最新トレンドから見る APIセキュリティの必要性と F5 API Security 戦略

F5ネットワークスジャパン合同会社

ソリューションアーキテクト

小峰 洋一

アジェンダ

API マーケットの状況

API Security に必要なプラットフォーム

Shift-left と Shield-right で実現する
全段階で取り組む API Security

まとめ

API マーケットの状況

API セキュリティに関連したインシデント

Target	Impact
Trello	15M
Peloton	2.6M records
Duolingo	2.6M records
Coinbase	Fraudulent transactions
USPS	60M records
Venmo	207M records
Experian	10s of millions
Instagram	Account takeover
Optus	10M records
Bumble	95M records
T-Mobile	30M records

Target	Impact
Facebook	530M records
John Deere	Account harvesting
Twitter	5.4M records
Sumo Logic	Key leak
Pokemon Go	Data exposure
Yandex	Hacktivism
Zoom	Unauthorized access
Linkedin	700M
Dropbox	Key leak
Tesla Backup	Data exposure
First American	885M

Target	Impact
7-Eleven 7Pay	Account takeover
Tinder	Data exposure
Waze	Data exposure
Wordle	Data manipulation
Echelon	Data exposure
Clubhouse	1.3M
Parler	70TB data harvested
Grinder	Account takeover
Ring App	Data exposure
Plenty of Fish	Data exposure
JustDial	100M

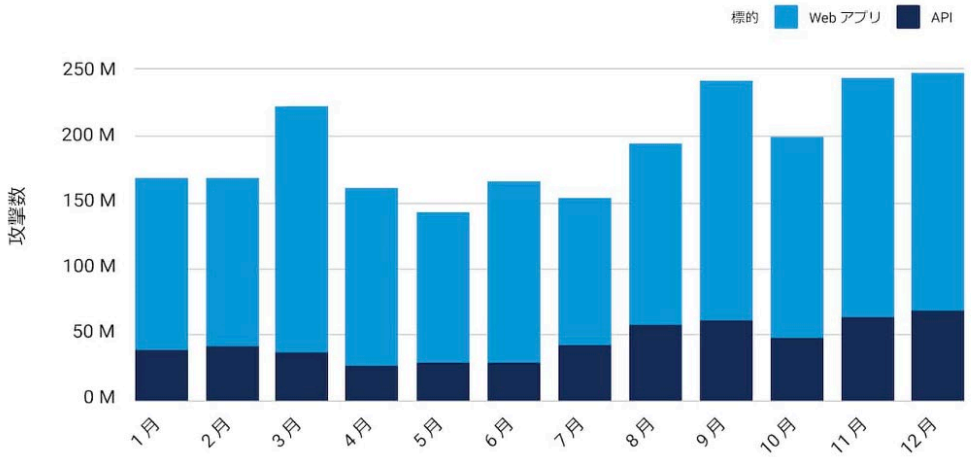
過去5年間で発生したAPI セキュリティに関連したインシデント（情報漏洩関連）

引用:”APISEC UNIVERSITY 2024 API Security Market Report”

