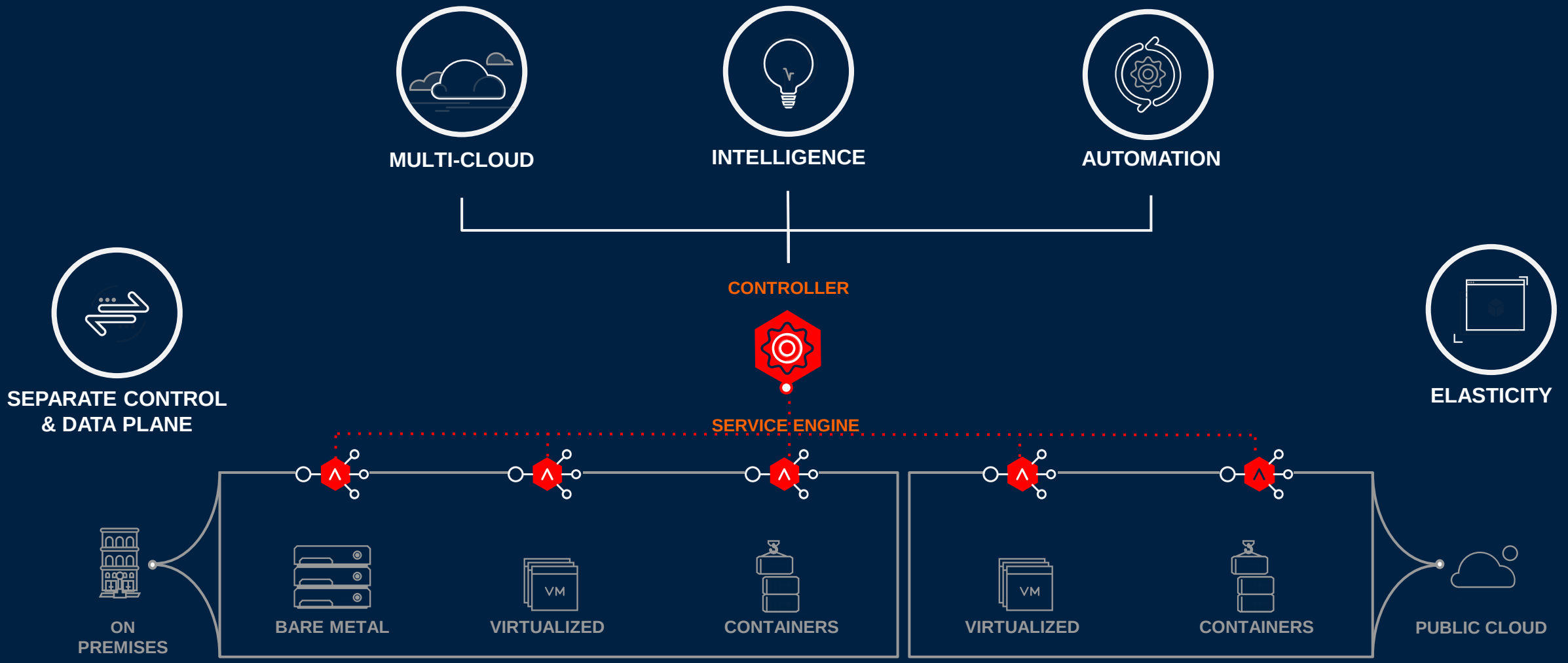
Securing Web Applications using ML and Automation

Gaurav Rastogi
Director, NSBU

Ashutosh Gupta
Staff Engineer, NSBU

Modern, Scalable, Multi-Cloud Architecture



Why this talk ?

Web Application Security is Necessary

Web Application Security is Hard

Availability comes before Security.

Attack Types

Application availability
(Network, Host etc)

Data leakage
(SSN, Credit cards etc)

Data integrity
(bank balance etc)

Possible Approaches

- Secure Coding Guidelines
- Security focused application architecture
- Security-team <> Application team
- WAF for Application attacks
- DDoS protection for volumetric attacks

SecOps Comp.

