# API Security—10 Best Practices and Strategically Applying AI

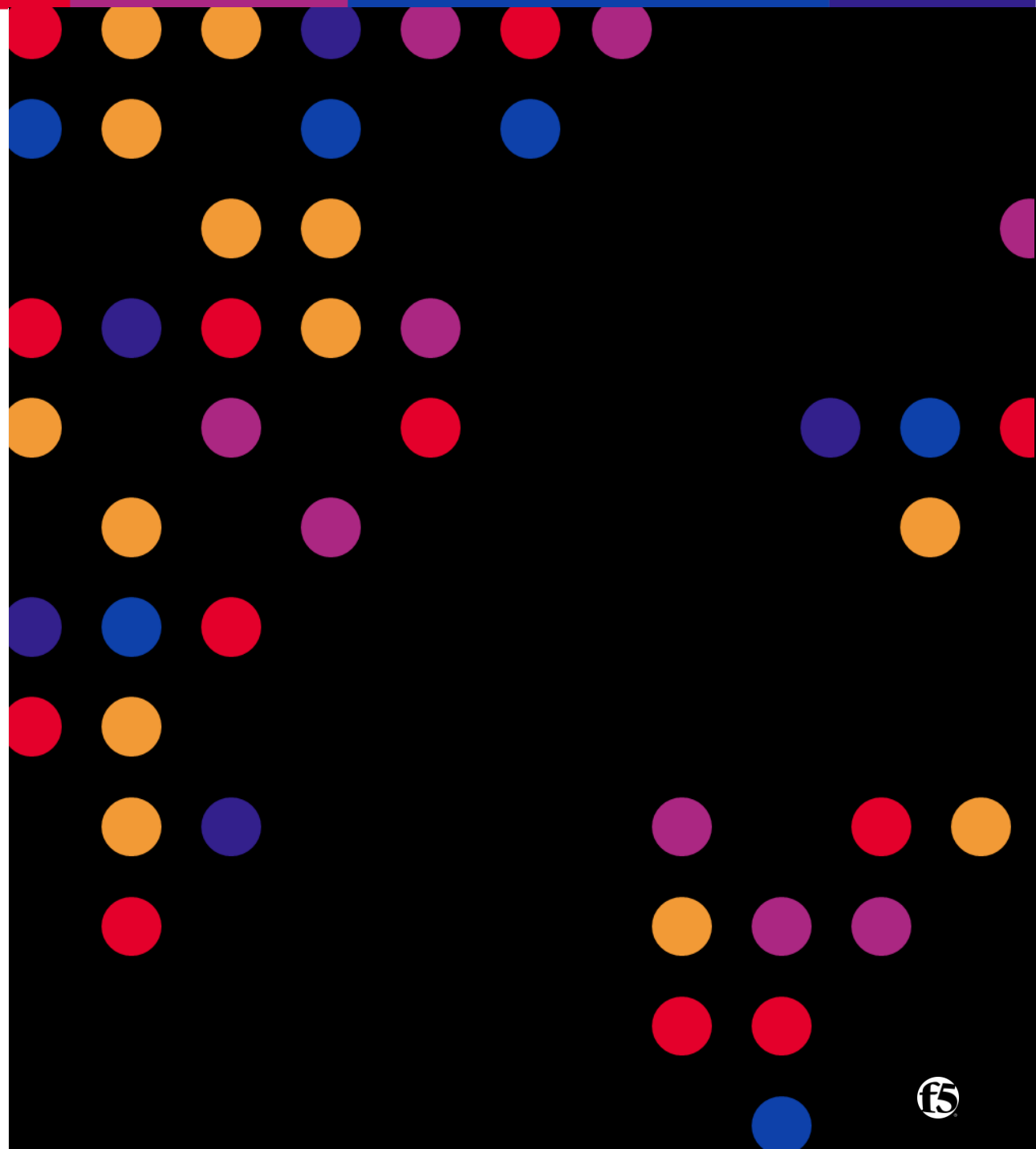
**Josh Goldfarb**
Global Solutions Architect for Security, F5

# Agenda

The State of API Security—Why do we need new approaches?

