NEXT-GENERATION SECURITY

DigitalData

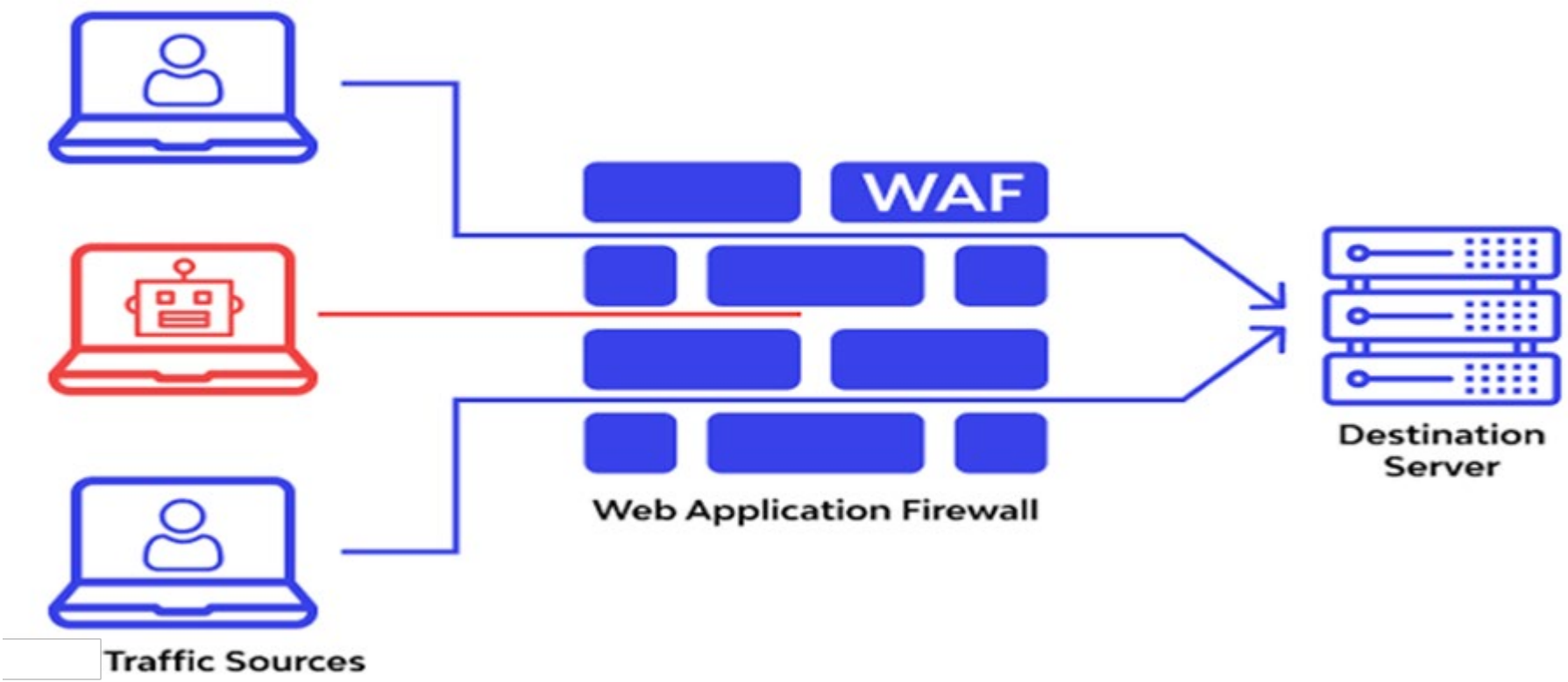
AI-based Web Application Firewall

Intelligent, adaptive protection for Web, API, and Apps.
Move beyond static rules with machine learning–driven defense.

Machine Learning Anomaly Detection API Protection Bot Mitigation

Web App Firewalls

Protect against application attacks, mitigate application vulnerabilities, and prevent data leakage



Inspects traffic to block bad traffic and allow legitimate traffic

AI Based WAF

DigitalData

- Utilizes advanced ML algorithms (NLP, behavioral analysis) instead of relying solely on static rulesets.

