CROWDSTRIKE

ЭРА ИИ-УГРОЗ: КАК CROWDSTRIKE ЗАЩИЩАЕТ ОТ АТАК БУДУЩЕГО

CrowdStrike 2025 Global Threat Report

51 sec — the fastest recorded eCrime breakout time
150% increase in China-nexus activity
79% of detections were malware-free

ЧТО ТАКОЕ «ИИ-УГРОЗЫ»

- Prompt Injection — заражение модели через ввод
- Data Poisoning — искажение обучающих данных
- Model Exfiltration — кража/копирование модели и весов
- Hallucination Attacks — манипуляция контекстом и выводами

Secure AI Agent and App Interactions

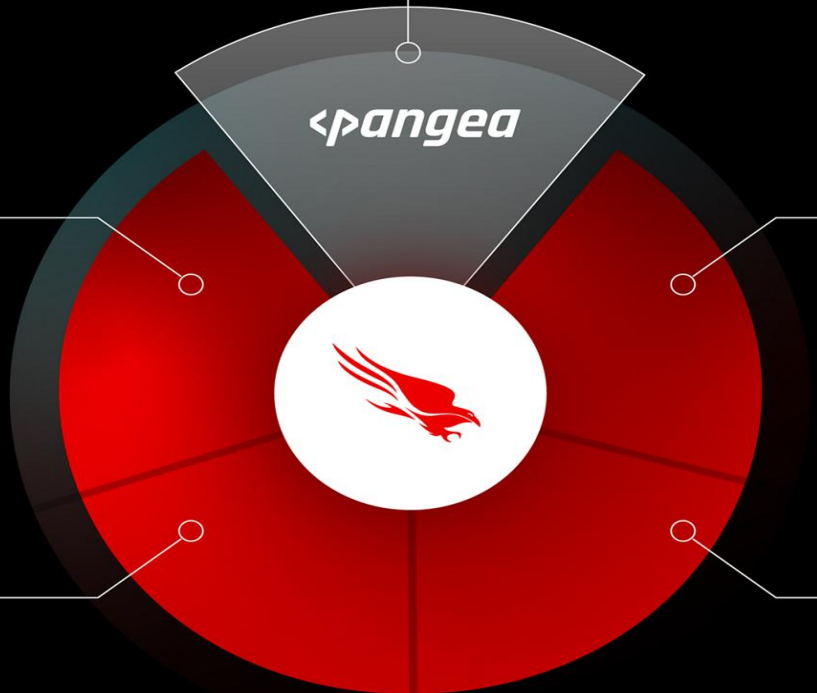
from development to workforce usage

Secure Cloud AI Apps

across models, libraries, and APIs

Discover Shadow AI

and identify asset exposure across on-prem and cloud

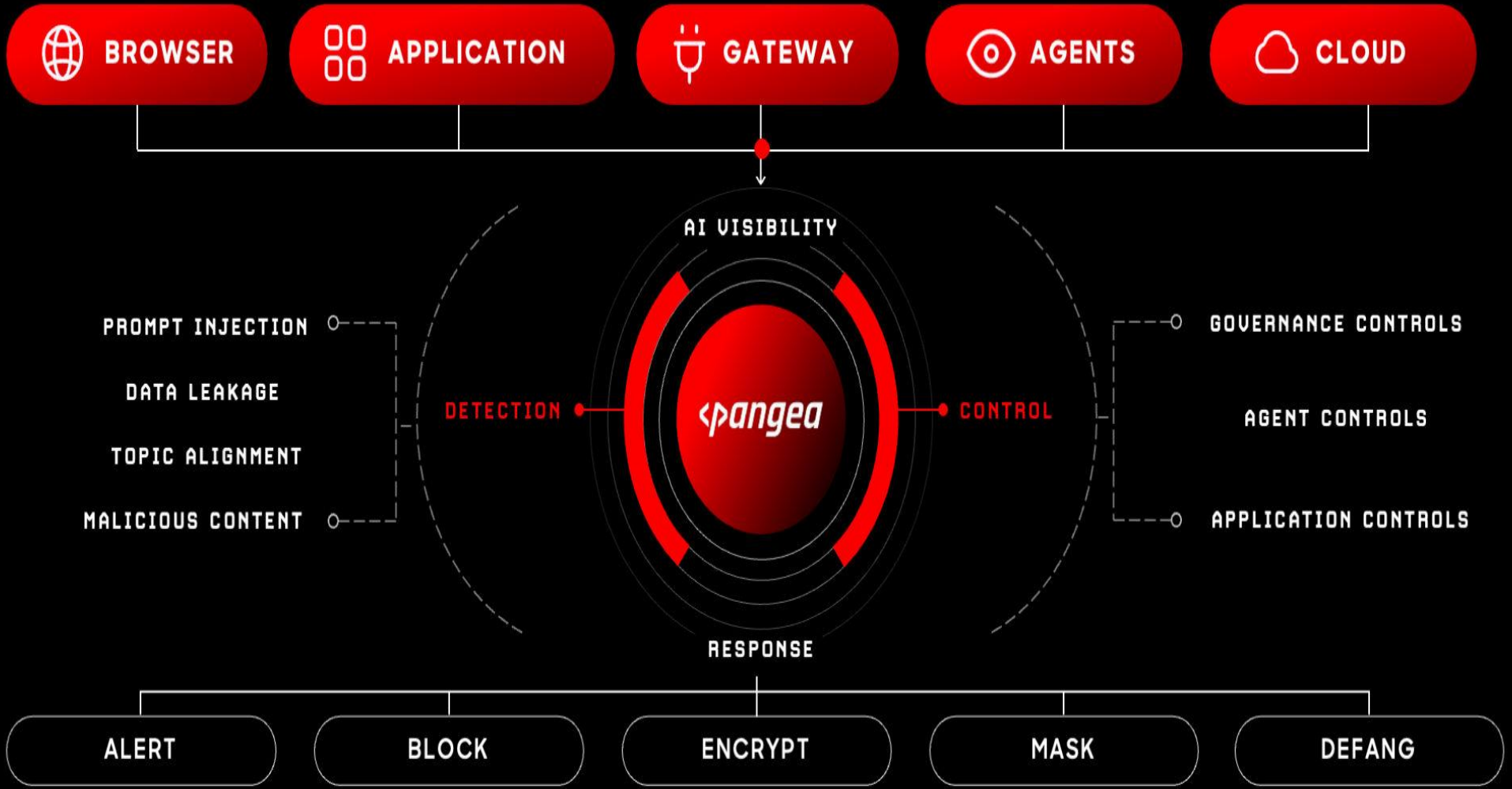


Secure AI Agents

discover agents and secure identities & privileges across SaaS apps

Stop GenAI Data Leaks

across browsers, endpoints, and cloud environments


BROWSER
APPLICATION
GATEWAY
AGENTS
CLOUD
AI VISIBILITY
PROMPT INJECTION
DATA LEAKAGE
TOPIC ALIGNMENT
MALICIOUS CONTENT
DETECTION
pangea
CONTROL
GOVERNANCE CONTROLS
AGENT CONTROLS
APPLICATION CONTROLS
RESPONSE
ALERT
BLOCK
ENCRYPT
MASK
DEFANG

Мейржанулы Даурен