10 Best Practices

Strategic and Targeted Ways to Apply AI to API Security



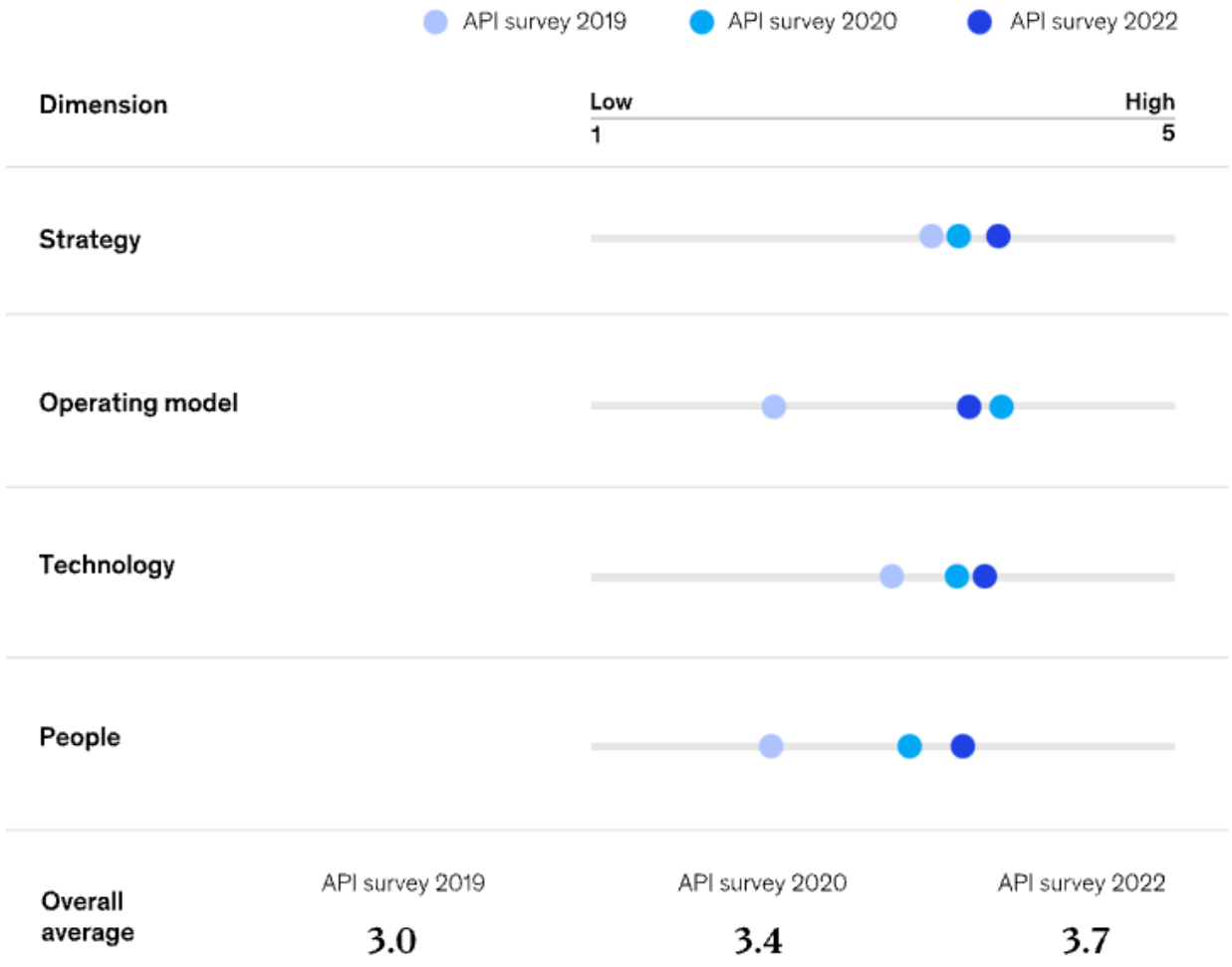
 

# The State of API Security