- Safeguards against OWASP Top 10, bot attacks, and emerging zero-day threats with high precision

- Continuously learns from traffic patterns across millions of requests, updating protections automatically

- Understands the "intent" behind requests rather than just matching keywords, reducing false positives

Technical Architecture

DigitalData

End-to-End ML Pipelining

GPU based Real-time Processing

Ingestion

Traffic Collection

HTTP(S) requests, headers, bodies, cookies

Context Extraction

Client IP, Geo, Device Fingerprint, TLS info

RAW DATA

Feature Eng.

Normalization

Tokenize inputs into n-grams (NLP)

Embeddings

Vectorize text (Word2Vec, TF-IDF)

VECTORS

Reduction

PCA to project into attack feature space

Modeling

Probability

Gradient Boosted Trees for likelihood score

GBT

Classification

Neural Networks for attack type labeling

DEEP LEARNING

Types

SQLi, XSS, RCE, LFI, etc.

Decisioning

` Policy Engine

Combine ML score with reputation & rules

Enforcement

Allow, Block, Rate Limit, or Challenge

ACTION

Bot Defense

CAPTCHA / JS Injection

MLOps

Monitoring

Drift detection & KPI tracking

Retraining

Automated model updates with new samples

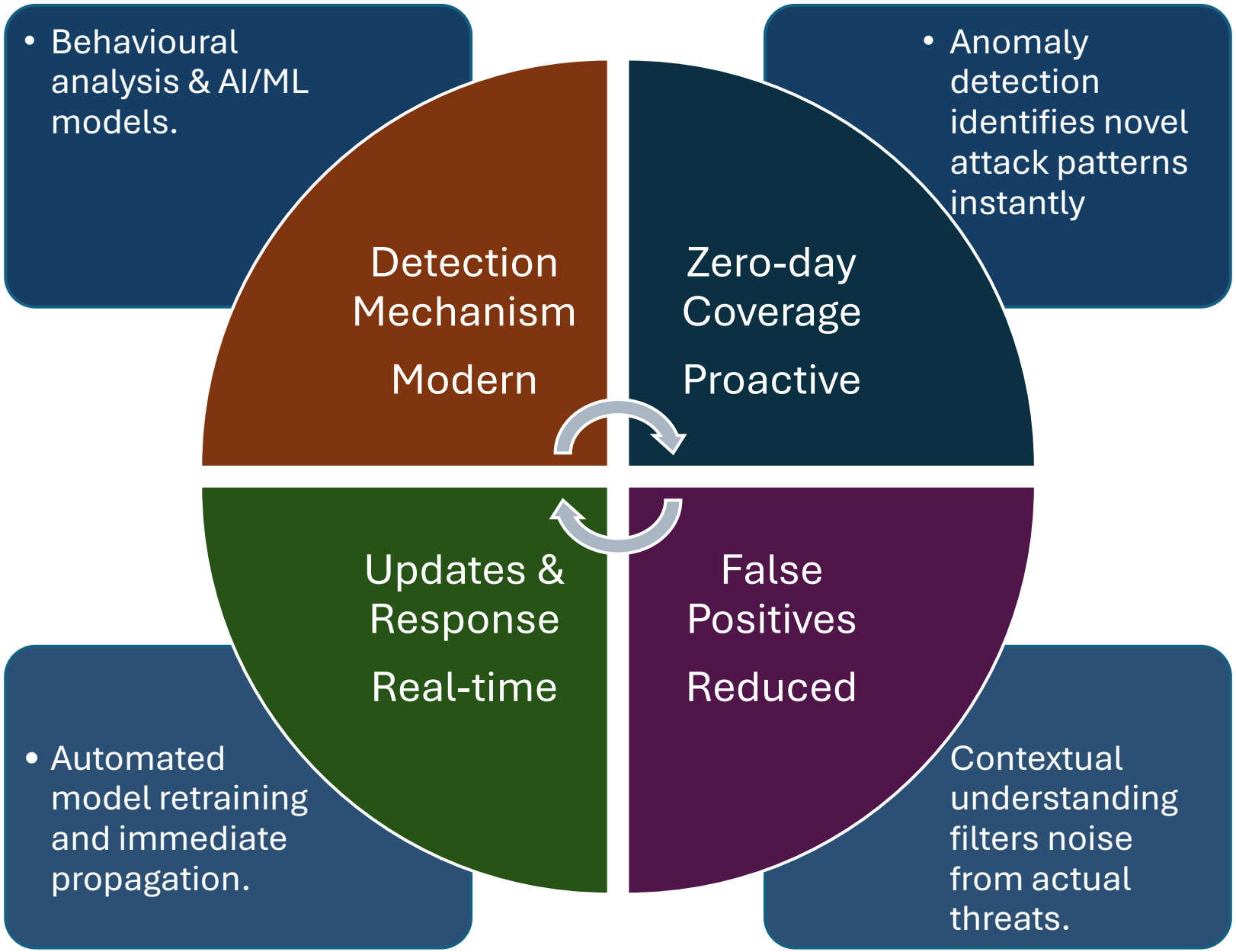
LOOP

Mode

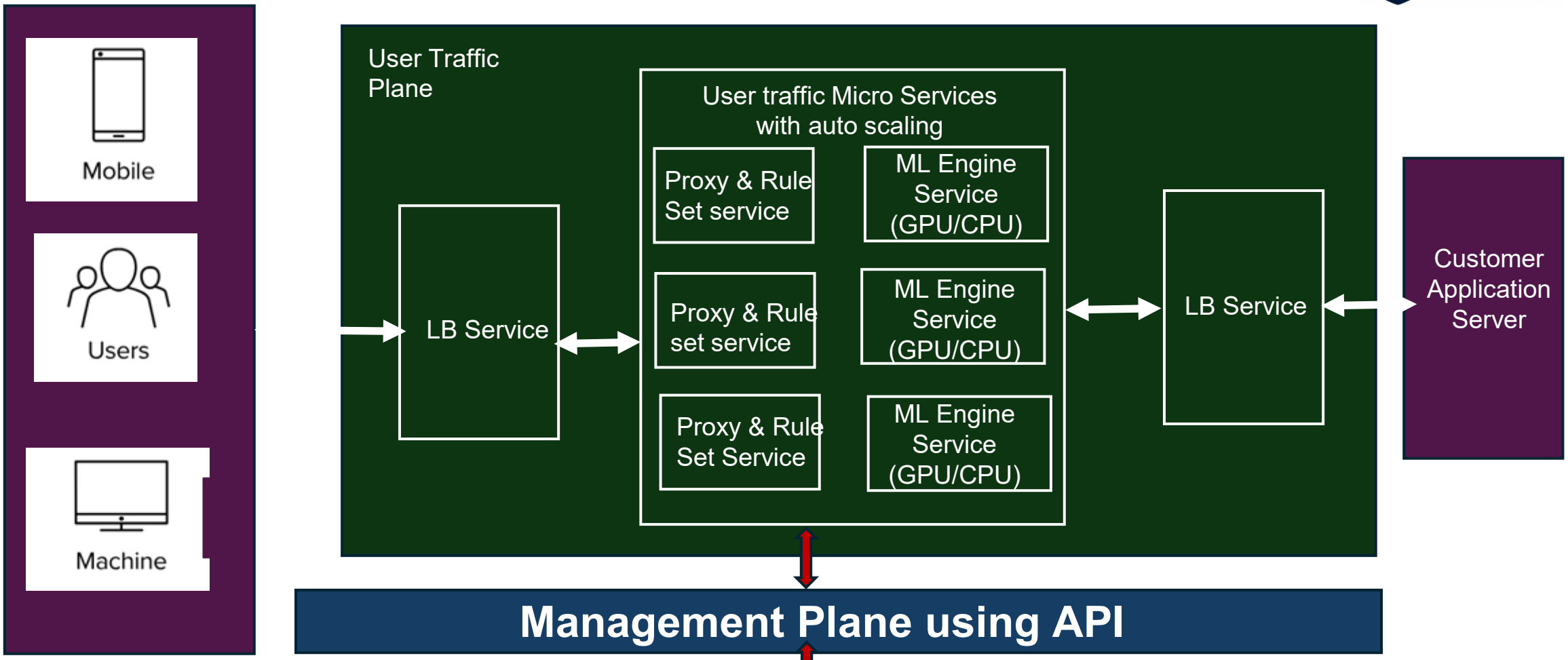
Shadow mode → Active blocking

Data Flow → Processi ng → AI Analysis → Security Action

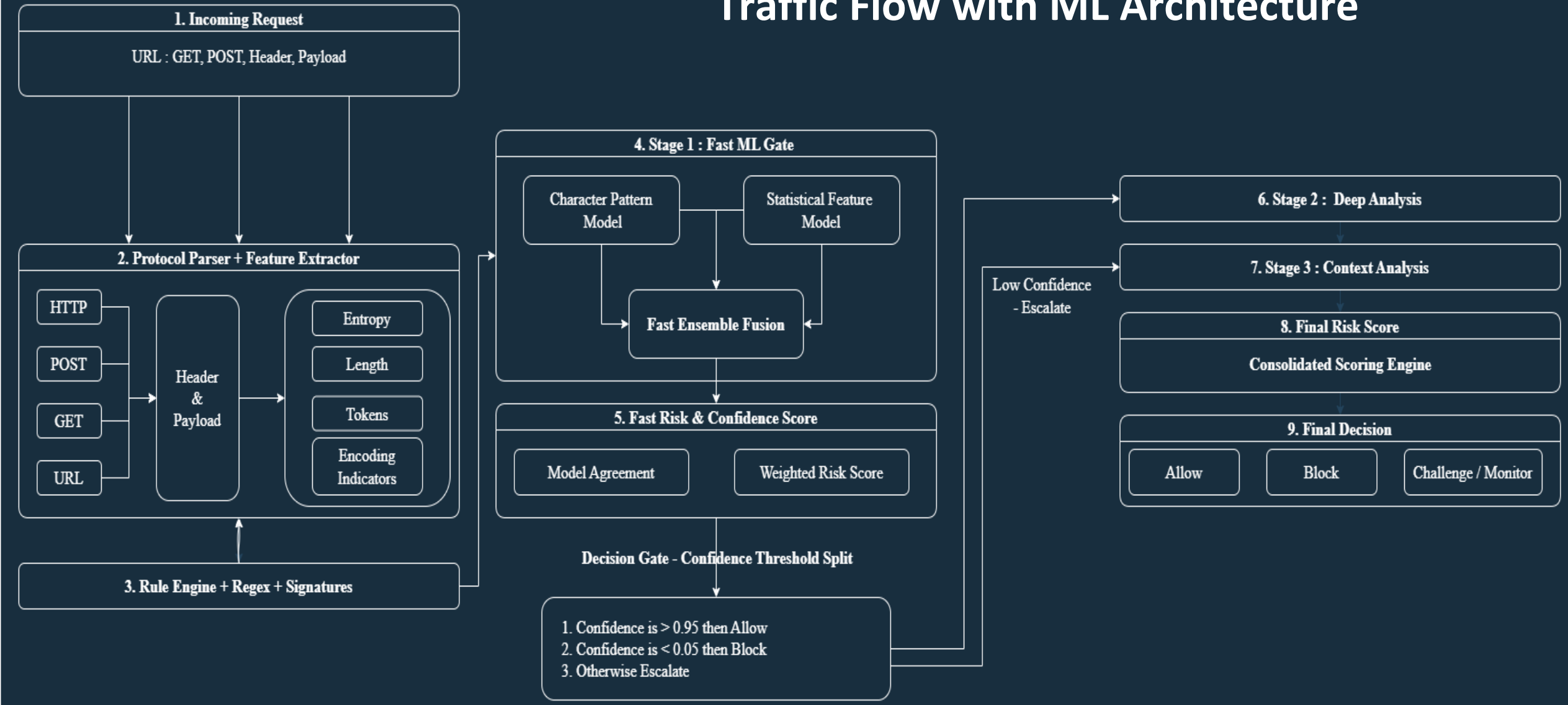
