# Securing APIs to Mitigate Risk of Business Logic Abuse

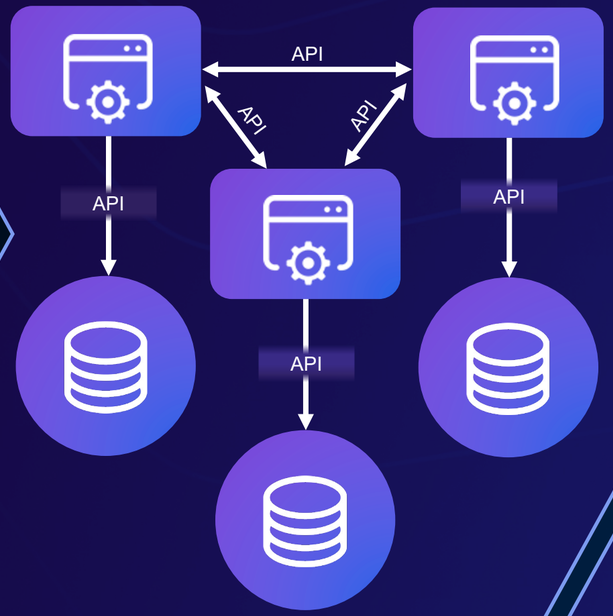
Luke Babarinde
Global Solution Architect