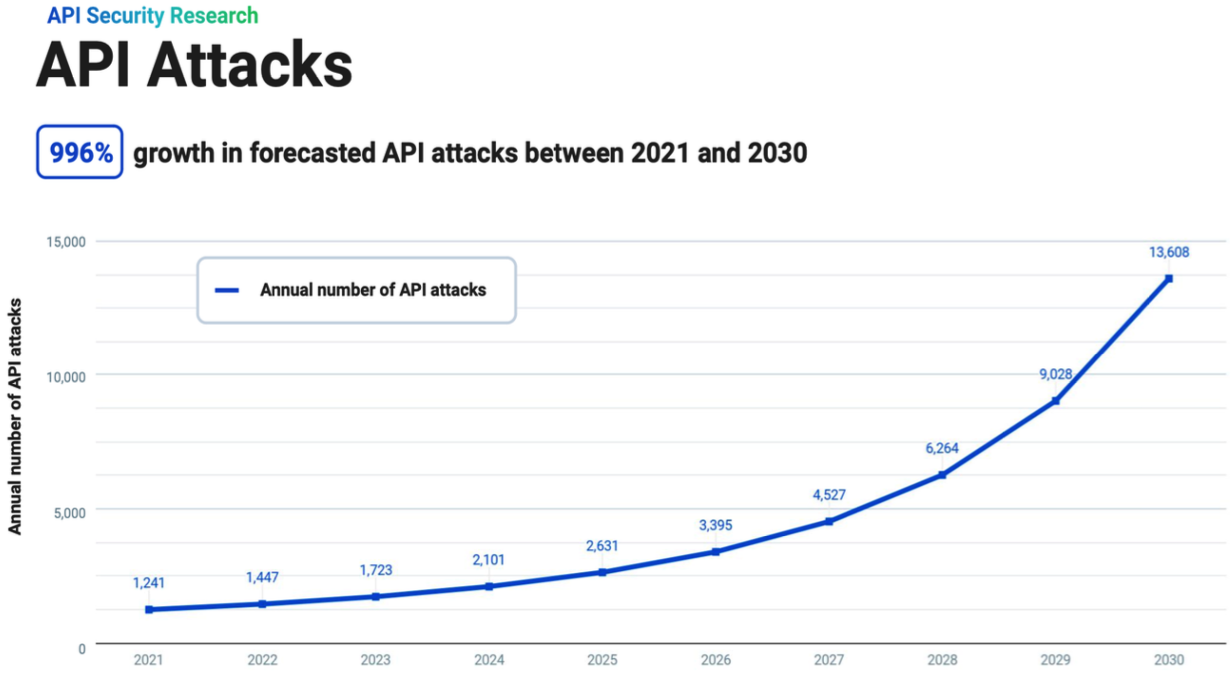
# FI innovation is fueled by APIs

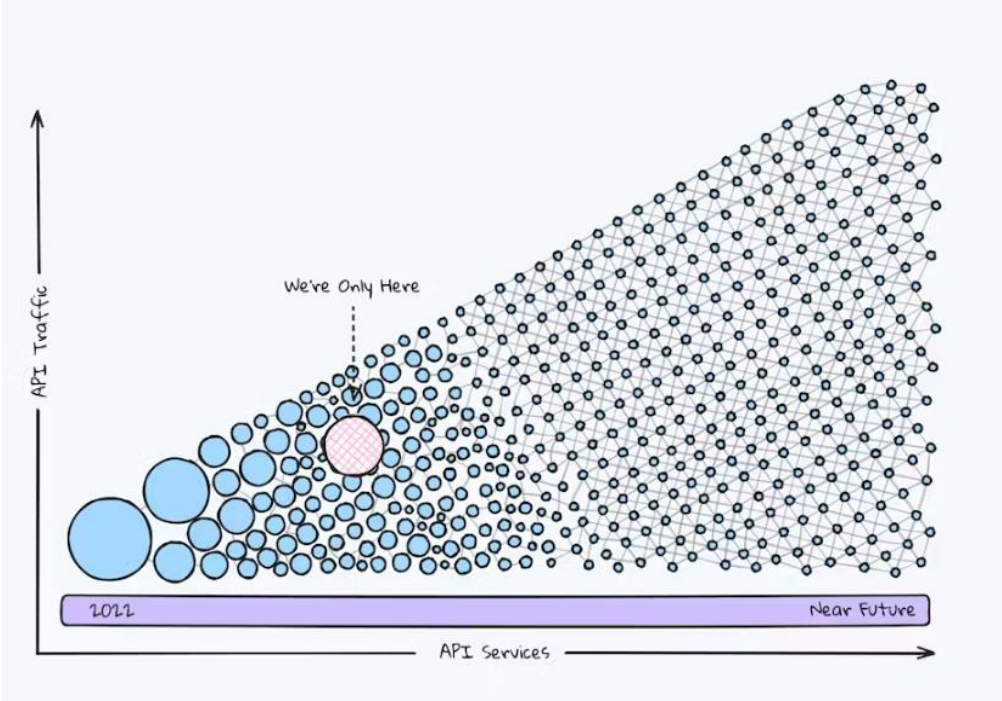
## Level of maturity across key dimensions