Security Stack with WAF, SSL, DDoS and Rate Limiting

Fully integrated with Avi's comprehensive security services

REST API

- Centralized Management
- Multi-Cloud Elastic Fabric
- Automation & Programmability
- Real Time Visibility & Analytics

DATA CENTER

PRIVATE CLOUD

PUBLIC CLOUD

Web Application Firewall
OWASP CRS protection, Attack Analytics

Application Rate Limiting
Control and restrict by application or tenants

DDoS Protection
DDoS detection and mitigation with elastic scaling

L7 ACLs
Content (URI) based security rules

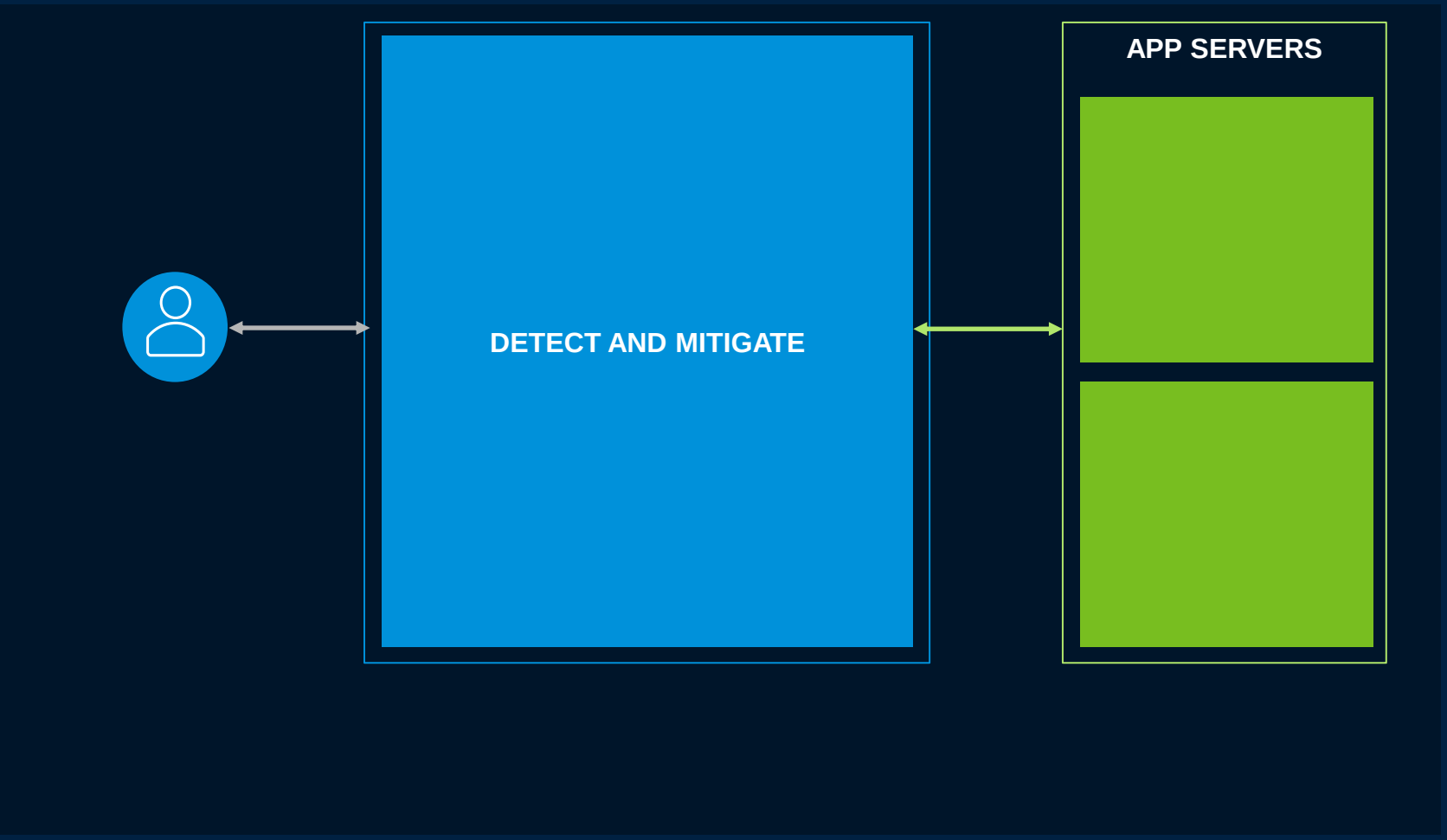
L3/4 ACLs
IP-Port based Security Rules

Encryption
SSL/TLS

Security Insights

Security score
Attack insights
SSL Insights
WAF analytics

Traditional DDoS Protection



Detect and Mitigate

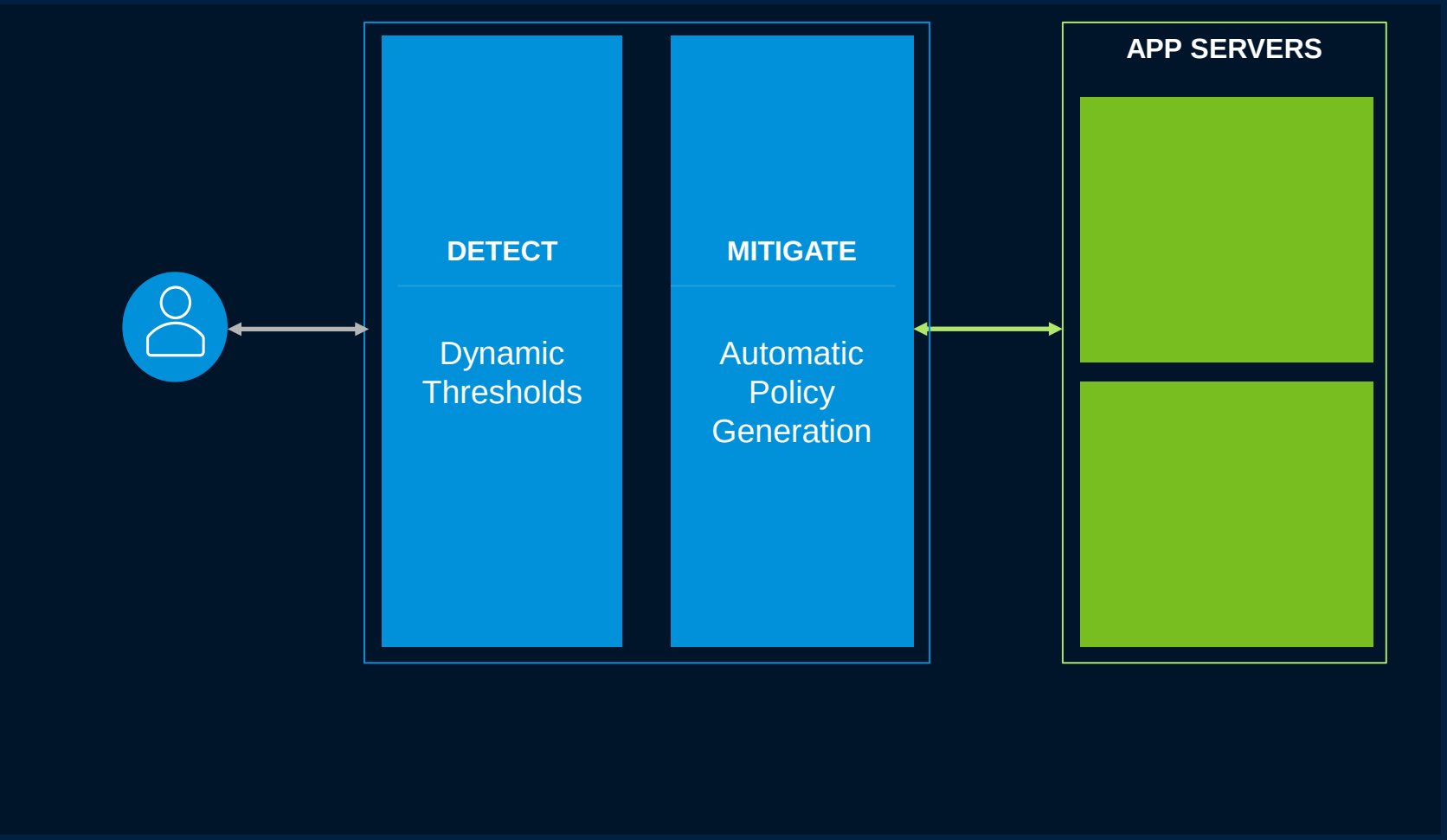
- Always on
- Based on App specific thresholds
- Mitigate actions - rate-limit or drop
- Admins figure out right thresholds

Issues

- Continuous detection & mitigation can lead to self-DDoS
- Place in Network matters
- Static thresholds are not effective

