# Annual Threat Forecast – 2026

## Executive Summary

Prepared By

Castellum Labs

# Table Of Content

# Foreword

As we stand at the threshold of 2026, the cybersecurity landscape has undergone a tectonic shift. We have transitioned from the era of "GenAI experimentation" in 2024 and 2025 to the era of Agentic AI - where autonomous systems, both malicious and defensive, make decisions in milliseconds without human intervention.

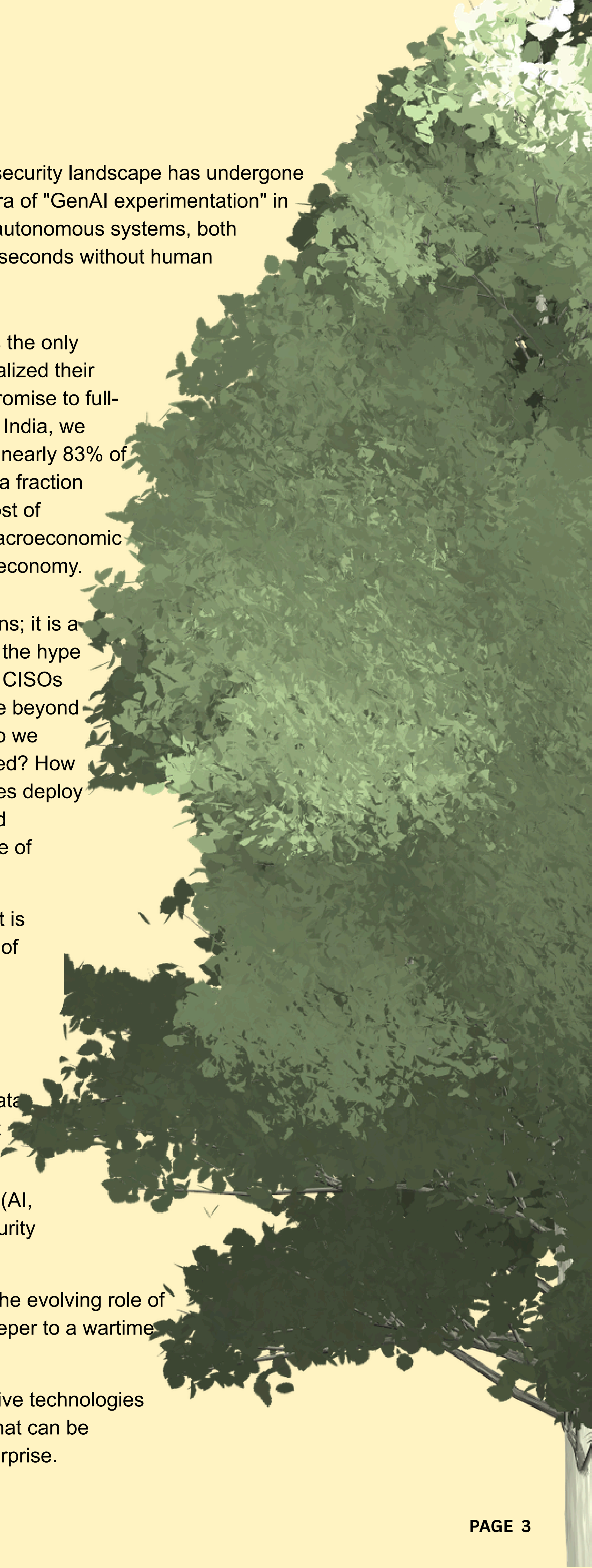
The previous year, 2025, taught us that speed is the only metric that truly matters. Attackers have industrialized their operations, collapsing the time from initial compromise to full-scale data extortion from days to mere hours. In India, we witnessed a digital ecosystem under siege, with nearly 83% of organizations facing significant threats, yet only a fraction reporting true "cyber readiness." Globally, the cost of cybercrime is no longer just a line item; it is a macroeconomic force, projected to drain trillions from the global economy.

This report is not merely a collection of predictions; it is a strategic roadmap. Our objective is to dismantle the hype surrounding emerging technologies and provide CISOs with actionable, real-world intelligence. We move beyond the "if" and "when" to address the "how": How do we defend an identity that can be perfectly deepfaked? How do we govern "Shadow AI" agents that employees deploy in secret? And most importantly, how do we build organizational resilience that survives the "Triage of Doom"?

The 2026 Forecast is designed to turn the tide. It is time to move from reactive firefighting to a state of Continuous Exposure Management, where the defender finally holds the advantage of speed.

## Objective of the Report

- Contextualize 2025 Realities: Analyze the data from the past year to understand the current baseline of threats in India and the World.
- Define 2026 Pillars: Identify the core drivers (AI, Identity, Supply Chain) that must dictate security budgets and board-level conversations.
- Empower the CISO: Provide a blueprint for the evolving role of the security leader - from a technical gatekeeper to a wartime intelligence chief.
- Operationalize Innovation: Separate disruptive technologies from fleeting trends, offering "Quick Wins" that can be executed immediately to safeguard the enterprise.



# EXECUTIVE SUMMARY

## Drivers of Threats and Risks in 2026

The 2026 threat landscape is no longer defined by human-to-human conflict, but by the Velocity of the Autonomous. The following three drivers are rewriting the security playbook:

- **Agentic AI & The "Shadow Agent" Crisis:** 2026 marks the shift from Generative AI to Agentic AI - autonomous systems that "act" rather than just "talk". Attackers deploy AI agents to navigate internal networks and exfiltrate data without human intervention.

- **The Identity Erosion (Deepfake Industrialization):** Identity has become the only perimeter, but it is currently crumbling. Automated "CEO Fraud" is now powered by flawless, real-time AI audio and video deepfakes.