2023年の日本におけるAPI攻撃状況

（トラフィックベース）

全体の**1/4** (23.4%) をAPIへの攻撃が占めている

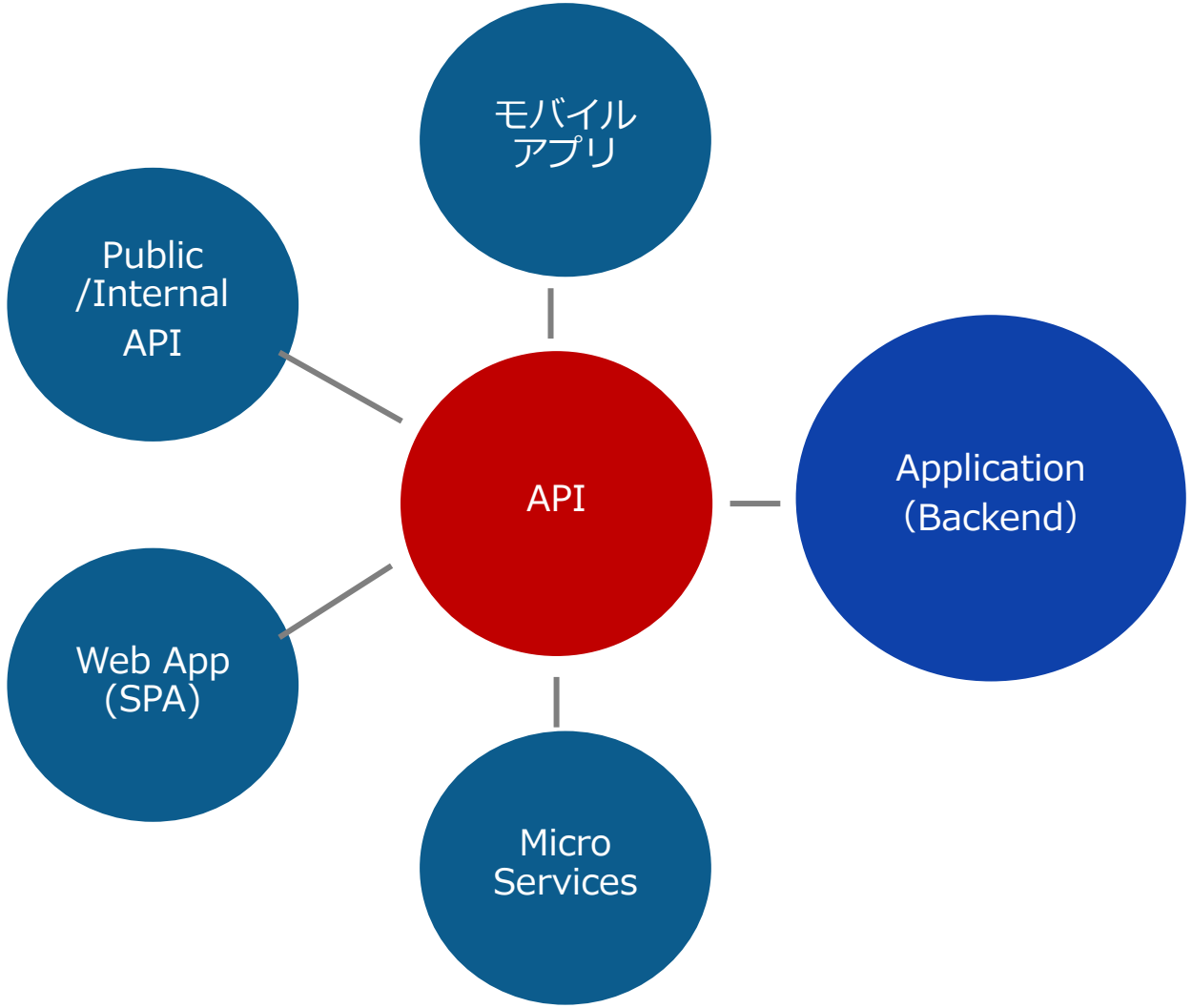


ブログ：影に潜んでいるAPIの脅威に光をあてる

API がセキュリティ上重要である理由

1. 重要なデータを保持するアプリケーションを、外部に公開する際の重要なポイント（各種インターフェースに対する窓口）に位置する

2. APIは、機密情報を含む重要データを保持するアプリケーションに、**“直接”**アクセスすることができ、設計上、**”強力な権限”（Create/Read/Update/Deleteの全て）**が実装されているケースが多い



API がセキュリティ上重要である理由

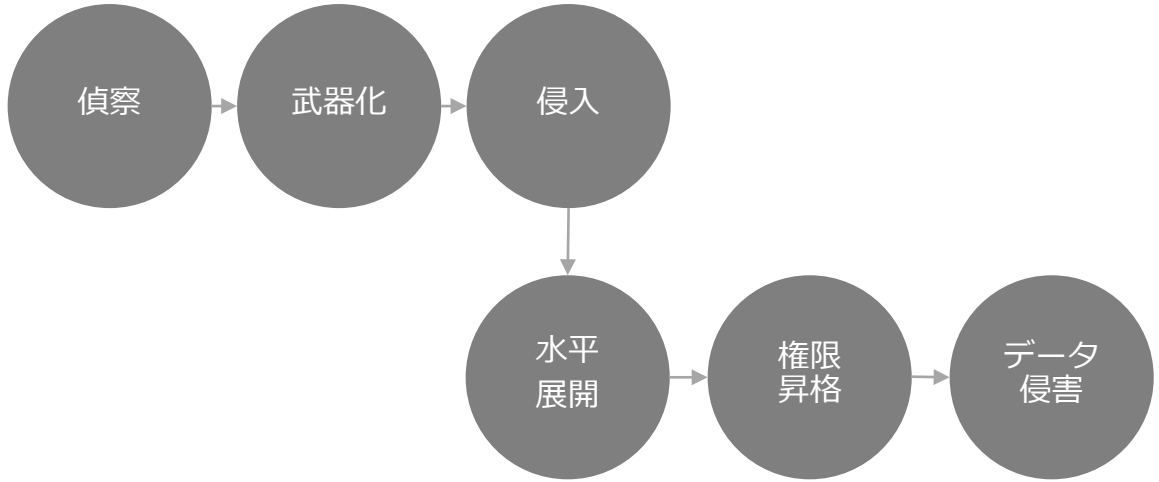
3 APIは、先の2つの特徴から、脆弱性が発見された時点で**即座にデータ侵害につながる悪用がされ易い**傾向にある。