# Application Modernization Drives Growth

## But the Journey Creates Security Challenges

### High-Quality Customer Experiences

### New Application Architectures




### New Challenges

- API Sprawl
- DevOps — Rapid API Churn
- Expanded Attack Surface

# APIs enable business logic

**Protocols:** Normalization of legacy and new datasets

**Integration:** Enable interoperability in heterogeneous systems and service meshes

**Service Delivery:** Exchange data with consumers, producers and partners

# APIs Pose New Challenges

**Highly lucrative targets**

**Exposed business logic**

**Lack of visibility into automated traffic**

# The Two Unknowns

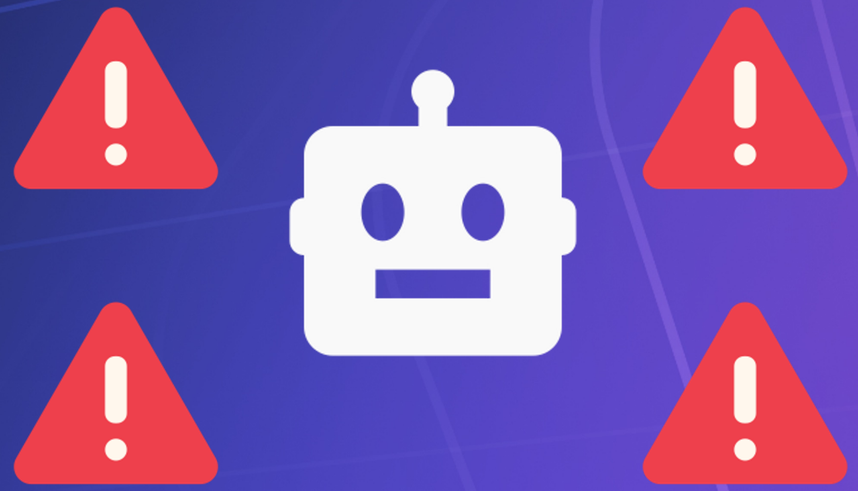
## Attack Surface and Attack Vectors

### Lack of Visibility into the Attack Surface

APIs


### Lack of Awareness of Automated Threats

Advanced Bots



imperva
a Thales company

# The Two Unknowns by the Numbers

**1.5bn**

**Average number of API calls per year to enterprise sites**

**613**

**Average number of API endpoints discovered per account**

**71%**

**Of all web traffic is API related**

**46%**

**Of Account Takeover attacks targeted API endpoints**

**20%**

**Of API attacks targeted Financial Services sites**

**27%**

**Of attacks mitigated targeted Business Logic**

Source: The State of API Security in 2024 Report

# Anatomy of Service Abuse

## Attack Vectors

### Bad Actor

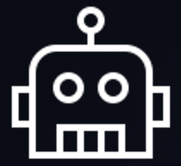
**Motivation**

Service Abuse

Fraud

Service Disruption

### Automated Bot



**Automated Functions**

Scanning

Fuzzing

Enumeration

Botnet

## Attack Surface

### Application/API Endpoint


**Service Layer**

Public APIs

Private APIs

### Data

**Distributed Datastores**

Intellectual Property

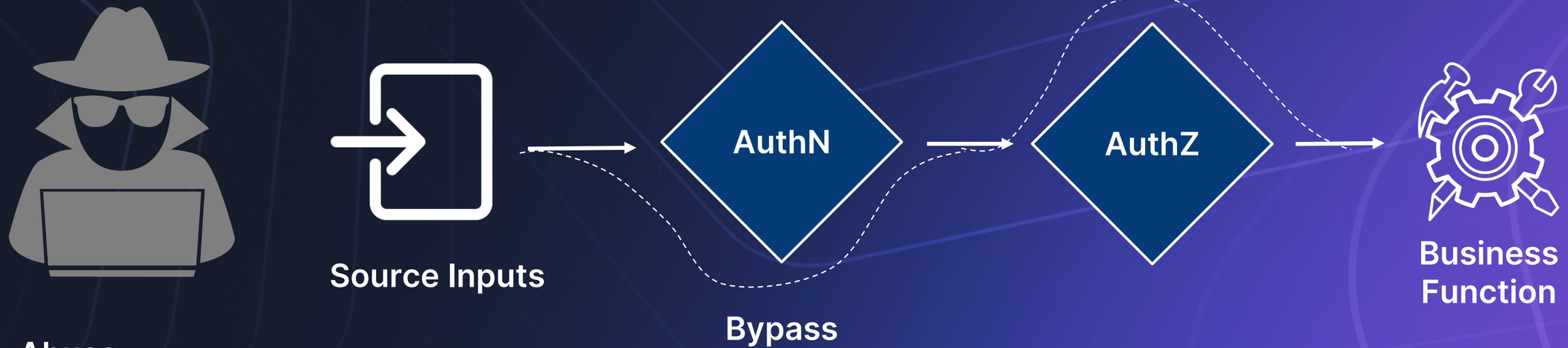
Consumer Sensitive Data

A **business logic attack** leverages design flaws and occurs when a legitimate **flow of functionality** is **manipulated** or **misused** in a way which could lead to an adverse effect on the business function

***Vulnerabilities*** have the same characteristics across different applications

***Design Flaws*** are application specific and lack common signatures

# Business Logic Attacks in Action




Abuse functionality

Manipulate parameter(s)

Bypass or side step workflow

# Business Logic Abuse Spans the Customer Journey

## Account Creation

### Fake Account Creation

Create accounts for subsequent misuse

## Login

### Account Takeover

Unauthorized access to user accounts by a motivated attacker

## Browsing

### Scraping

Using bots to extract content or data from a website

## Add to Cart

### Inventory Hoarding

Acquiring a large amount of products specifically for resale and not personal use

## Checkout

### Carding

Fraudulent use and theft of stored value cards or credit cards

# Traditional Security Is Not Enough

## Traditional Attacks


Remote Code Execution

SQL Injection

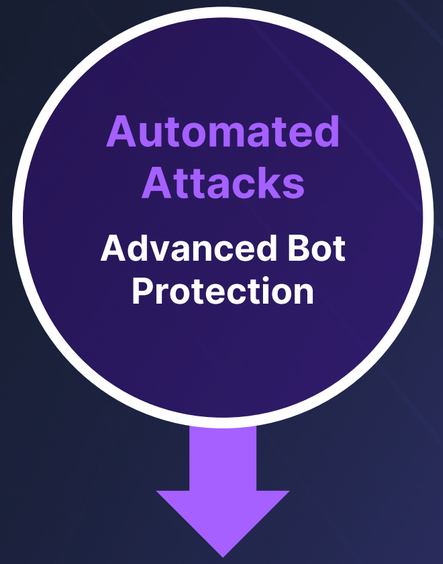
L3/L4/L7 DDoS

Supply Chain

SSRF

Security Misconfiguration

## Business Logic Abuse and Bot Attacks




Credential Stuffing

Carding

Scraping

Fake Account Creation

Influence Fraud


BOLA & BFLA

Mass Assignment & BPLA

Broken Authentication

Improper Inventory Management

# API Gateways Are Not Enough

## API **Gateway**

API Lifecycle Management

Authentication & Authorization*

Mediation

Monetization

## API **Security**

Exploit Defense

Layer 3/4/7 DDoS Mitigation

API Abuse

Data Theft

# Build Your API Security Strategy

## Adopt an integrated approach

### 1 Continuous Discovery

*Discover all APIs and updates*

Unknown APIs

Unauthenticated APIs

Shadow APIs

Deprecated APIs

### 2 Risk Assessment

*Identify high risk APIs*

Uncover design flaws

Identify OWASP API Security Top 10 risks

### 3 Protect High Risk APIs

*Adopt a platform for full protection*

Block reconnaissance attacks

Detect anomalies

Apply bot protection

**OWASP API Security Top 10 2023**

- A10: Unsafe Consumption of APIs
- A2: Broken Authentication
- A9: Improper Inventory Management
- A7: Server side Request Forgery
- A4: Unrestricted Resource Consumption
- A8: Security Misconfiguration
- A6: Unrestricted Access to Sensitive Business Flows
- A1: Broken Object Level Authorization
- A5: Broken Function Level Authorization
- A3: Broken Object Property Level Auth