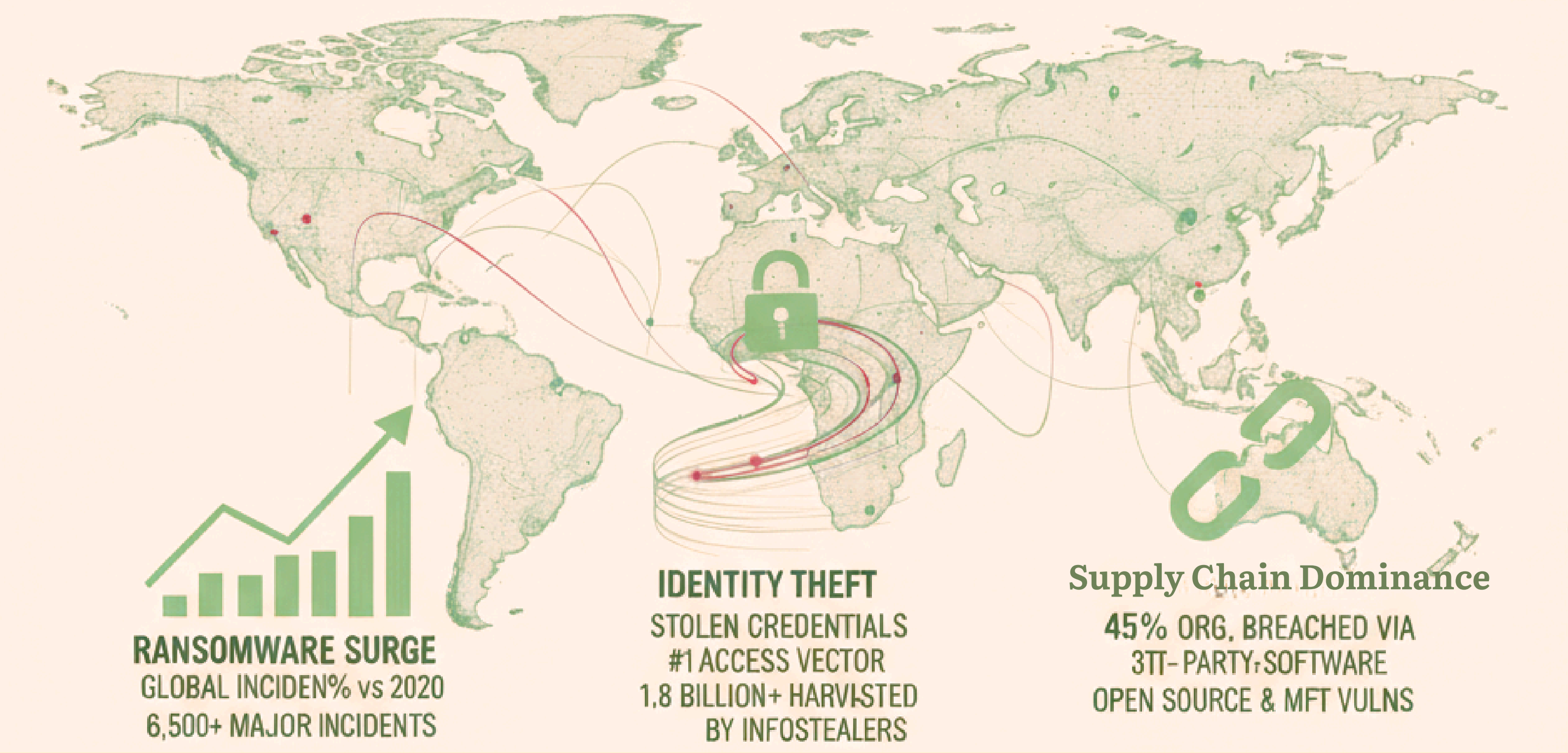
- **Machine Identity Sprawl:** The ratio of machine and agent identities to human identities has reached 82:1 in 2026, rendering traditional MFA-based trust models obsolete.

- **Geopolitical Fragmentation:** Cybersecurity has become a tool of national sovereignty following a sharp 2025 increase in state-sponsored attacks on critical infrastructure like power grids and water systems.

- **Cyber Inequity:** A widening gap exists where smaller nations and mid-market companies are increasingly becoming "digital collateral" in larger geopolitical crossfires.

- **Autonomous Insider Threats:** Compromised AI tools are being effectively turned into autonomous threats that can escalate privileges independently.

# 2025 Retrospective: The Baseline for 2026



## Global Retrospective

- **The Ransomware Surge:** Global ransomware incidents surged by 355% compared to 2020 levels, with nearly 6,500 major incidents recorded in 2025 alone.

- **Identity Theft:** Stolen credentials became the #1 initial access vector, fueled by "Infostealers" that harvested over 1.8 billion credentials globally.

- **Supply Chain Dominance:** Nearly 45% of global organizations experienced a breach originating from a third-party vendor or software supply chain (e.g., vulnerabilities in Open Source and Managed File Transfer platforms).

- **The Cost of Inaction:** The average cost of a healthcare breach crossed $9.7 million, marking the 14th consecutive year as the most expensive sector for cyber incidents.

## India Retrospective

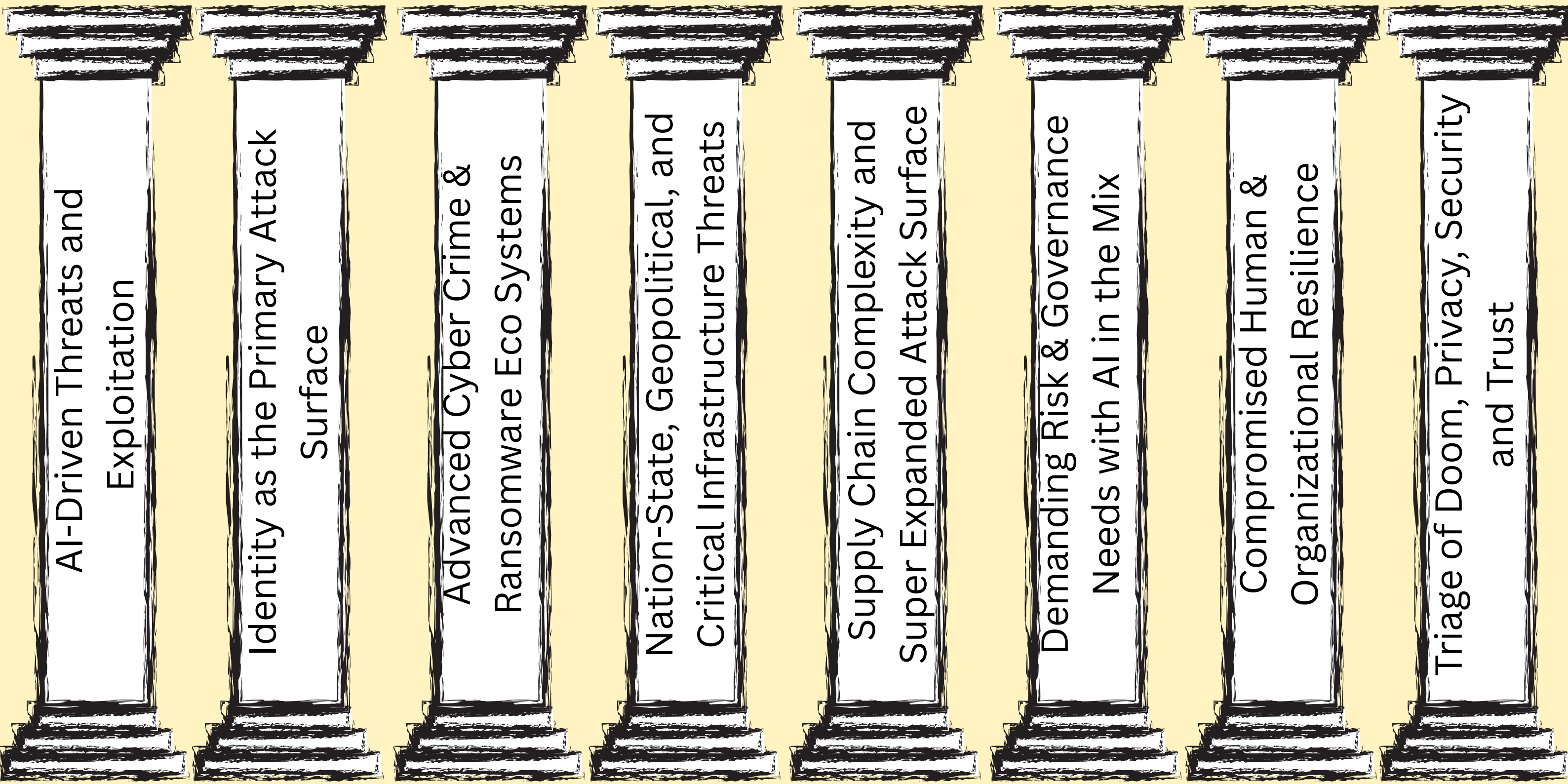
- **Malware Explosion:** India witnessed over 369 million malware detections across nearly 8.5 million endpoints, highlighting a critical inflection point in digital vulnerability.