旧来型サービスでは、攻撃が成立するまでに攻撃者が膨大な手順と技術力が必要であるのと対照的。

攻撃者が最も好む
エンドポイントがAPI

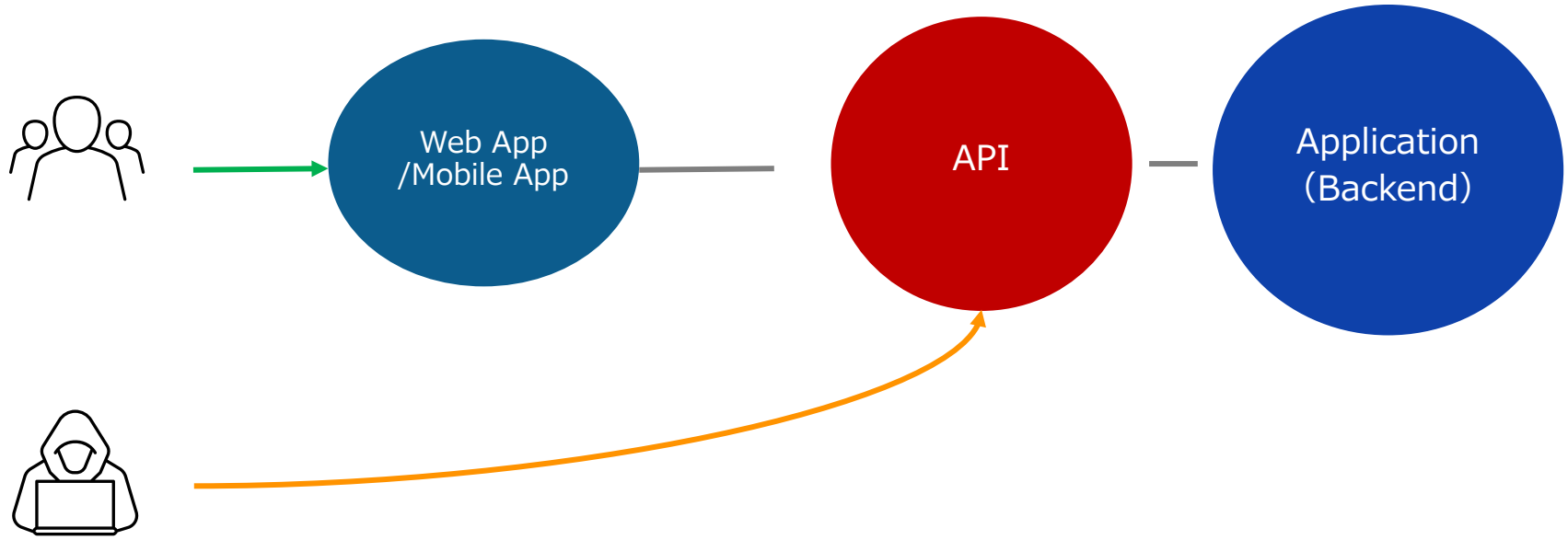
APIを標的としたデータ侵害までの攻撃ステップ

旧来型サービスを標的としたデータ侵害までの攻撃ステップ



API をターゲットにした攻撃の特徴

- Web/モバイルアプリで提供される**ユーザインターフェースを迂回し、APIのエンドポイントが直接ターゲット**にされる
- 従来のインジェクション攻撃(SQLi)等でだけでなく、**アプリケーションロジックの不整合や、認証不備、認可の不整合などを突いた攻撃**が多い



75%

（2024年）世界のインターネットトラフィックのうち、APIが占める割合

F5: 2024 Strategic Insights: API Security in APAC

90%

（2024年）APIを使っている開発者の割合

F5: 2024 Strategic Insights: API Security in APAC

31%

（2024年）シャドーAPIの割合

2024 API Security & Management Report

48%

（2023年）月に１回以上、APIインシデントに対応している企業、チーム

F5: 5 Cybersecurity Predictions for 2023

API に関わる数字

75%

（2024年）世界のInternet Trafficのうち、APIが占める割合

F5: 2024 Strategic Insights: API Security in APAC

31%

（2024年）シャドーAPIの割合

2024 API Security & Management Report

90%

（2024年）APIを使っている開発者の割合

F5: 2024 Strategic Insights: API Security in APAC

48%

（2023年）月に１回以上、APIインシデントに対応している企業、チーム

F5: 5 Cybersecurity Predictions for 2023

API に関わる数字

75%

（2024年）世界のInternet Trafficのうち、APIが占める割合

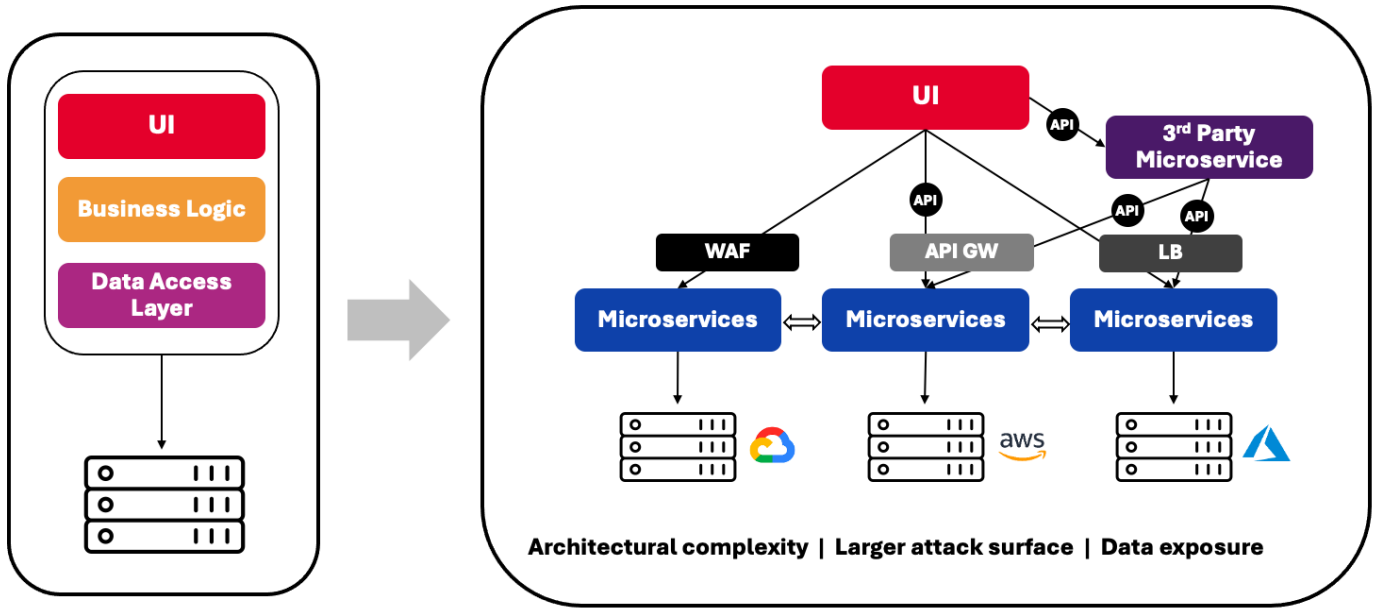
F5: 2024 Strategic Insights: API Security in APAC