**Technical Attacks**

**API Specific Attacks**

Low

Attack Complexity

High

**Bots to Humans Ratio**
**60% : 40%**

**Reconnaissance**

- Client-Side Threats
- Account Takeover
- Vuln Probing
- Unauthorised Scans

**DDoS Traffic**

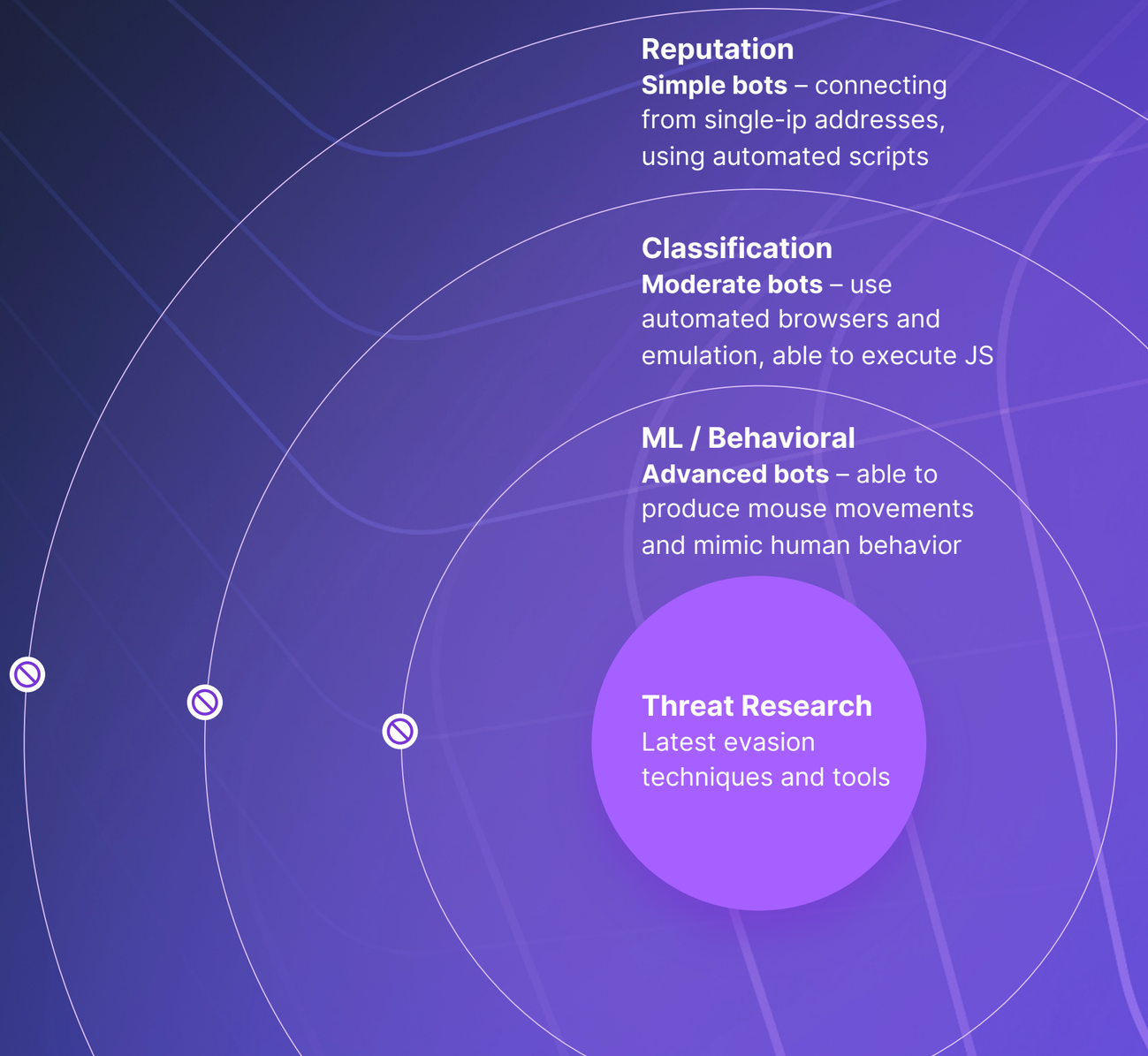
**OWASP Technical Attacks**

**API Business Logic Attacks**

**Insider Threats & Runtime Threats**

**Data Layer Attacks**

# Defeating sophisticated API attacks requires layered bot protection




imperva

# Protect Your Business Logic Layer

## Best Practices to improve your API security posture

Discover, classify, and inventory all APIs, endpoints, parameters, and payloads

Use continuous discovery to maintain an always up-to-date API inventory

Identify and protect sensitive and high-risk APIs

Perform risk assessments on vulnerable API endpoints

Establish a robust monitoring system to detect suspicious activity

Adopt a comprehensive approach to API Security

Download the *Imperva State of API Security in 2024 Report*

imperva
a Thales company

# Thank You