Key Benefits of AI Based WAF



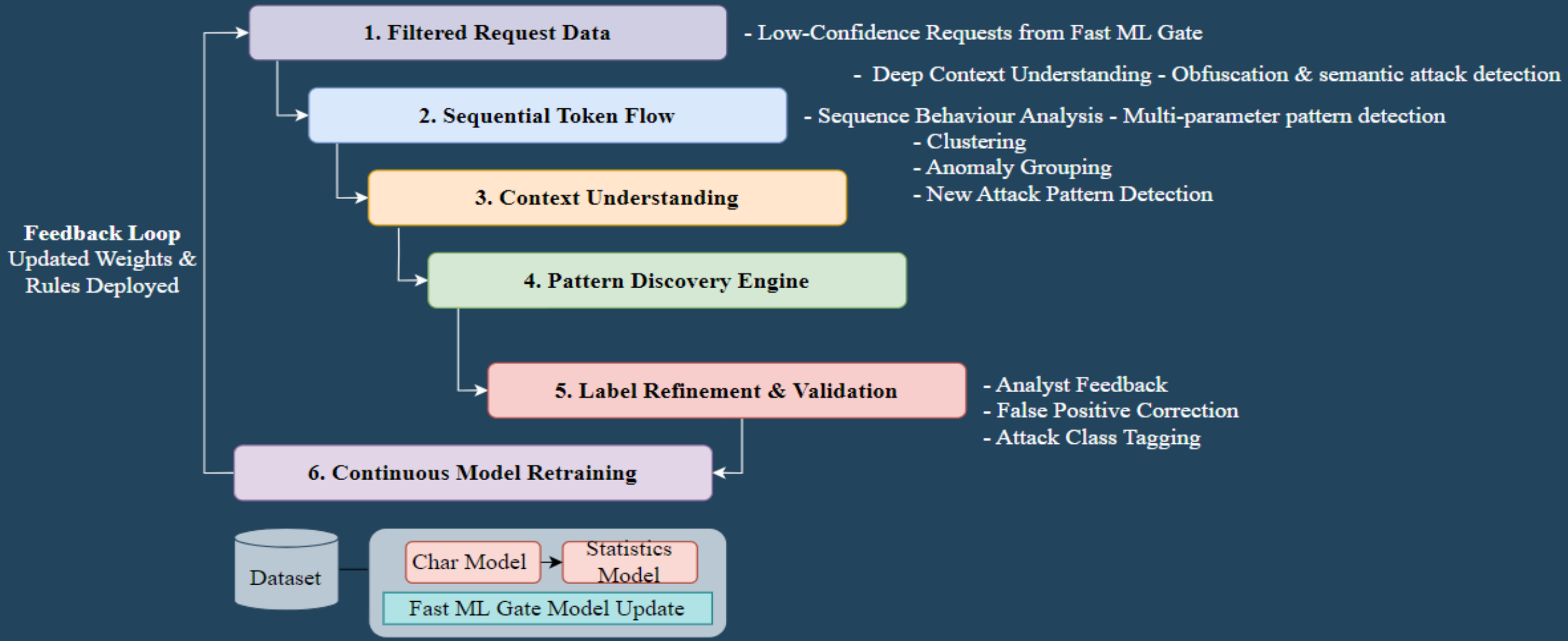
WAF Mico Services Architecture



Traffic Flow with ML Architecture



Feedback Loop



Traffic Intelligence

AI Based Drill Down Dashboard

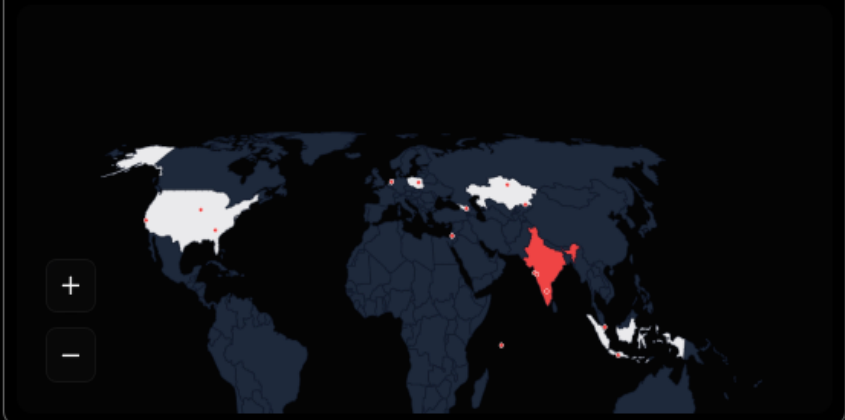
All Domains | Last 24h

Total Requests	Allowed	Blocked
41,526	16,496	25,030
Peak RPS	**Peak Throughput**	**Attack Rate**
41.55	0.48 MBps	60.28%
Top Priority	**Top Country**	**Critical Threats**
High	India	24,996