- **Sector Targets:** The BFSI (Banking & Finance) and Healthcare sectors remained the most targeted, with digital payment (UPI) fraud resulting in monthly losses estimated at thousands of crores.

- **Preparedness Gap:** A startling 73% of Indian organizations were unaware if they had been attacked in 2025, and 57% lacked basic cyber hygiene practices despite the implementation of the Digital Personal Data Protection Act (DPDPA).

- **Regional Hotspots:** Telangana, Tamil Nadu, and Delhi emerged as the highest targeted regions due to their dense concentration of tech hubs and digital infrastructure. .

# CORE PILLARS For 2026



AI-Driven Threats and Exploitation

Identity as the Primary Attack Surface

Advanced Cyber Crime & Ransomware Eco Systems

Nation-State, Geopolitical, and Critical Infrastructure Threats

Supply Chain Complexity and Super Expanded Attack Surface

Demanding Risk & Governance Needs with AI in the Mix

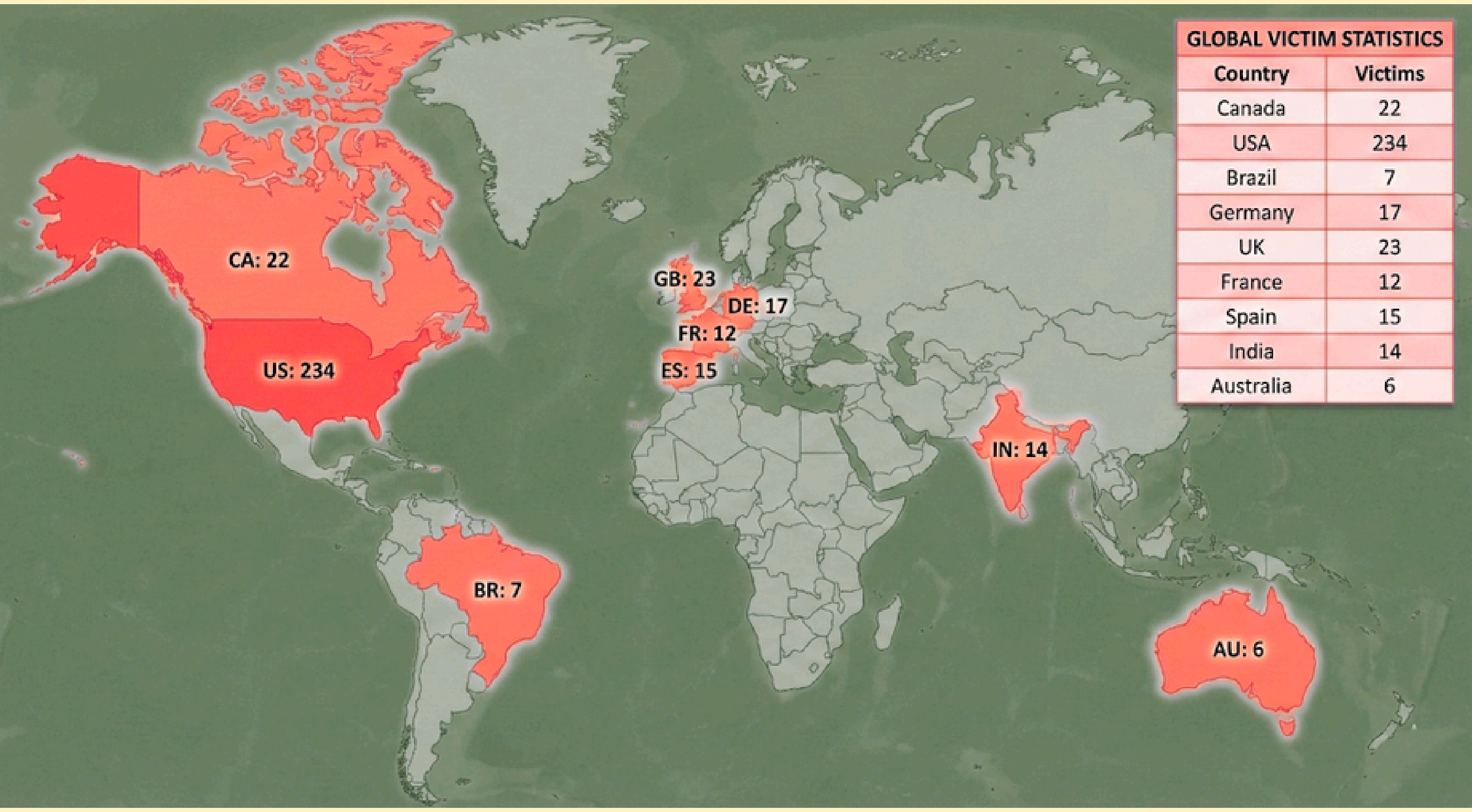
Compromised Human & Organizational Resilience