Source – McKinsey Global Survey on APIs in Banking

# APIs are under attack




Source – Kong API Security Research

# APIs are risky by definition

**Open by design**—APIs are created to share access to data and applications

**Larger attack surface**—Every API and endpoint expands the potential attack surface

**Difficult to observe**—API attacks can evolve slowly with small requests over weeks or months

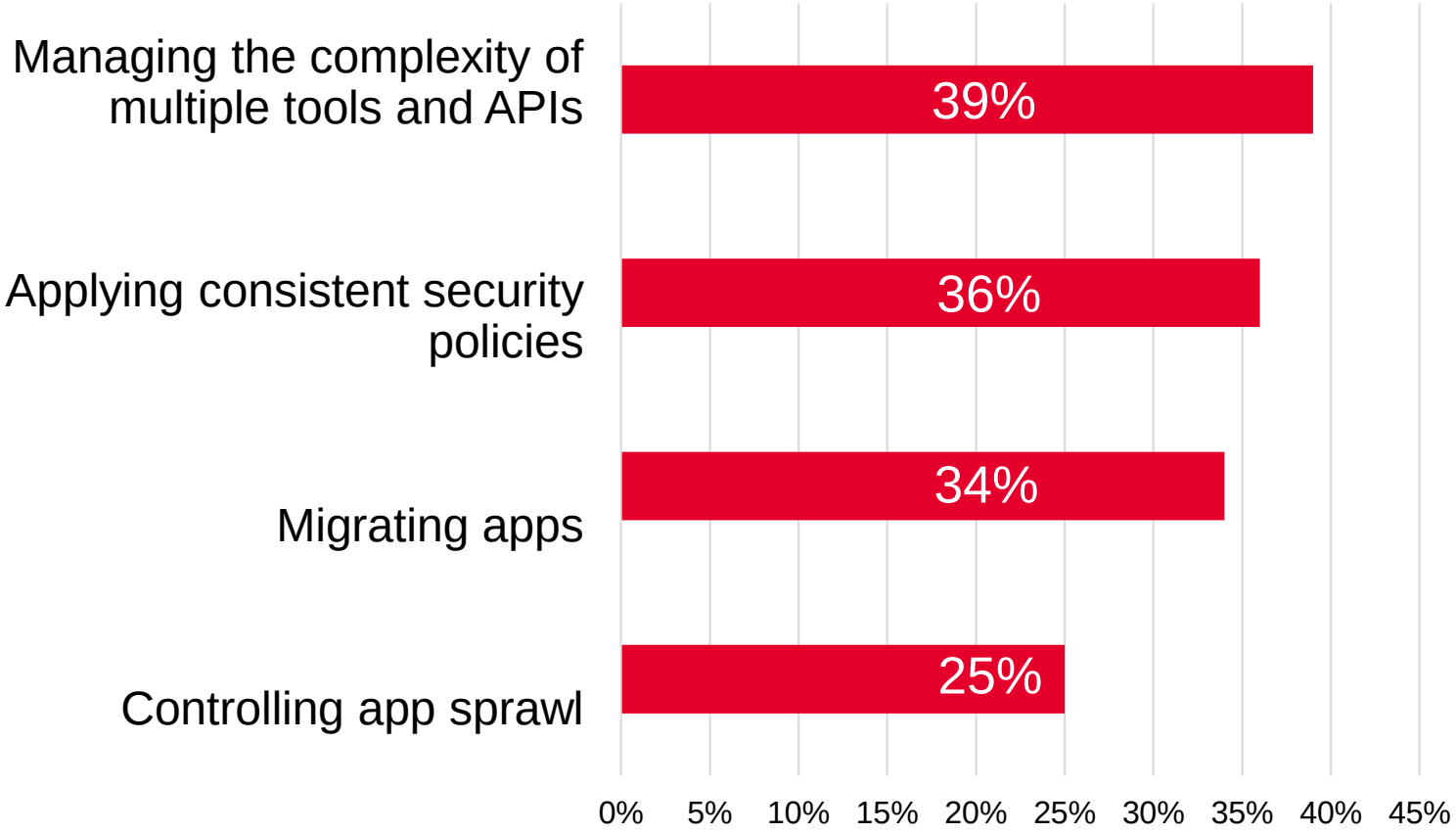

**Expose extra data**—Developers build flexible APIs that provide more data than is required

**Predictable structure**—APIs adhere to logical architectures (REST) making them easy to probe

**Lack protections**—APIs are often deployed without basic protections like access control

# Managing and securing APIs continues to be a challenge




Sources: State of Application Strategy Report (F5, 2023); Continuous API Sprawl (F5, 2021)

**9 out of 10 enterprises have experienced an API security incident**

# Why use AI/ML to protect APIs?

API security requires data-driven analysis to identify malicious usage patterns.

Top-tier threat actors are themselves using AI in their recon and attack campaigns—this will be arms race.

Rapid growth of API adoption makes manual approaches to API security impractical, slow, and costly.

Enables continuous traffic inspection, behavioral analysis and anomaly detection—security evaluation at machine speed.

Inform decision making—create new tools like risk scoring—aggregating insights to aid in analyst review for remediation.

# Gartner’s perspective on WAAP and AI

## Challenge

- The cloud WAAP market continues to suffer from excessive false positives
    - Driving a trend toward the adoption of Artificial Intelligence/Machine Learning (AI/ML)
    - Support to correlate and reduce alert fatigue and produce actionable events

## Recommendation

- Leverage AI/ML and large language models (LLMs) to reduce alert fatigue.
- Provide common language interpretation of events and identify advanced threats.

*— Gartner Market Guide for Cloud Web Application and API Protection, Nov. 13, 2023*

