prompts, outputs, and data flows in production
- [x] Apply identity and secrets management to AI pipelines
- [x] Use human review loops to validate AI-driven decisions
- [x] Monitor drifts in production to expose risky AI behavior

Energy
AI-driven optimization adds runtime complexity

Healthcare
AI in imaging and triage expands attack surfaces

Logistics
AI routing and forecasting create data dependencies

6. Deloitte. Cyber Threat Trends Report 2025. Deloitte, 2025. Available at: https://www.deloitte.com/us/en/services/consulting/articles/cybersecurity-report-2025.html

7. Arctic Wolf. AI in Cybersecurity Survey Results 2025. Reported in TechRadar Pro: "AI is taking over cybersecurity—but businesses still know the risks." TechRadar, 2025.

TREND 4

Supply Chain andThird-Party Risk

Third-party compromise is growing. Verizon notes third-party involvement in breaches doubled year over year. Health-ISAC flags supply chain breaches as a top concern, citing ripple effects from vendor software vulnerabilities and zero-day exploitation events.

For Houston, vendor reliance spans hospitals, billing systems, imaging providers, industrial control vendors, and energy contractors. A breach in one supplier can cascade into citywide disruptions. Even when vendor code appears safe pre-deployment, runtime telemetry shows whether it behaves securely once integrated into critical environments.

Third-party involvement in breaches doubled YoY

Checklist

- [ ] Require vendors to provide runtime telemetry and logs
- [ ] Stage and validate updates before promotion
- [ ] Establish emergency credential rotation with suppliers

Hospitals
Payment and imaging vendors create high-risk exposure

Energy
Contractors and OT software suppliers are often overlooked

Cascading Disruption
A single breach can ripple across multiple sectors

TREND 5

Cloud and Hybrid Environments: Identity and Shadow AI Pressure

Cloud and hybrid environments continue to expand the attack surface for Houston organizations. IBM's 2025 outlook[8] warns that shadow AI is emerging as a major enterprise risk, creating unmanaged workloads and unexpected data exposures. Verizon's report also highlights the growing role of vulnerability exploitation in cloud breaches, especially when configuration drift and unpatched services are involved.

For Houston hospitals, energy firms, and port operators, the hybrid reality is here: most are familiar with SaaS and vendor-hosted platforms that must all be defended as one environment. Yet, there are applications and data centers that are deployed in the organization's environment that needs security in its own way. Misconfigurations, API misuse, and shadow AI services often introduce risks that surface only at runtime. Real-time monitoring of workloads and identities is essential to detect abnormal activity and contain threats before they spread.

Shadow AI emerged as a top enterprise risk in 2025

Checklist

- [ ] Detect and control shadow AI services and unsanctioned workloads
- [ ] Continuously validate workloads for vulnerability exploitation
- [ ] Monitor runtime activity for API misuse and privilege escalation attempts

Hybrid Risk
Services and workloads span multiple environments

Unmanaged AI
Shadow AI introduces hidden workloads and vulnerabilities

Misconfigurations
Drift and weak configurations create runtime exposures

[8] IBM. Cybersecurity Predictions 2025. IBM Think, 2025.
https://www.ibm.com/think/insights/cybersecurity-trends-ibm-predictions-2025

Building a Houston-First Security Strategy

From pipelines to patient care, Houston's infrastructure is both vital and vulnerable. Threats increasingly appear at runtime, when applications, AI systems, and vendor integrations are live and interacting. Pre-deployment checks and perimeter defenses are necessary, but not sufficient.

Resilience for 2026 means combining sector-specific readiness, supply chain vigilance, AI governance, cloud identity, and above all, visibility into how systems behave in real time.

Domain	Key Risk	Action Now
Oil and Gas	Vulnerability exploitation	Patch faster, monitor SCADA anomalies
Healthcare	Ransomware and extortion	Tabletop downtime, encrypt at rest
AI Systems	Prompt injection, poisoned models	Monitor outputs, apply identity to pipelines
Supply Chain	Vendor compromise	Require telemetry, validate updates
Cloud/Hybrid	Shadow AI, identity sprawl	Identity-first controls, detect shadow AI

Miggo's Perspective: Securing Runtime in the Age of AI

The trends outlined in this report point to one reality: Houston organizations are under pressure from attackers who exploit vulnerabilities that only appear once systems are running. Whether it is an AI model that uses tools in unexpected ways, a third-party library introducing hidden backdoors, or just classic threats and exploits in web applications, the common thread is runtime risk.

Security, however, cannot stop at pre-deployment testing. Applications and AI systems need full lifecycle coverage: validated before release and continuously protected in production. Static scans and shift-left testing reduce known risks, but they cannot anticipate how applications, APIs, or AI models will behave under live conditions.

Miggo was built to close that gap. Miggo maps live code paths and dependencies, showing where vulnerabilities exist and how they can be reached. By focusing on exploitability proof, Miggo distinguishes real threats from noise, prioritizing the risks that matter most. And through WAF Copilot, Miggo turns that runtime evidence into precise, app-specific shields that can block attacks with confidence. In AI-driven environments, this same approach tracks prompt interactions and model behavior to catch poisoning or misuse in real time. The result: organizations can know, prove, and shield against runtime threats - across both traditional applications and AI systems.

For Houston leaders preparing for the challenges of 2026, this means critical operations can stay resilient even when attackers bypass other defenses. Runtime protection transforms into a closed loop: applications are secured before deployment and continuously safeguarded after, ensuring that even if attackers get in, they cannot achieve their objectives.