Triage of Doom, Privacy, Security and Trust

## PREDICT THE *today* THREATS

# RASOMWARE LANDSCOPE

*The ransomware economy in 2026 has transitioned from a fragmented "wild west" into a highly disciplined, Industrialized Extortion Machine. Attacks are now faster, more targeted, and increasingly automated through the use of Agentic AI.*



GLOBAL VICTIM STATISTICS

| Country | Victims |
|---|---|
| Canada | 22 |
| USA | 234 |
| Brazil | 7 |
| Germany | 17 |
| UK | 23 |
| France | 12 |
| Spain | 15 |
| India | 14 |
| Australia | 6 |

***Ransomware Victims in January 2026***

## MOST TARGETED SECTORS

1. **Manufacturing**
2. **Healthcare**
3. **IT Service**

## MOST ACTIVE THREAT ACTORS

1. **Qilin**
2. **Akira**
3. **Ransomhub**

## GLOBAL FINANCIAL LOSS

**$57 billion**

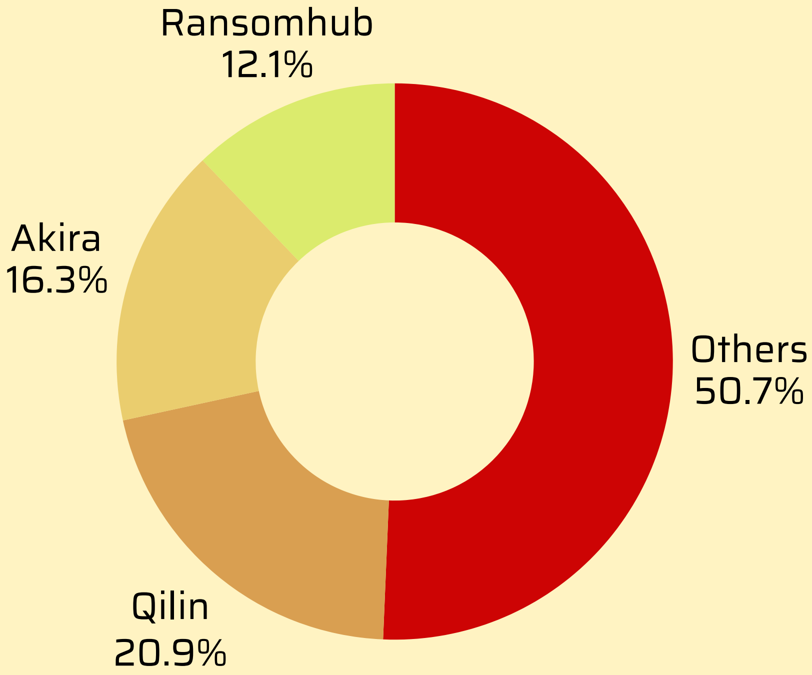
## 1. Threat Actor Analysis: 2025 vs. 2026

By 2026, ransomware has matured into a highly structured, corporate-grade extortion industry, moving away from simple "smash-and-grab" tactics toward strategic, high-impact operations.

### The New Operational Model

- Ransomware-as-a-Corporate-Service (RaCS): The ecosystem has industrialized, with over 124 distinct named groups operating in a manner similar to professional cartels, utilizing specialized affiliates and automated victim selection.
- Encryption-less Extortion: A significant pivot has occurred toward "pure extortion" where attackers eschew encryption entirely to avoid detection, focusing solely on data exfiltration and the threat of public disclosure.
- AI-Driven Negotiation: Attackers now utilize intelligent bots to analyze exfiltrated data, calculate optimal ransom amounts, and conduct real-time negotiations with victims.
- Triple Extortion: Beyond encryption and data theft, attackers now add third layers of pressure, such as launching DDoS attacks or directly harassing a victim's customers and partners to force payment.