# 10 Best Practices

# API Visibility and Discovery

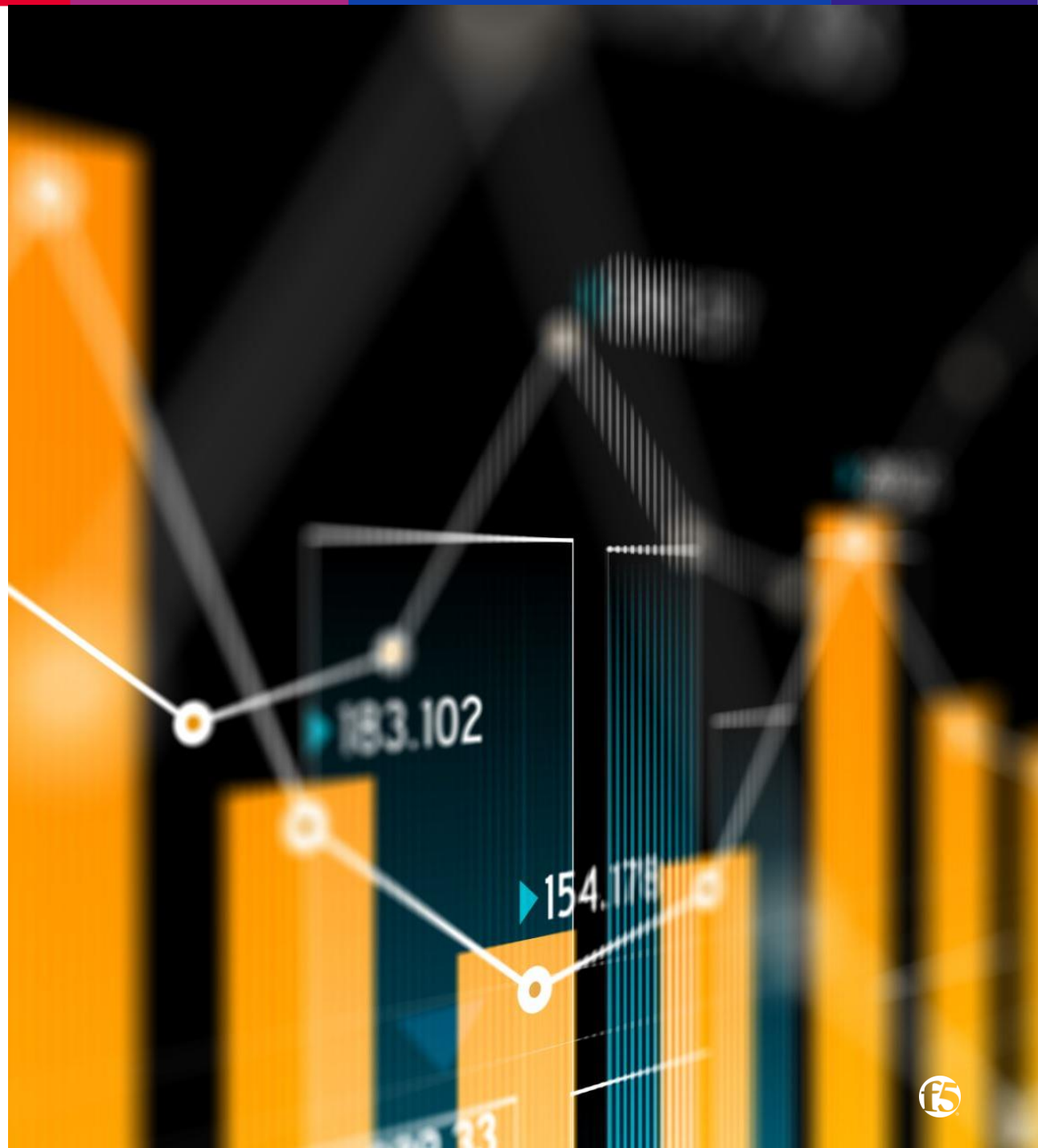
# Schema Validation

# Policy Enforcement

# Safeguarding Sensitive Data



# Abuse and DoS Protection

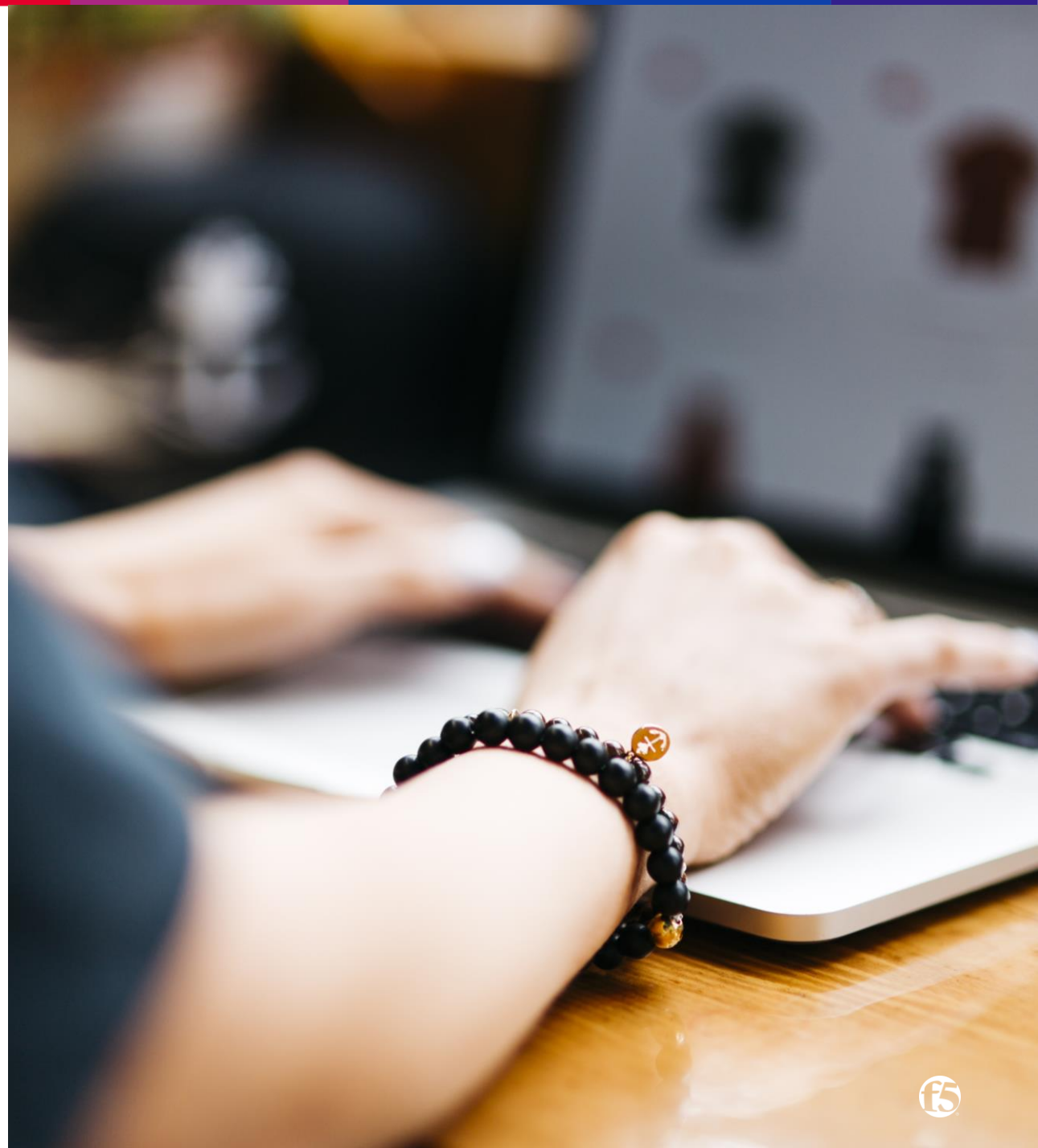
# Attack Protection

# Access Control

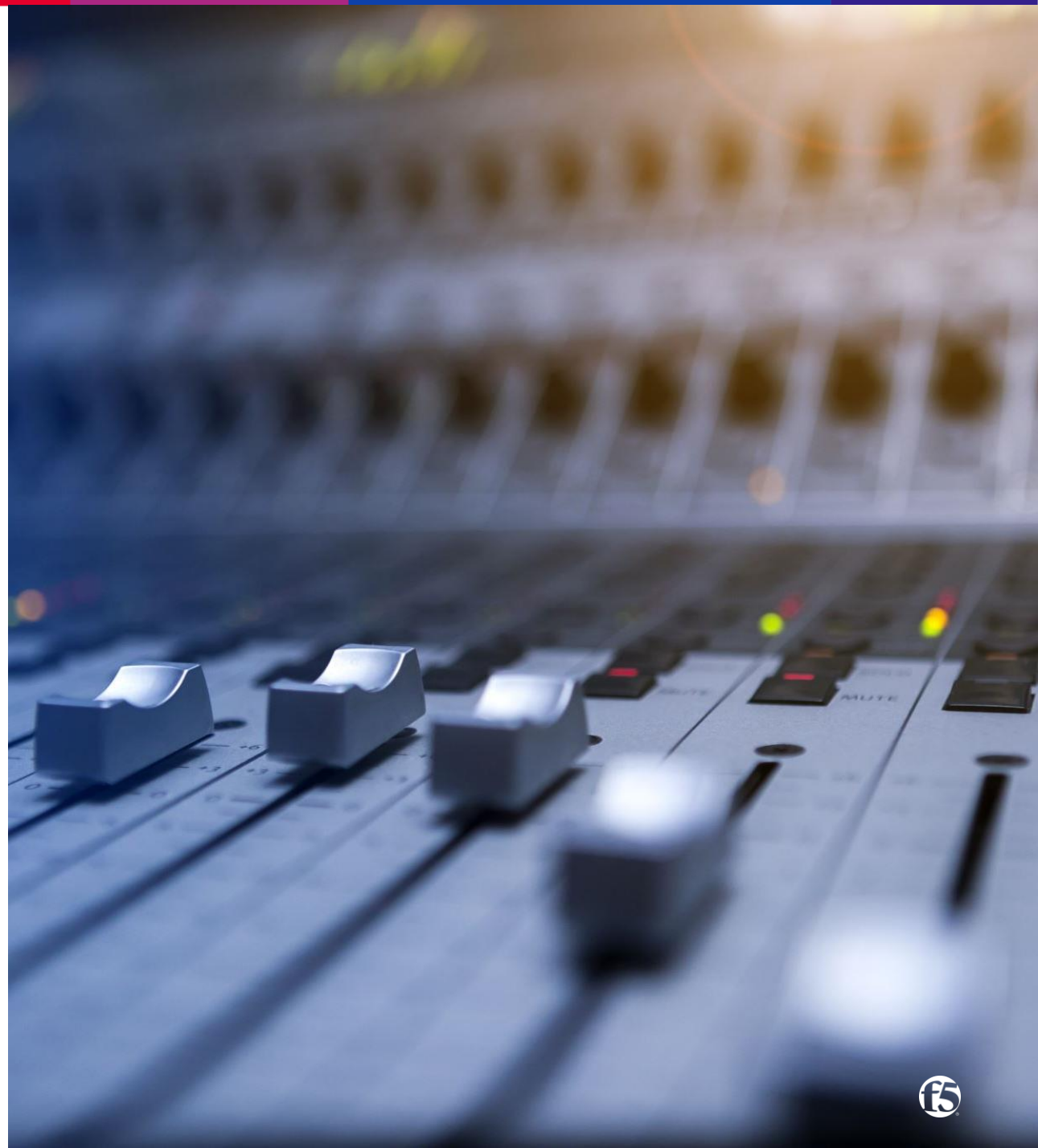
 

# Malicious User Detection



# Configuration and Management



# Behavioral Analysis

# Strategic and Targeted Ways to Apply AI to API Security

# API Visibility and Discovery

# How?

- Begin with inventory, management, and security of known API endpoints
- Study traffic to learn of additional API endpoints
- Include legitimate API endpoints in inventory, management, and security
- Decommission illegitimate API endpoints
- Work with the business to reduce the number of unknown API endpoints
- Continually iterate