DDoS Protection

Learning based DDoS protection



Detect + Mitigate

Detection Always On

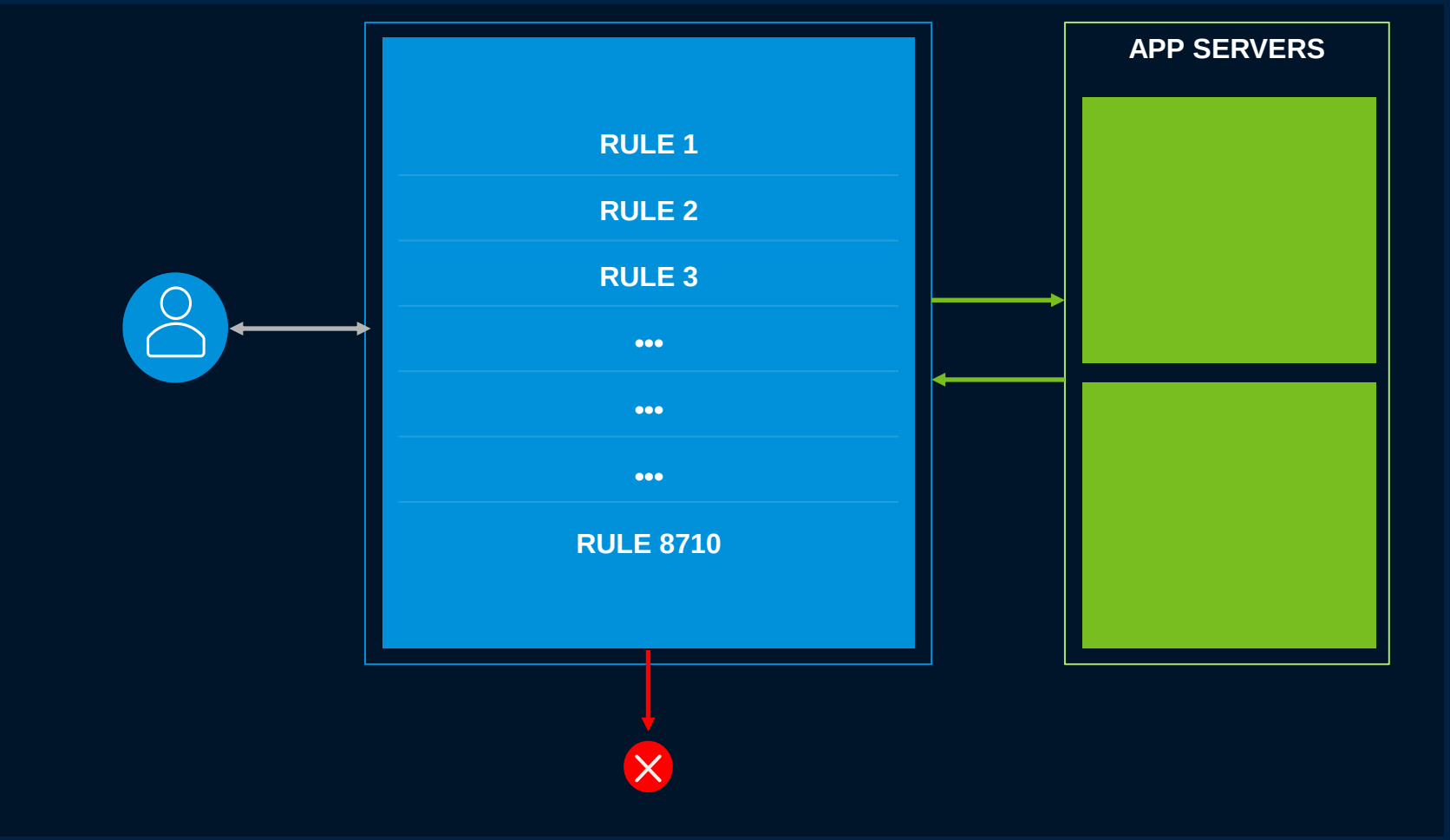
Dynamic thresholds by Anomaly Detection (incl. seasonal pattern)

Learn good vs bad traffic, uses IP reputation , Bot detection

Issues

Need good thresholds for day-1

Traditional Web Application Firewalls (WAF)