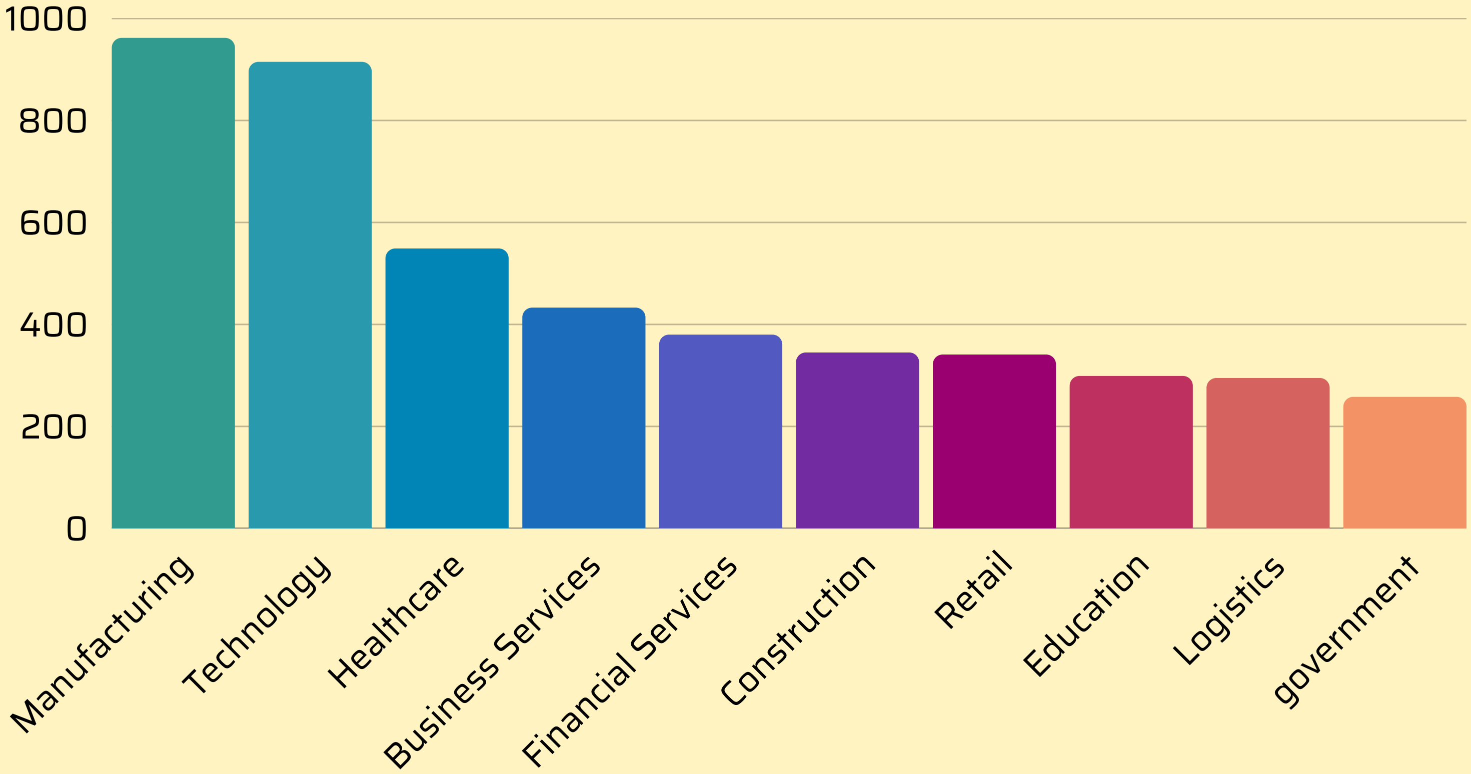
### Top Ransomware Group in 2025

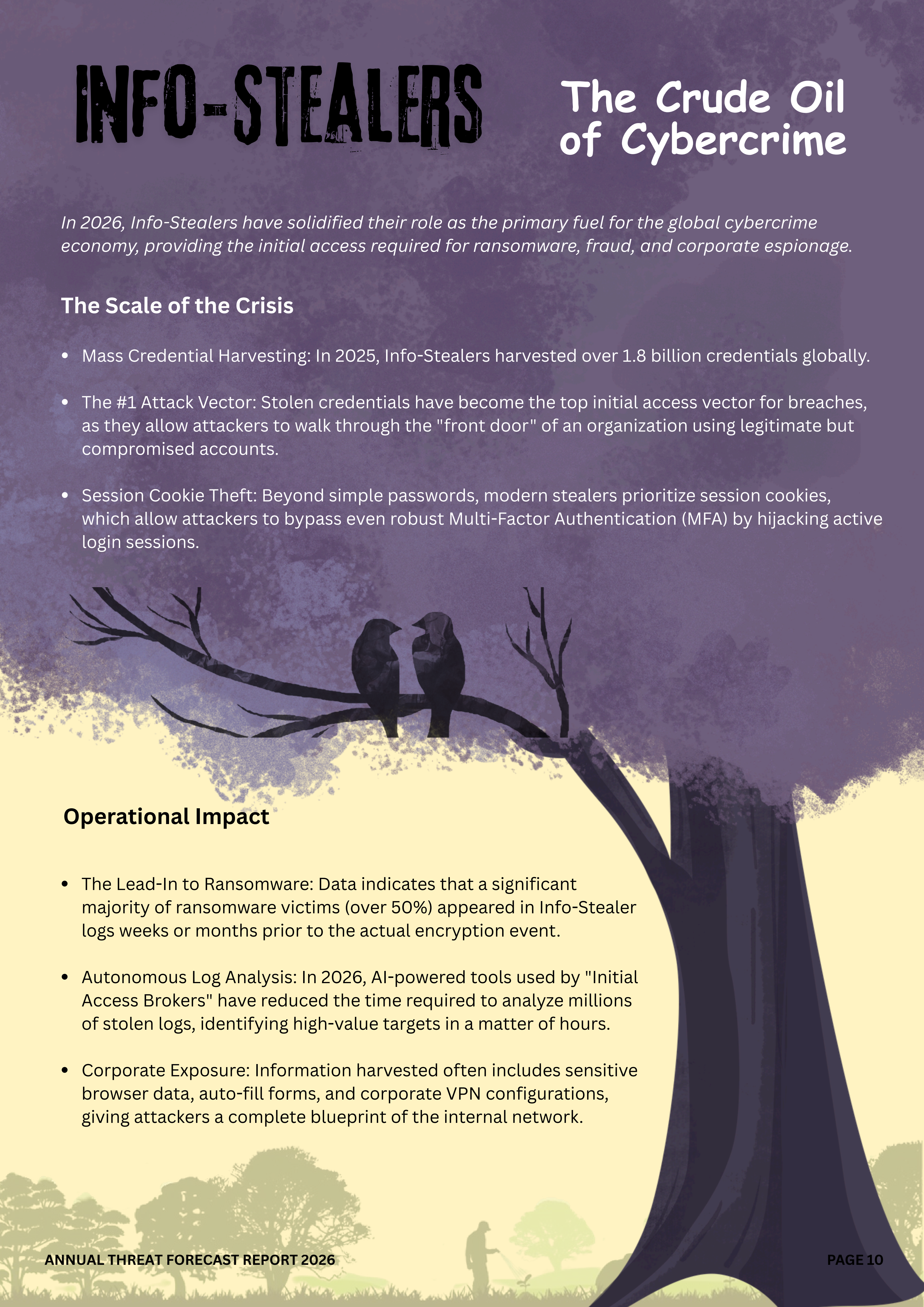


## 2. Sector Targeting: The Shift in Pressure Points

- Primary Targets: Healthcare, Manufacturing, and Energy/Utilities remain the most targeted sectors due to the critical nature of their uptime and the immediate life-safety or supply chain risks associated with their downtime.
- Global Losses: Annual global ransomware losses are projected at $57 billion for 2026.
- Cost of Breach: The average cost of a healthcare breach is projected to reach $12.6 million by 2026, while financial sector breaches are expected to exceed $6.08 million.
- Payment Trends: While the number of incidents may show signs of stabilization, the financial impact per attack is rising sharply, with average payments reaching $3.6 million+.

### Most Affect Sector by Ransomware group in 2025





# INFO-STEALERS

# The Crude Oil of Cybercrime

*In 2026, Info-Stealers have solidified their role as the primary fuel for the global cybercrime economy, providing the initial access required for ransomware, fraud, and corporate espionage.*

## The Scale of the Crisis

- Mass Credential Harvesting: In 2025, Info-Stealers harvested over 1.8 billion credentials globally.
- The #1 Attack Vector: Stolen credentials have become the top initial access vector for breaches, as they allow attackers to walk through the "front door" of an organization using legitimate but compromised accounts.
- Session Cookie Theft: Beyond simple passwords, modern stealers prioritize session cookies, which allow attackers to bypass even robust Multi-Factor Authentication (MFA) by hijacking active login sessions.