Top Attacker IPs

49.43.26.101	46,237
115.246.38.51	53
194.26.192.57	22
219.91.178.127	7
143.244.139.244	3

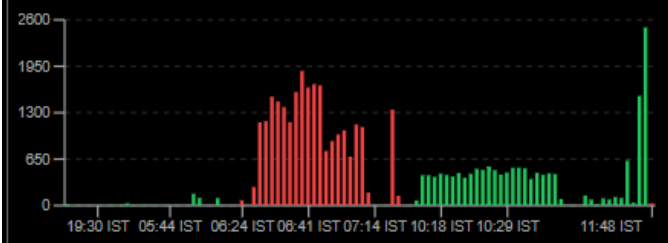
Traffic Intelligence (Geo Map)



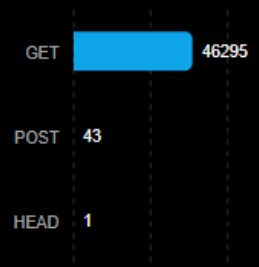
OWASP Top 10 Attack

Requests Per Second (RPS)

Total Requests(Allowed/Blocked)

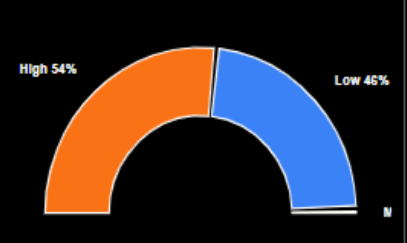


Attack Methods Used

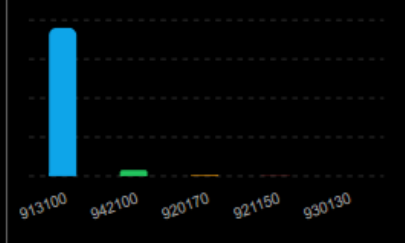


Peak Throughput(MBps)

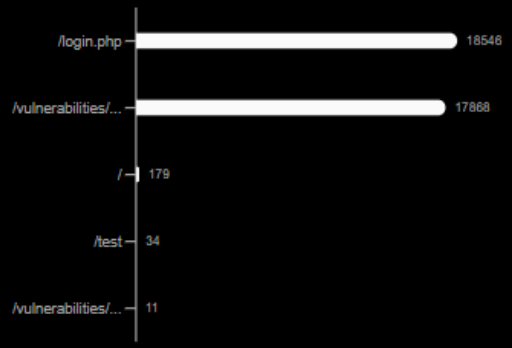
Top Attack Priority



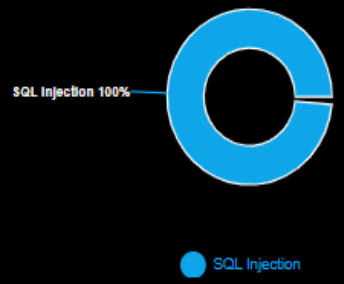
Top Triggered Rules



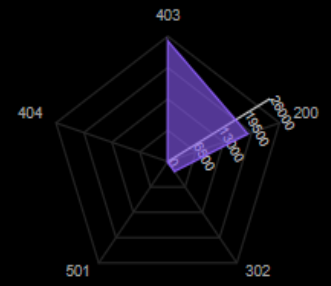
Top 5 URIs



Top 5 Attacks



Top 5 HTTP Codes



Top 5 Applications

www.abc.com	46,339

Key Features of AI Based WAF

DigitalData

- GPU Enbaled
- Micro Services
- Guard Rule Set
- AI/ML Deep Learning
- Zero Day Protection
- API Security

- AI Powered Bot Guard.
- Advance Client-Side Protection
- Advance Login Security
- Intelligent HTTP Protocol Protection
- Advance JSON/XML protection
- LLM Applications Protection

- Comprehen sive ACL
- Advance L7 DDoS Protection.
- Enhanced SSL offloading
- Flexible Deployment
- Actions
- AI Powered Drill down dashboard

- Centralized Policy Management
- Threat Intelligence
- Role based Administration
- Predefined security reports
- AWS Cloud WAF
- GPU Based Appliances HW