90%

（2024年）APIを使っている開発者の割合

F5: 2024 Strategic Insights: API Security in APAC

- マイクロサービス化等によるアプリケーションの進化
- クラウドやオンプレ、エッジ等、分散環境の拡大
- モバイル、IoT等、アプリの多様化



APIの利用は更に拡大

API に関わる数字

攻撃の高度化、アプリ・環境の複雑化、組織の壁・・・

アプリの進化とセキュリティ基盤の進化が合っていない？

アプリに合わせて、**セキュリティのモダナイズが必要**では？

31%

（2024年）シャドーAPIの割合

2024 API Security & Management Report

48%

（2023年）月に１回以上、APIインシデントに対応している企業、チーム

F5: 5 Cybersecurity Predictions for 2023

API Security に必要なプラットフォーム

API Security の３つの要素

Access Control

- APIエンドポイントに対する認証認可の管理

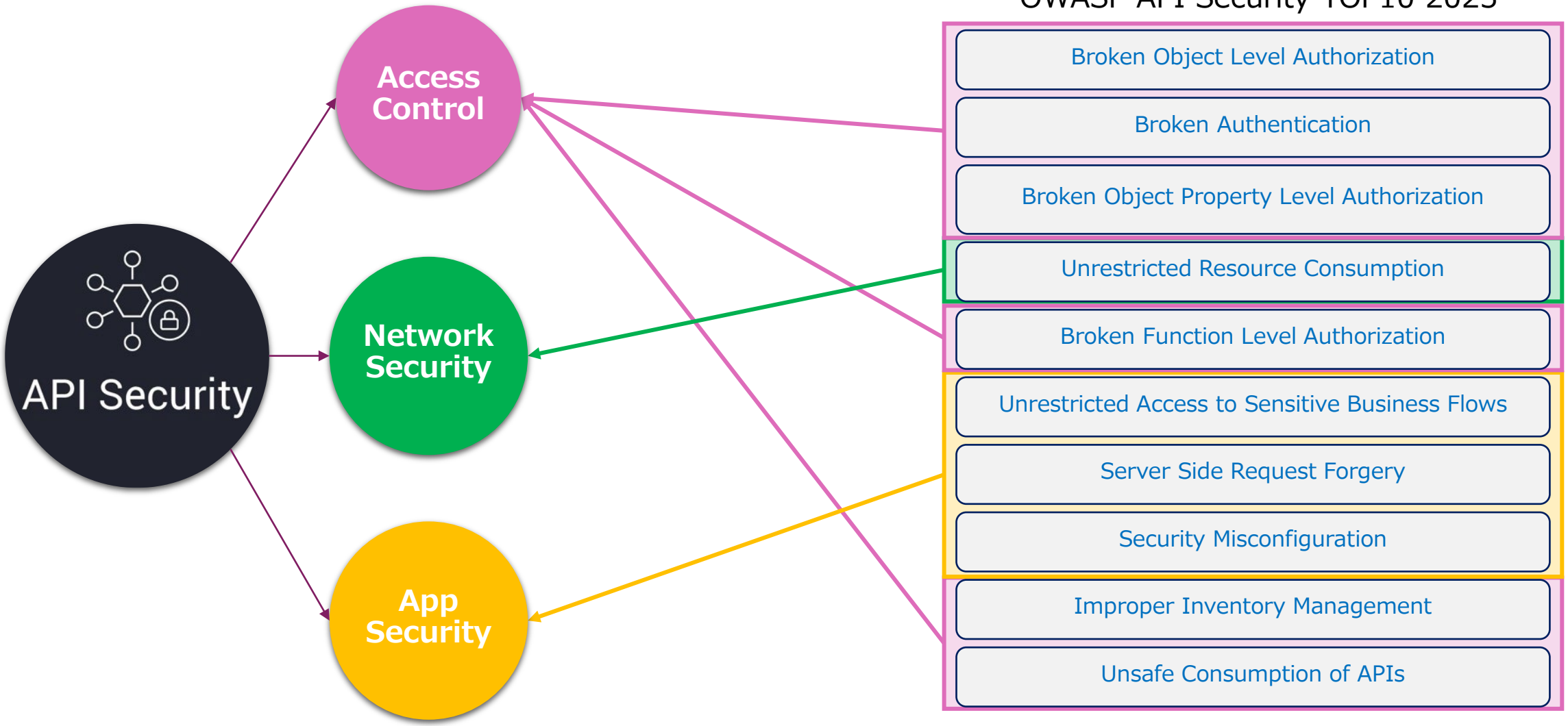
Network Security

- 安全なネットワーク通信（mTLS）
- ネットワークレベルで、不要なトラフィックを防ぐ（DDoS、レートリミット）

App Security

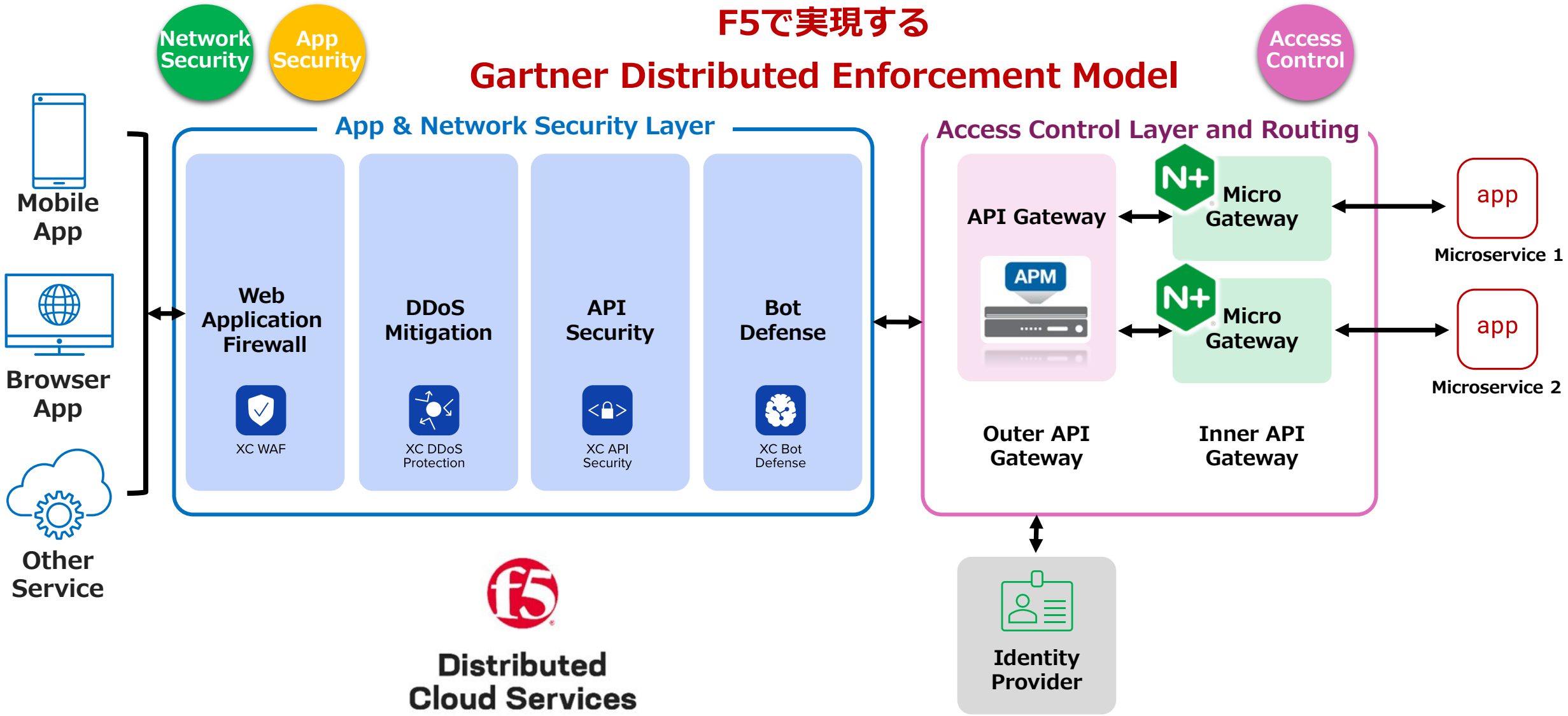
- 脆弱性を軽減
- 高度なBot対策技術によるAPI不正利用対策
- ペイロードセキュリティ（WAF）