## Operational Impact

- The Lead-In to Ransomware: Data indicates that a significant majority of ransomware victims (over 50%) appeared in Info-Stealer logs weeks or months prior to the actual encryption event.
- Autonomous Log Analysis: In 2026, AI-powered tools used by "Initial Access Brokers" have reduced the time required to analyze millions of stolen logs, identifying high-value targets in a matter of hours.
- Corporate Exposure: Information harvested often includes sensitive browser data, auto-fill forms, and corporate VPN configurations, giving attackers a complete blueprint of the internal network.

# AI The HEADACHE or HYPE

*2026 marks the definitive shift from Generative AI experimentation to the era of Agentic AI, where autonomous systems make high-speed decisions without human intervention. This transition has turned AI from a productivity tool into a complex security headache.*

## The Rise of Agentic Threats

- Agentic AI Predator Swarms: Attackers now deploy autonomous AI agents that map an entire enterprise attack surface in minutes, identifying zero-days that human teams would take weeks to find.
- Autonomous Insider Threats: Employees unknowingly deploy "Shadow Agents" to automate tasks, creating invisible pipelines for sensitive company data to leak externally.
- Polymorphic Exploits: AI is used to rewrite malware code on the fly to evade EDR (Endpoint Detection and Response) signatures, rendering traditional detection-based security obsolete.

## Structural Vulnerabilities

- "Vibe Coding" Risks: The surge in AI-generated code by non-developers (Vibe Coding) is injecting massive security debt and unvetted libraries into production environments.
- Shadow AI Proliferation: Organizations are seeing a massive 890% increase in GenAI traffic, much of which operates in the enterprise "blind spot".
- Model Poisoning: The AI supply chain is now vulnerable to "Model Poisoning" and "Prompt Injection" through third-party AI integrations.

## The Defensive Mandate

- AI-SPM: CISOs must move toward AI Security Posture Management (AI-SPM) to govern autonomous agents and secure AI traffic.
- Machine-Speed Defense: Because attackers operate at "the Velocity of the Autonomous," defensive systems must also be capable of millisecond decision-making to remain resilient.

# CISO Priority & Operating Model

*In 2026, the CISO role undergoes its most significant transformation yet, moving from a technical gatekeeper to a Wartime Intelligence Chief. The operating model shifts from "defending the perimeter" to "managing continuous exposure" in a machine-speed environment.*

## CISO Strategic Priority Matrix 2026

| S.no | Priority | Strategy | Success Metric |
|---|---|---|---|
| 1. | **Identity Resilience** | Move beyond legacy MFA to Phishing-Resistant MFA (FIDO2) and Continuous Session Validation. | **> 85%** of identities under phishing-resistant MFA. |
| 2. | **Exposure Management** | Implement Continuous Threat Exposure Management (CTEM) to replace quarterly scanning. | **MTTR < 48 Hours** for critical edge assets (vs. industry average of 5–7 days). |
| 3. | **AI-Native SOC** | Deploy Agentic AI to automate triage and containment; shift human talent to high-level strategy. | **Detection Breakout Time < 30 Minutes** (Current attacker average is ~50 mins). |
| 4. | **Cloud Sovereignty** | Secure the Management Plane; treat cloud misconfigurations as a "P0" prevention priority. | **Zero** high-risk unauthenticated cloud APIs; 100% P0 remediation within 4 hours. |
| 5. | **Supply Chain Trust** | Operationalize Continuous Assurance for vendors; move from surveys to real-time control validation. | **> 60% of critical vendors providing continuous telemetry (Industry avg: 15-20%).** |

## The Strategic Shift: From Preventative to Validative

*To survive 2026, the CISO's focus must transition away from periodic testing toward a continuous validation model*

- **From VAPT to CTEM:** Continuous Threat Exposure Management (CTEM) replaces legacy periodic testing.

- **Continuous Automated Red Teaming (CART):** Security teams must employ autonomous red teaming to validate defensive posture in real-time, matching the speed of AI-driven attackers.

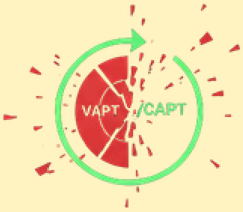
- **Human Risk Management:** Shifting to Behavioral Defense, focusing on psychological resilience and "Out-of-Band" verification for high-value transactions.

- **Unified AI Governance:** Establishing an AI-SPM framework to oversee the 890% increase in GenAI traffic and "Shadow Agents" operating in the enterprise blind spot.

# Emerging Technologies & Investment Focus

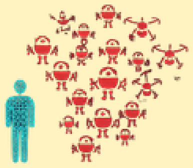
*As the threat landscape shifts toward autonomous and AI-driven attacks, security technology in 2026 consolidates around "The Vanguard" - a set of emerging solutions designed for machine-speed validation and governance.*

## Core Investment Areas



**CTEM and CART:** Investment is shifting from traditional point-in-time testing (VAPT) to Continuous Threat Exposure Management (CTEM). Organizations are deploying Continuous Automated Red Teaming (CART) to provide real-time validation of their defensive posture.

**AI-SPM Platforms:** With a projected 890% increase in GenAI traffic, organizations are investing in AI Security Posture Management (AI-SPM) to govern autonomous "Shadow Agents" and secure invisible data pipelines.



**Non-Human Identity (NHI) Management**: As the ratio of machine-to-human identities reaches 45:1 (up to 82:1 in some sectors), new identity platforms focus on securing over-privileged bots and service accounts.

**Post-Quantum Cryptography (PQC):** To counter "Harvest Now, Decrypt Later" strategies, forward-leaning enterprises are beginning the "Quantum Imperative" - migrating sensitive data to Quantum-Resistant Encryption.

## The Strategic Advantage

**Validated Resilience:** Organizations that invest in continuous validation (CTEM) are projected to be 3× less likely to suffer a successful breach by the end of 2026 compared to those relying on legacy models.

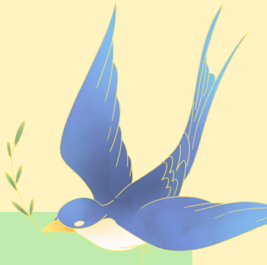
**Consolidation:** The market is moving toward "The Vanguard" of integrated security platforms that unify identity, AI governance, and exposure management into a single defensive fabric.