Security Rules

Generic sources like OWASP/CRS

Formed by a Security Expert having intimate application knowledge

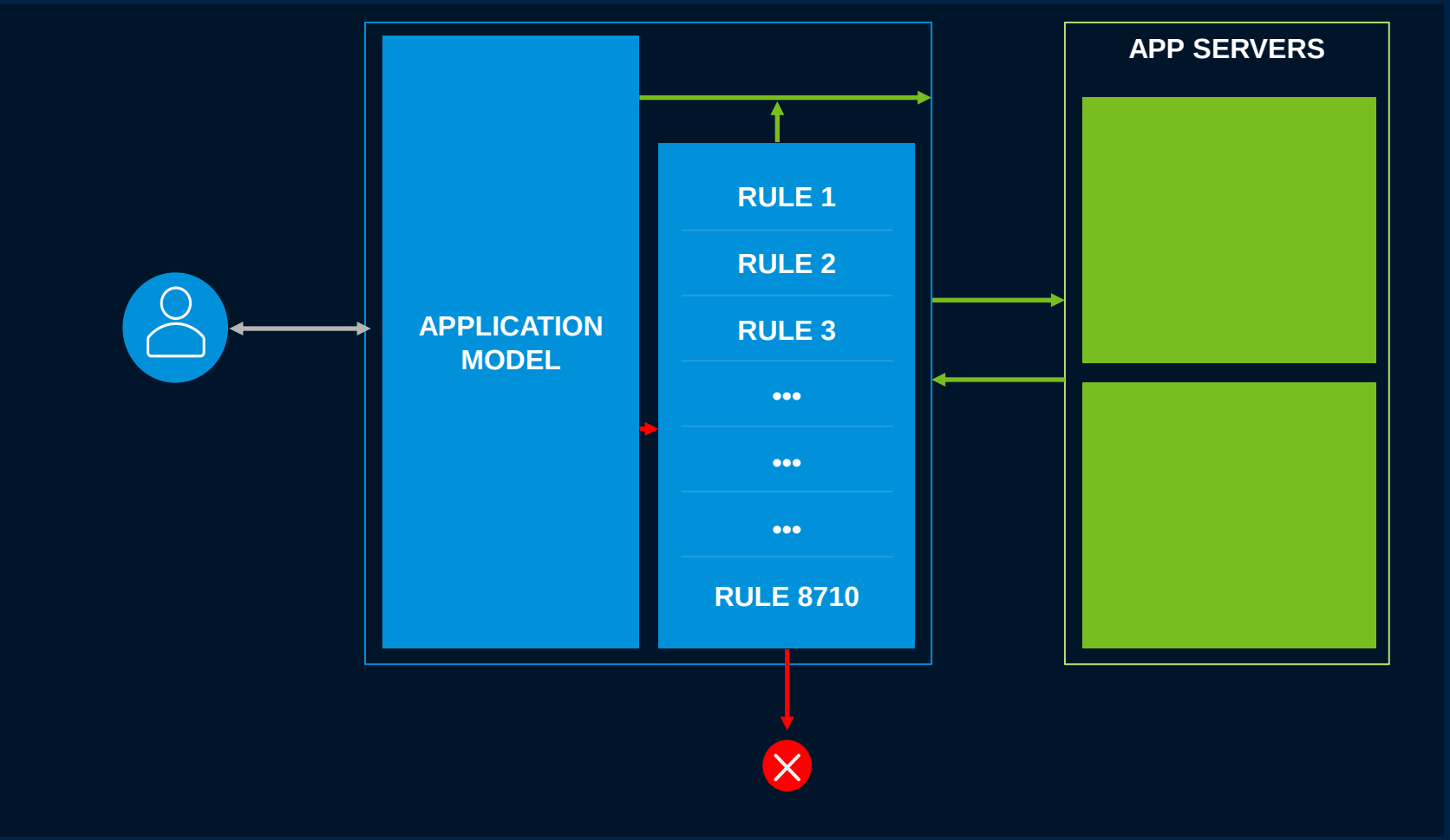
Issues

incorrectly formed rules can block legitimate traffic. (False Positives)