API Security の３つの要素



１つのレイヤーだけではなく、多層面での対応が必要

F5 API Security リファレンスアーキテクチャ

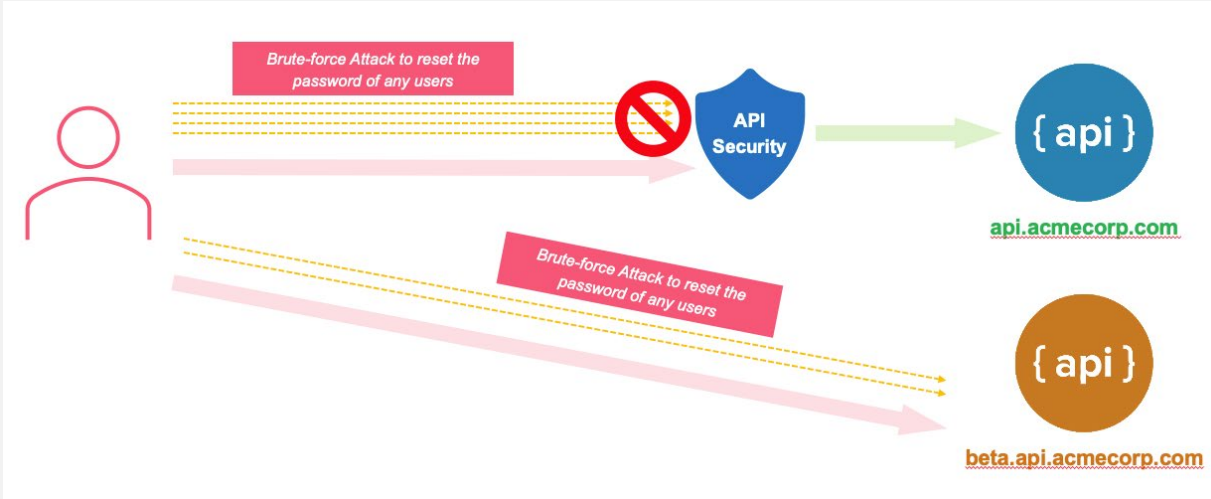


API9：不適切な資産管理 (Improper Inventory Management)

- 古い、もしくは不完全なAPIインベントリが原因で発生
- 管理されていない古いバージョンのAPIが問題を引き起こす可能性が高い
- **シャドーAPI**等の管理されていない不透明なAPIや、**ゾンビAPI**と呼ばれる忘れ去られたAPIが問題の例

修復するために

- 継続的な監視とAPIの検出が必要
- パブリッククラウド、プライベートクラウド、データセンター等、すべての場所でアクティブにネットワークトラフィックを監視することが必要
- 管理されていない隠れたAPI（シャドーAPI）を検出し、必要な管理ポリシーを適用