# Executive Takeaway & 2026 Outlook

*The defining challenge of 2026 is the transition from human-managed security to validated resilience at machine speed. As the "Velocity of the Autonomous" becomes the new standard for conflict, the enterprise must evolve or face digital obsolescence.*

## Core Strategic Mandates

- **The Governance of Autonomy:** Organizations must move beyond blocking AI to actively governing Agentic AI and "Shadow Agents" through robust AI-SPM frameworks.
- **Identity as the Final Frontier:** With human and machine identities reaching a ratio of up to 82:1, the focus must shift to securing Non-Human Identities (NHIs) and defending against industrialized deepfakes.
- **Continuous Validation over Compliance:** Success in 2026 is measured by Continuous Threat Exposure Management (CTEM) and real-time validation via Continuous Automated Red Teaming (CART) rather than periodic checklists.
- **Supply Chain Vigilance:** Security is now only as strong as the worst vendor's AI model; securing the "AI Supply Chain" against model poisoning is critical.



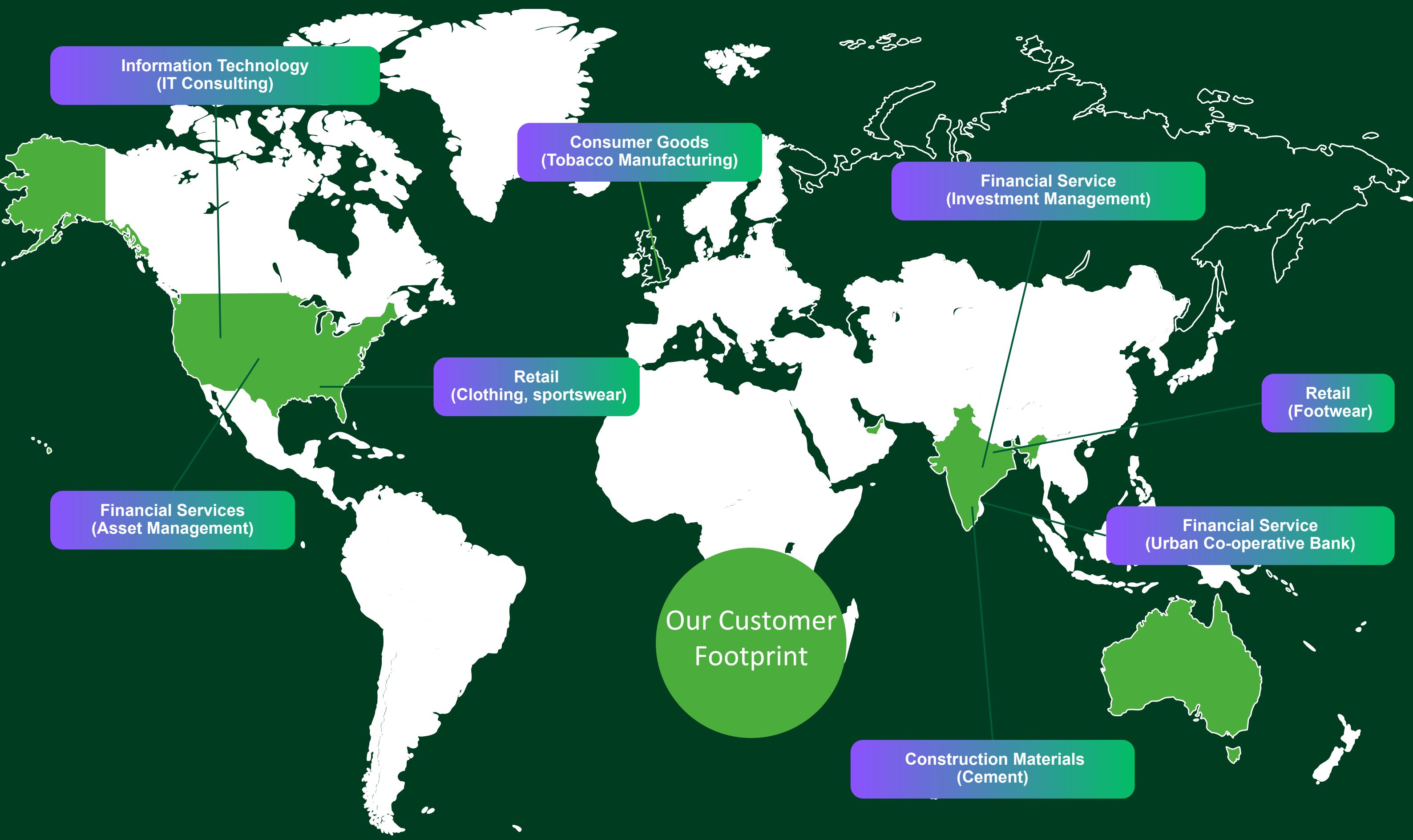
## Final Word

**Cybersecurity has officially transitioned from a technical back-office function to a board-level survival strategy. The "Liability Shift" now places direct legal responsibility on CISOs and Boards for "AI Malpractice" and data failures. Those who prioritize Quantum-Resistant Encryption, behavioral human defense, and autonomous response will not only survive the "Triage of Doom" but convert security into a durable competitive advantage.**