# Schema Enforcement

# How?

- Begin with policy
- Learn schemas by analyzing traffic
- Detect departures from policy
- Detect drift
- Mitigate/enforce schema compliance

# Access Control

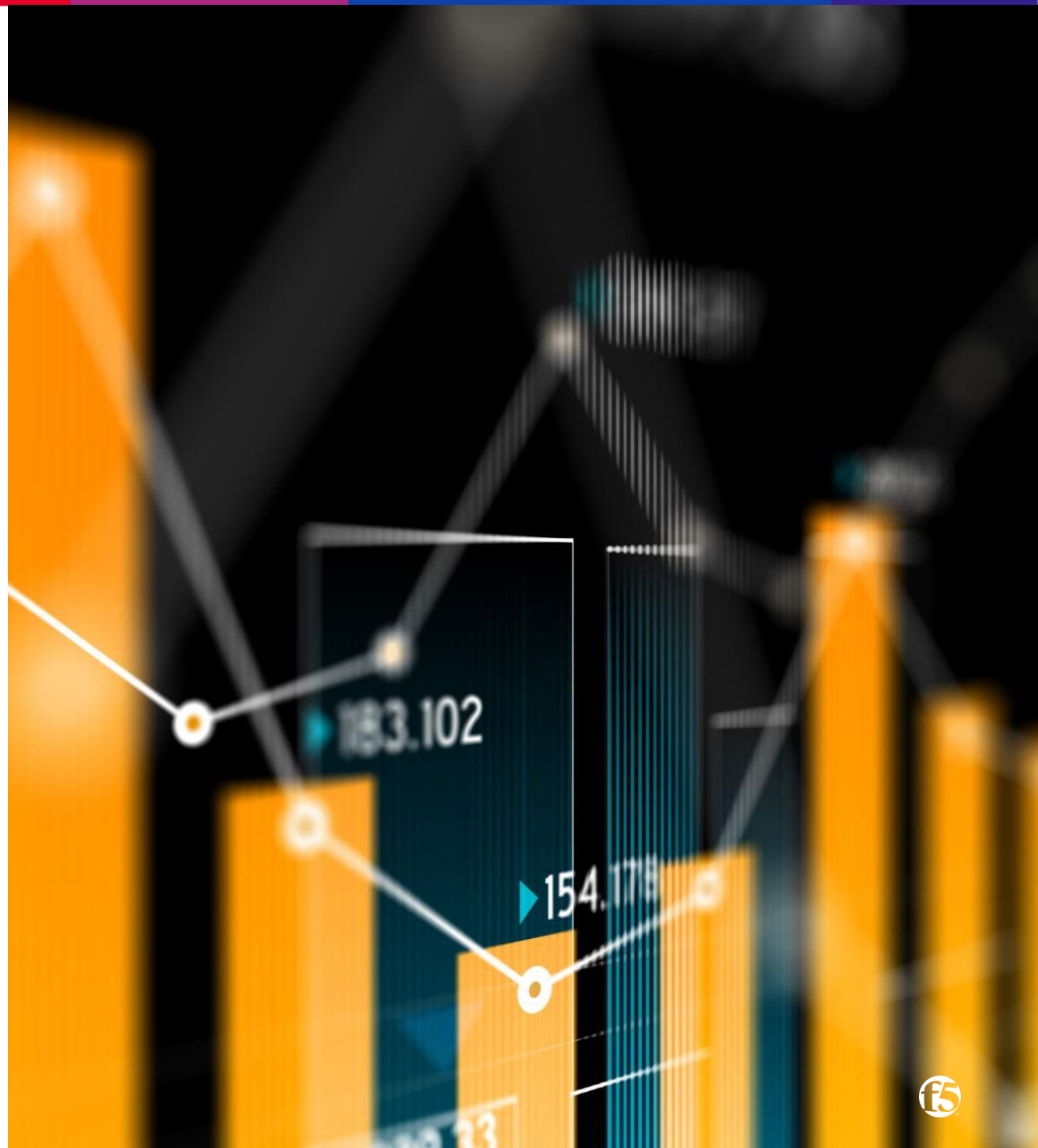
 

# How?

- Map APIs and identify gaps in API authentication and authorization
- Baseline authentication state of all APIs
- Evaluate existing authorizations
- Produce a threat level and risk score for each API
- Mitigate/refine access control as required