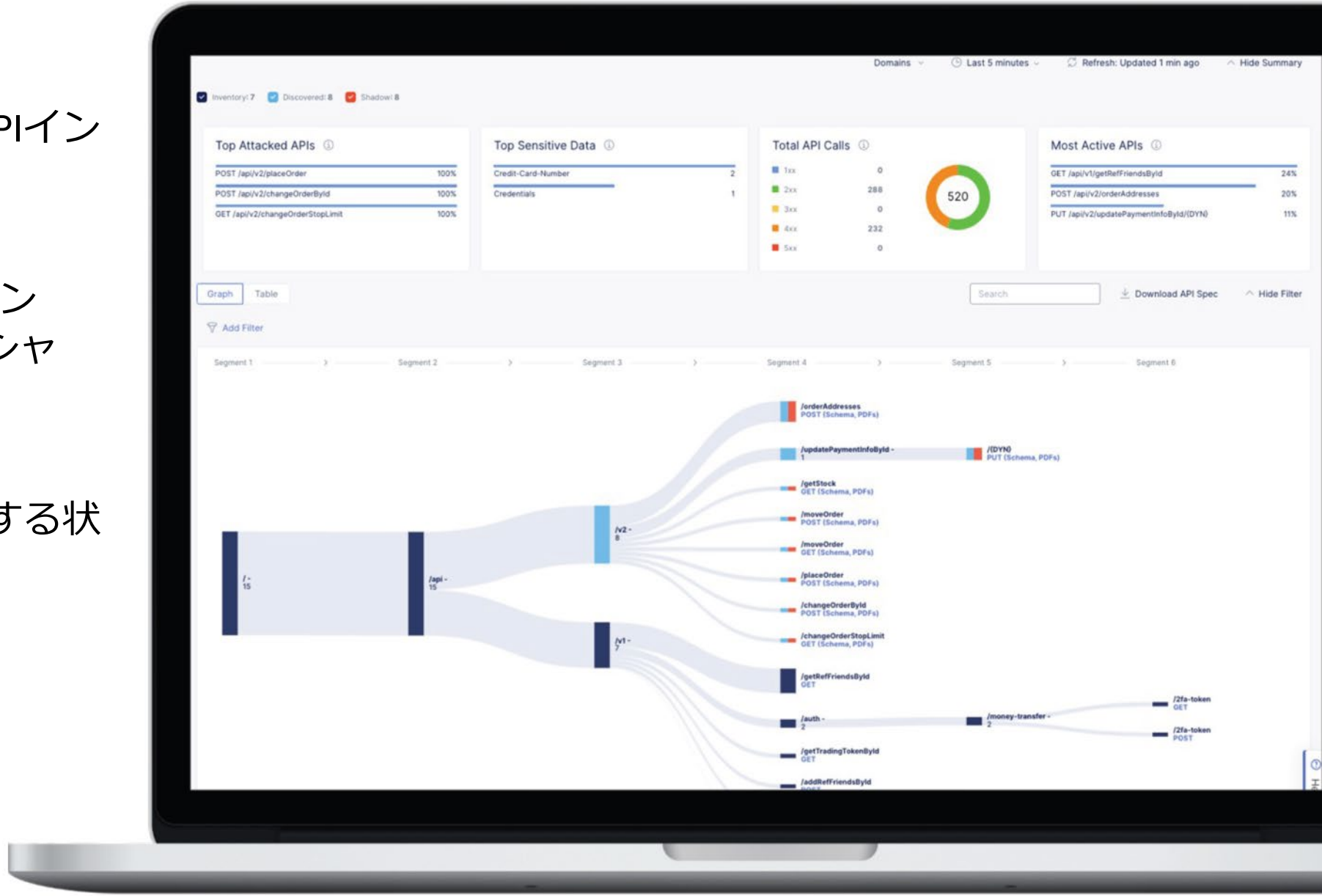


“…チームは*167*億を超える*API*トランザクションを分析し、*31%*、*50*億の悪意のあるリクエストが、シャドー*API*と呼ばれる未知の管理・保護されていない*API*をターゲットにしていることを発見しました”

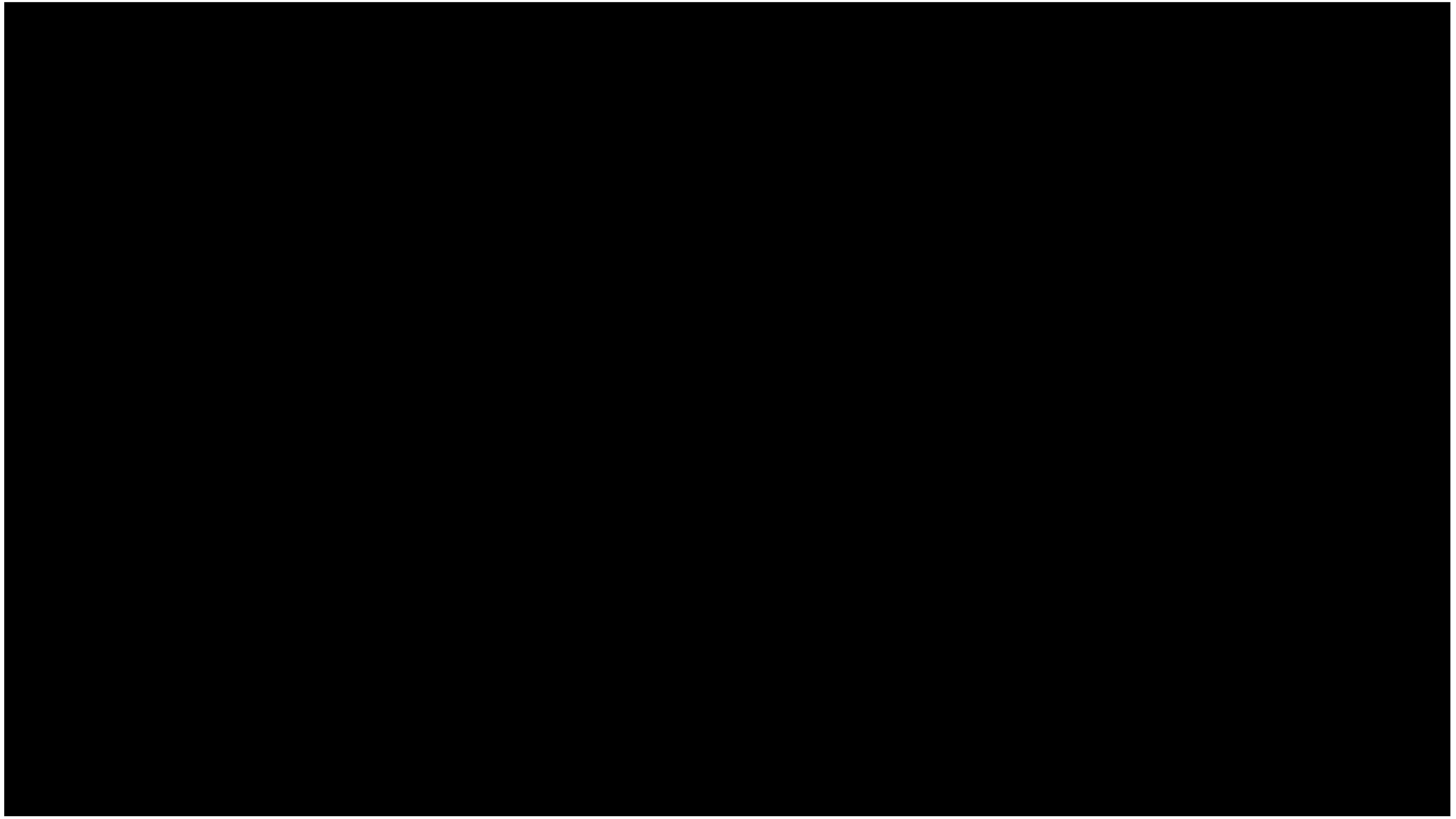
https://www.cpomagazine.com/cyber-security/shadow-api-is-the-leading-api-security-threat-with-over-5-billion-attacks-says-api-protection-report/