Modifying rules is risky

Applications keep evolving, rules don't

Application Modelling – Defense against False Positives



Application Model

Formed solely on the basis of traffic

Can have input from Scanners

Can be Statistical or Machine Learned

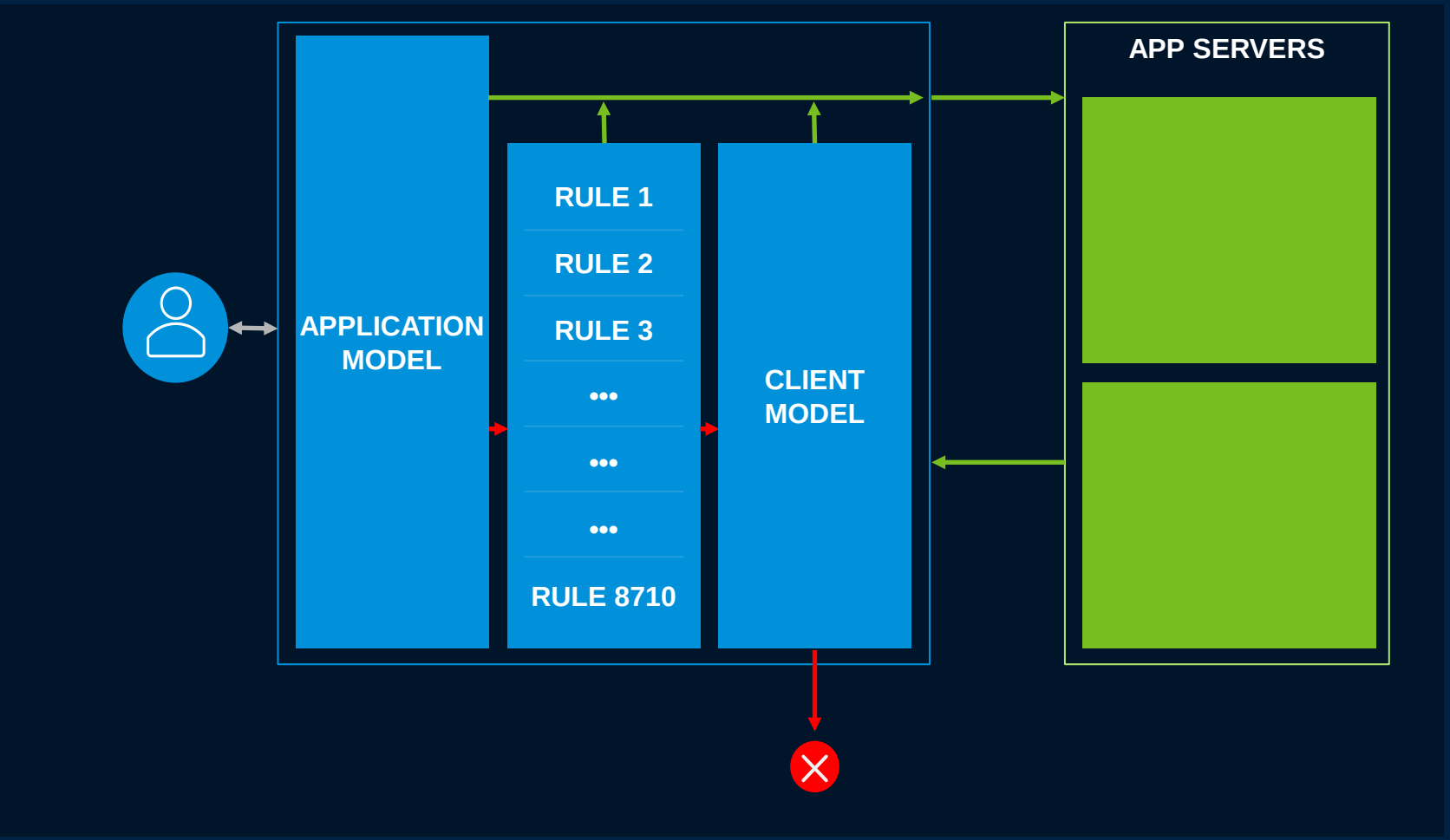
Issues

Model is formed over period of time

Not all parts of application can be modelled with high accuracy.

Still some traffic is inspected by rules, still false positives.

Client Modelling – Defense against False Positives



Client Model

Decides threat level of client request, bot or not.