# Safeguarding Sensitive Data



# How?

- Identify API endpoints where PII and other sensitive data is transferred
- Detect and flag PII and other sensitive data that is exposed
- Mitigate and/or mask

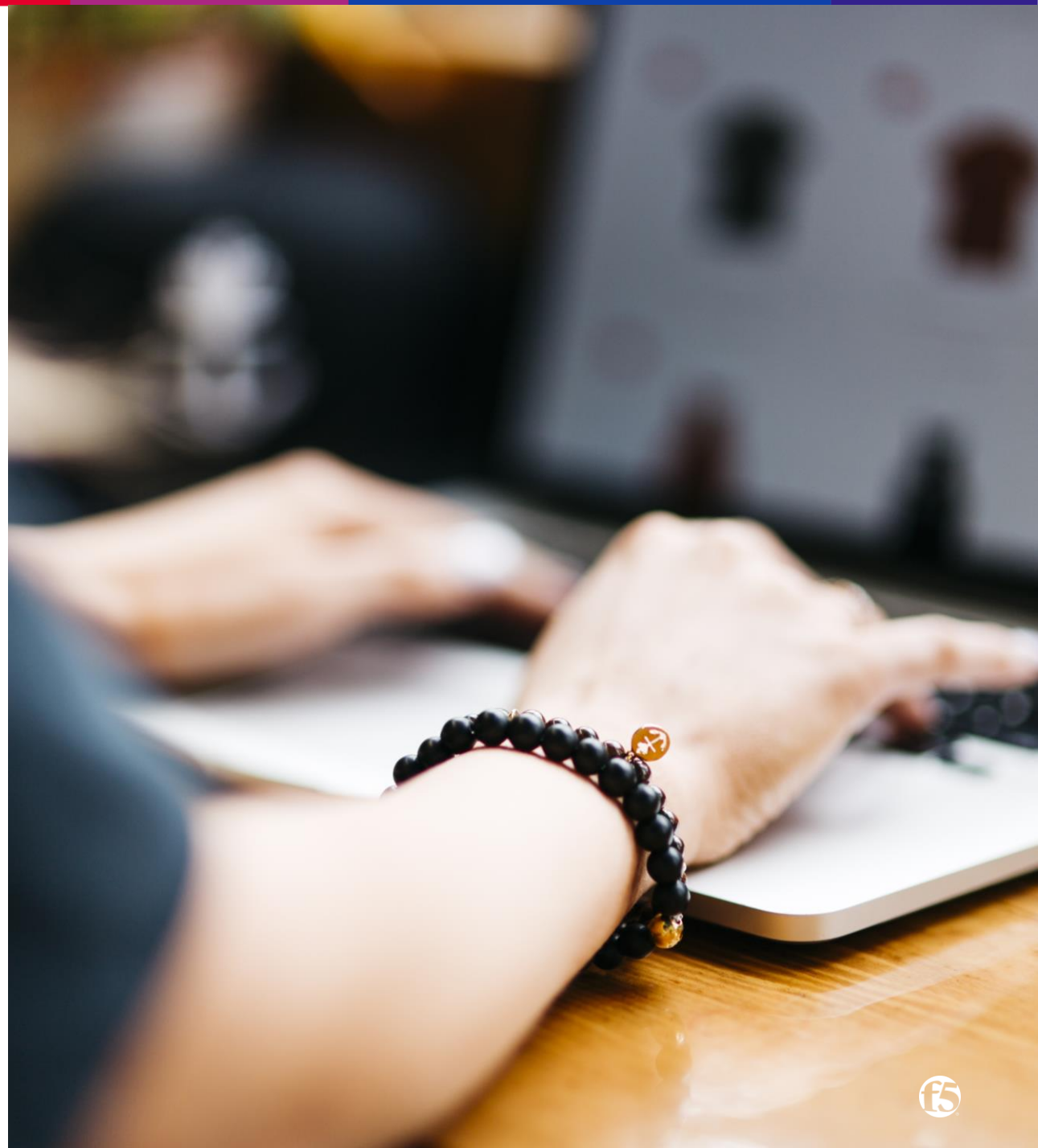
# Layer 7 DDoS Protection

# How?

- Begin with rate limiting as a first step
- Detect abuse of APIs at layer 7 (application layer)
- Use granular controls—one size does not fit all APIs
- Continually analyze and baseline each API's traffic
- Deny or limit based on IP address, region/country, ASN or TLS fingerprint, HTTP method, path, query parameters, headers, cookies, and more

# Malicious User Detection



# How?

- Analyze all client interactions, including with APIs
- Identify outliers
- Produce threat level and risk score for each client
- Continually adjust threat level and risk score based on subsequent interactions
- Continually adjust client access and permissions based on threat level and risk score

# Summary

# Key Takeaways

- See through the buzz and hype
- Push your vendors to articulate how they empower you to implement these 10 best practices
- Understand how your vendors leverage AI to improve API Security
- Be strategic and targeted with the API Security challenges you want to address with AI
- Track true positive and false positive rates
- Measure your performance and improvement around API Security
- Communicate successes to executives and the board in their language
- Adjust and iterate as necessary to continually improve