F5 API Security でのシャドー API 対策

- ✓ トラフィックを学習し、APIインベントリを動的に作成
- ✓ OpenAPI定義ファイルのインポート/エクスポートと、シャドーAPIの検出
- ✓ 各APIエンドポイントに対する状況を監視
  - エラー
  - レイテンシー
  - リクエストメトリクス
  - etc



F5 API Security でのシャドー API 対策 – デモ



https://www.youtube.com/watch?v=EDRAPD1G_aA

API1：オブジェクトレベルの認可の不備 (Broken Object Level Authorization)

ID: **1001**

API: /api/userinfo?id=**1001**

{name: Taro, Phone: 080xx}

API: /api/userinfo?id=**1002**

{name: Hanako, **Phone: 070xx**}

ID	name	Phone	Pic
1001	Taro	080xx	
1002	Hanako	070xx	
1003	Komine	090xx	
1004	Yoichi	090xx	

オブジェクトレベルのアクセスコントロールが実装されていないと

他人のデータを取得できてしまう

BOLA の事例

APPSECURE により2019年4月に発覚（BOLA等に関する不備）

新規ドライバー追加のAPIに、既に**登録済みの他人の電話番号**を指定

```
POST /p3/fleet-manager/¥_rpc?rpc=addDriverV2 HTTP/1.1
Host: partners.uber.com
{“nationalPhoneNumber”:”222333”,”countryCode”:”1"}
```

```
{
   “status”:”failure”,
   ”data”: {
      “code”:1009,
      ”message”:”Driver ‘47d063f8–0xx5e-xx’ not found”
   }
}
```

指定された電話番号のドライバーの**UUID**が含まれたエラーメッセージ

API3(2019): 過度なデータ公開

入手したUUIDを指定して**すべての個人情報を取得**

```
POST /marketplace/¥_rpc?rpc=getConsentScreenDetails HTTP/1.1
…
{“language”:”en”,”userUuid”:” 47d063f8–0xx5e-xx”}
```

{すべての個人情報とトークン}

API1: BOLA

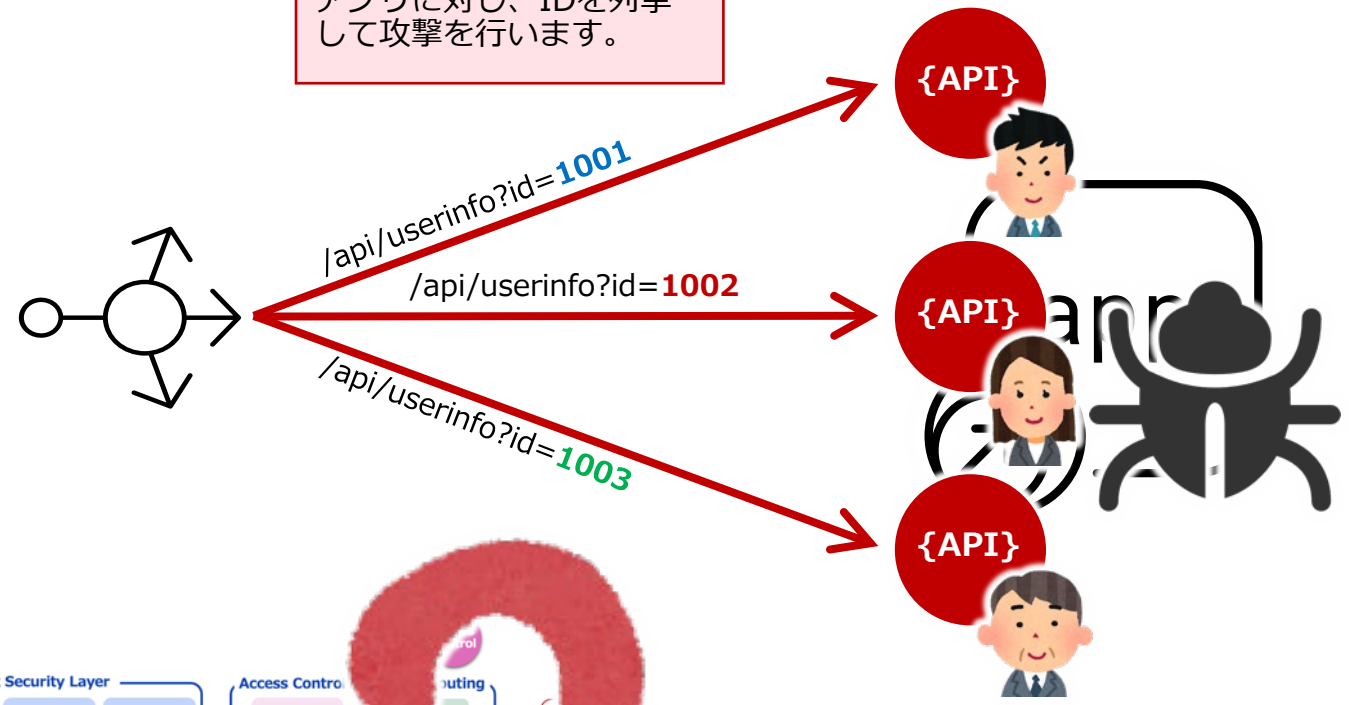
API3(2019): 過度なデータ公開

2段階の BOLA 攻撃

(1) 偵察フェーズ
ターゲットのアプリから有効なAPIエンドポイントを検出しようとします。
この段階では大量の403/404エラー応答が発生する可能性があります。