Can follow “zero trust” or Not

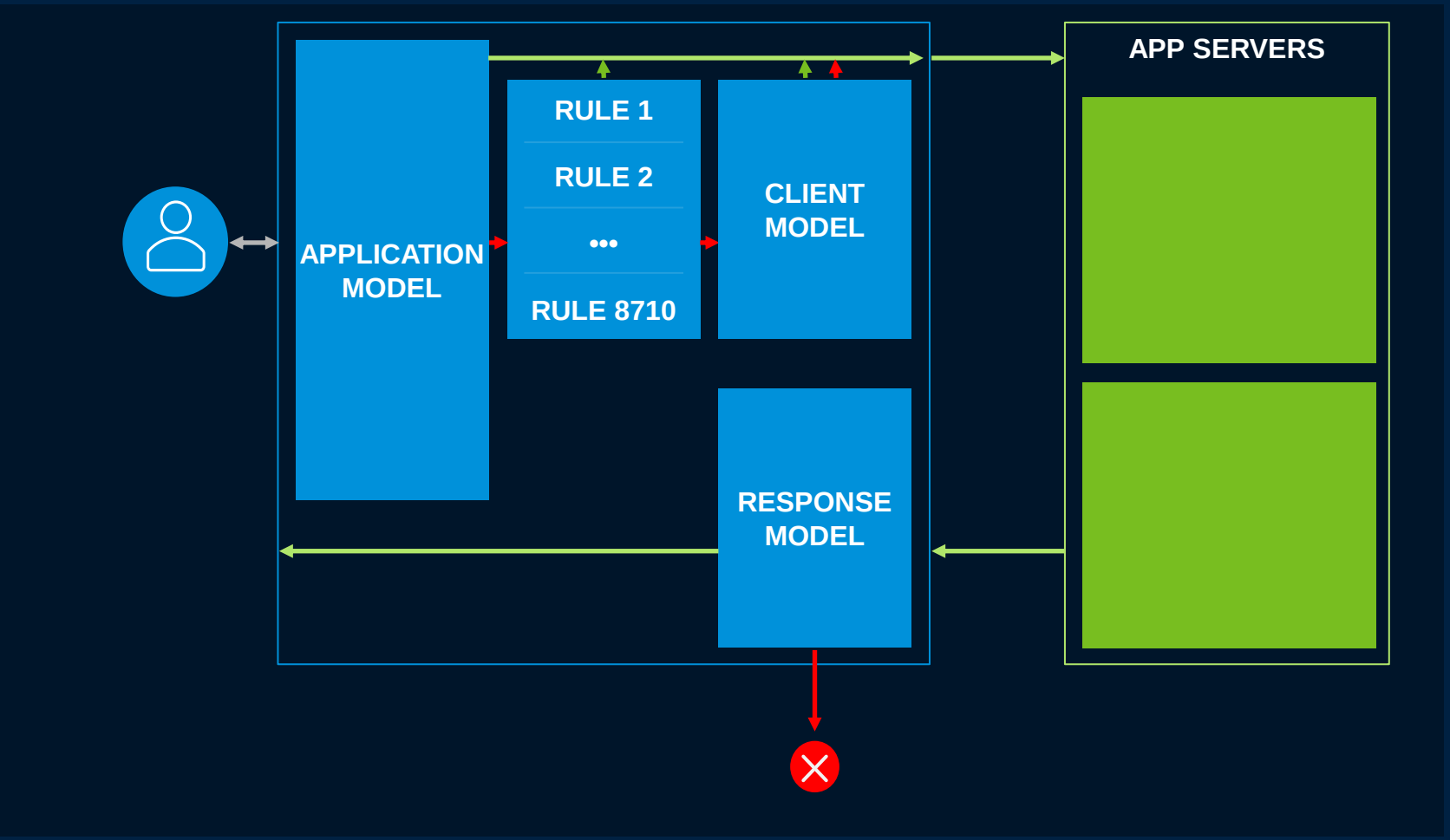
Consults IP reputation database, Client tracking database.

Issues

Zero Trust will generate false positive for new clients

Opposite approach can be abused by bad actors

Response Modelling – Defense against Zero-day attacks



Response Model

Model of a typical response to URI, param combinations

Evolves as Application changes

Evaluated only for failed requests

Issues

Compute intensive

Feature selection is critical

Key Challenges

Volumetric Attacks should be mitigated on Edge or even in provider network

Trade-off between security and availability

Solution must cater to all paranoia level use-cases

Distributed analysis and algorithms

Efficient use of IT resources

Thanks

Reach out to us on

GAURAV RASTOGI
rastogiga@vmware.com

ASHUTOSH GUPTA
ashutoshgupta@vmware.com