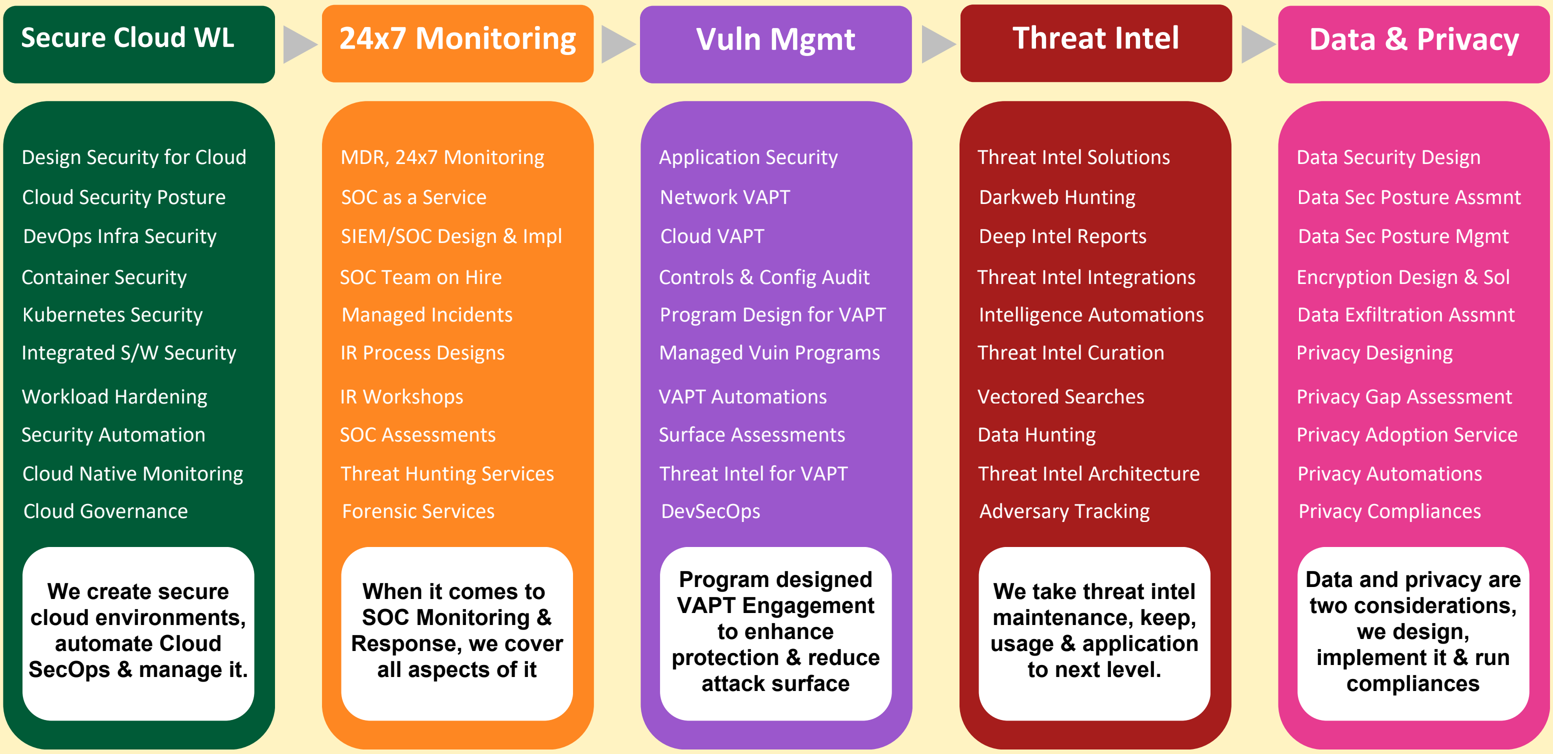
## About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

## 100's of Satisfied Customers Across the Globe!


Information Technology (IT Consulting)
Consumer Goods (Tobacco Manufacturing)
Financial Service (Investment Management)
Retail (Clothing, sportswear)
Retail (Footwear)
Financial Services (Asset Management)
Financial Service (Urban Co-operative Bank)
Our Customer Footprint
Construction Materials (Cement)

# Cyber Security Portfolio



**Secure Cloud WL**

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

**We create secure cloud environments, automate Cloud SecOps & manage it.**

**24x7 Monitoring**

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

**When it comes to SOC Monitoring & Response, we cover all aspects of it**

**Vuln Mgmt**

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuln Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

**Program designed VAPT Engagement to enhance protection & reduce attack surface**

**Threat Intel**

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

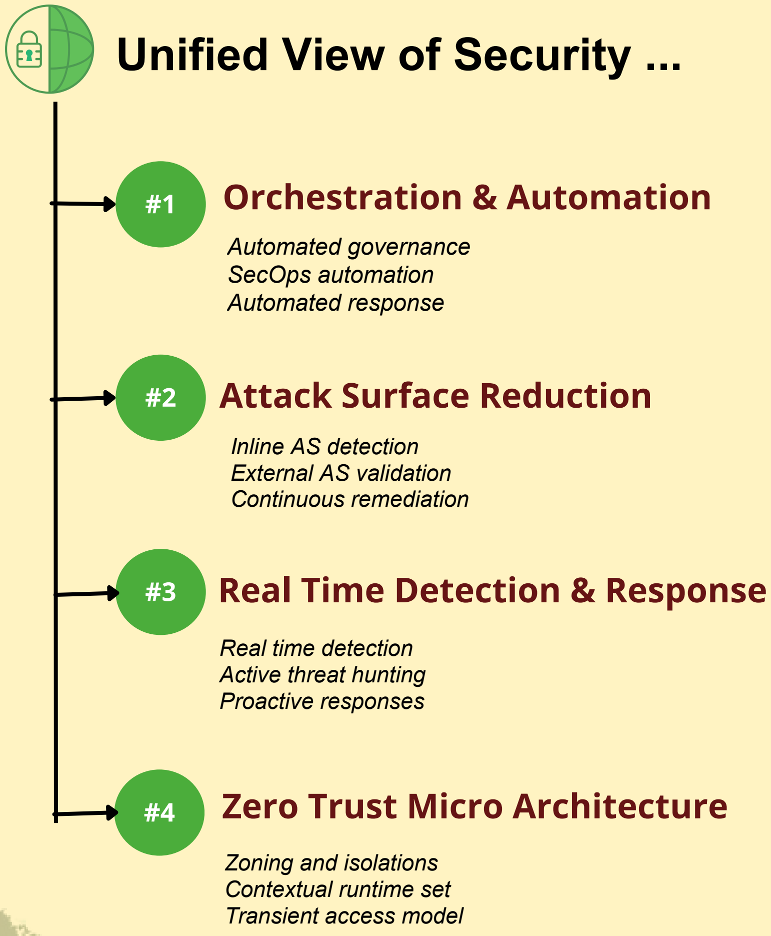
**We take threat intel maintenance, keep, usage & application to next level.**

**Data & Privacy**

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

**Data and privacy are two considerations, we design, implement it & run compliances**

## Unified View of Security ...



### #1 Orchestration & Automation

*Automated governance*
*SecOps automation*
*Automated response*

### #2 Attack Surface Reduction

*Inline AS detection*
*External AS validation*
*Continuous remediation*

### #3 Real Time Detection & Response

*Real time detection*
*Active threat hunting*
*Proactive responses*

### #4 Zero Trust Micro Architecture

*Zoning and isolations*
*Contextual runtime set*
*Transient access model*

## Castellum Labs

www.castellumlabs.com
Castellum Labs
reach@castellumlabs.com
+91 8639953505