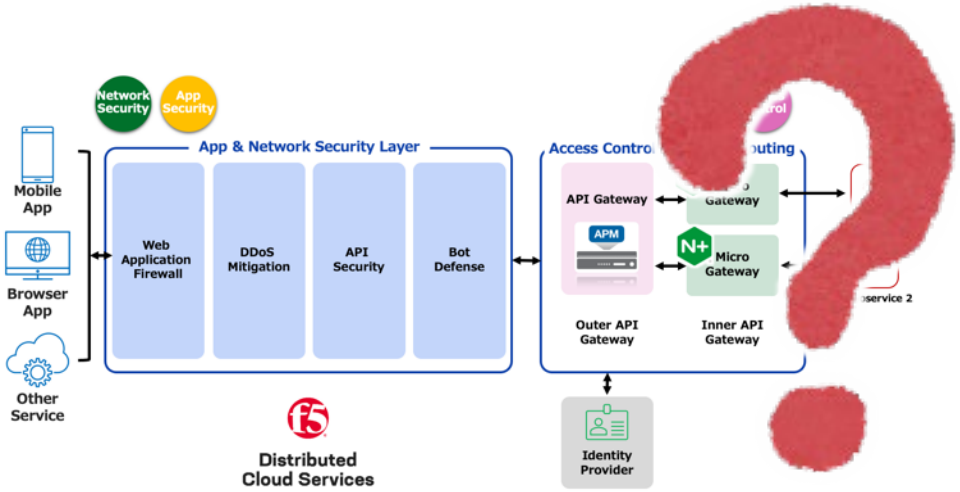
https://target.com/api/v1/userinfo
https://target.com/api/v1/users
https://target.com/api/v1/personalinfo
https://target.com/api/v1/subsinfo
…

(2) 実際の攻撃
BOLA攻撃に対して脆弱なアプリに対し、IDを列挙して攻撃を行います。



Distributed Cloud Services

WAAPでの対策



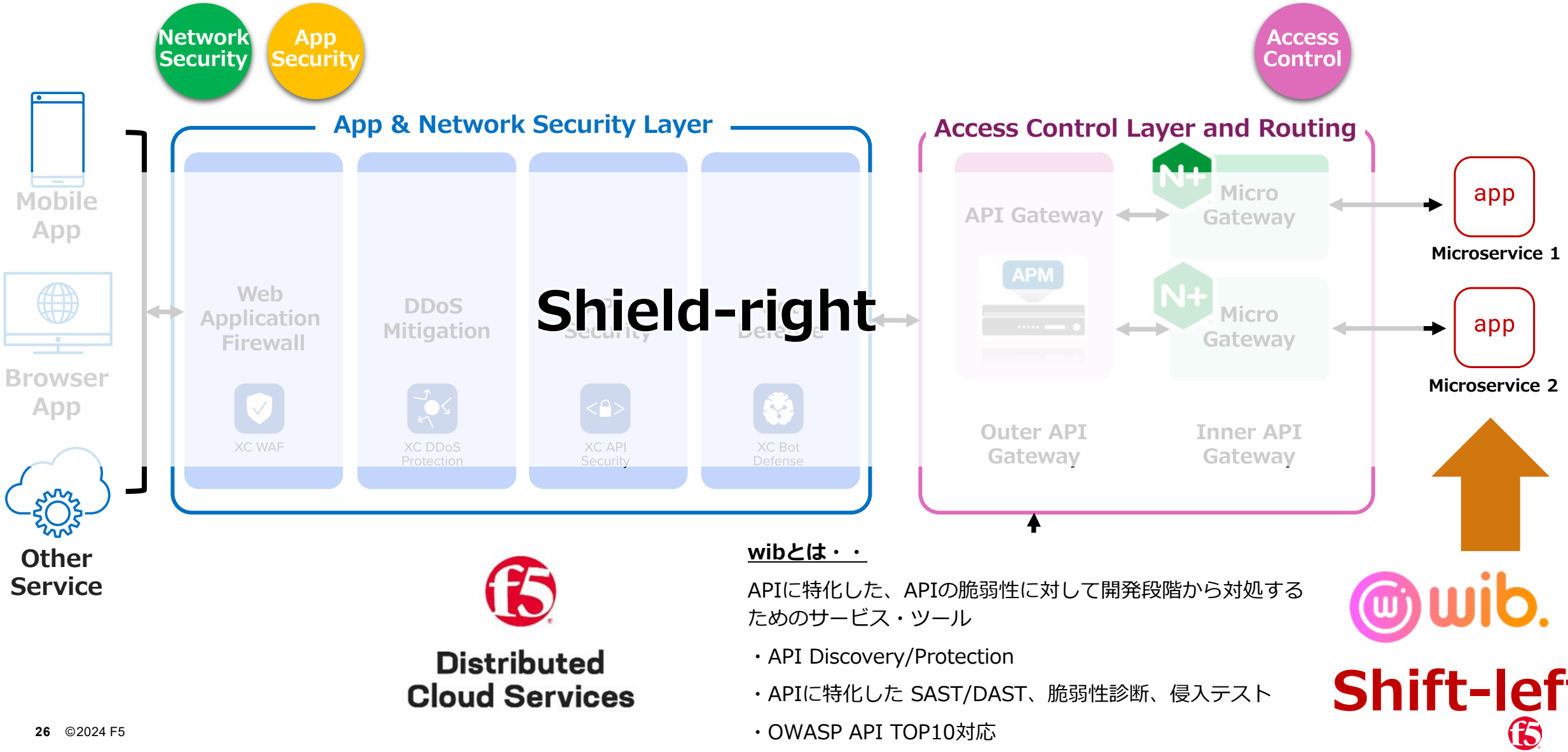
アプリの仕様に依存

→ 毎回プラットフォーム側で把握して対処するのは難しい

→ アプリ側でもしっかり API Security を意識する必要がある

Shift-left と Shield-right で実現する全段階で取り組む API Security

F5 API Security リファレンスアーキテクチャ



wibとは・・

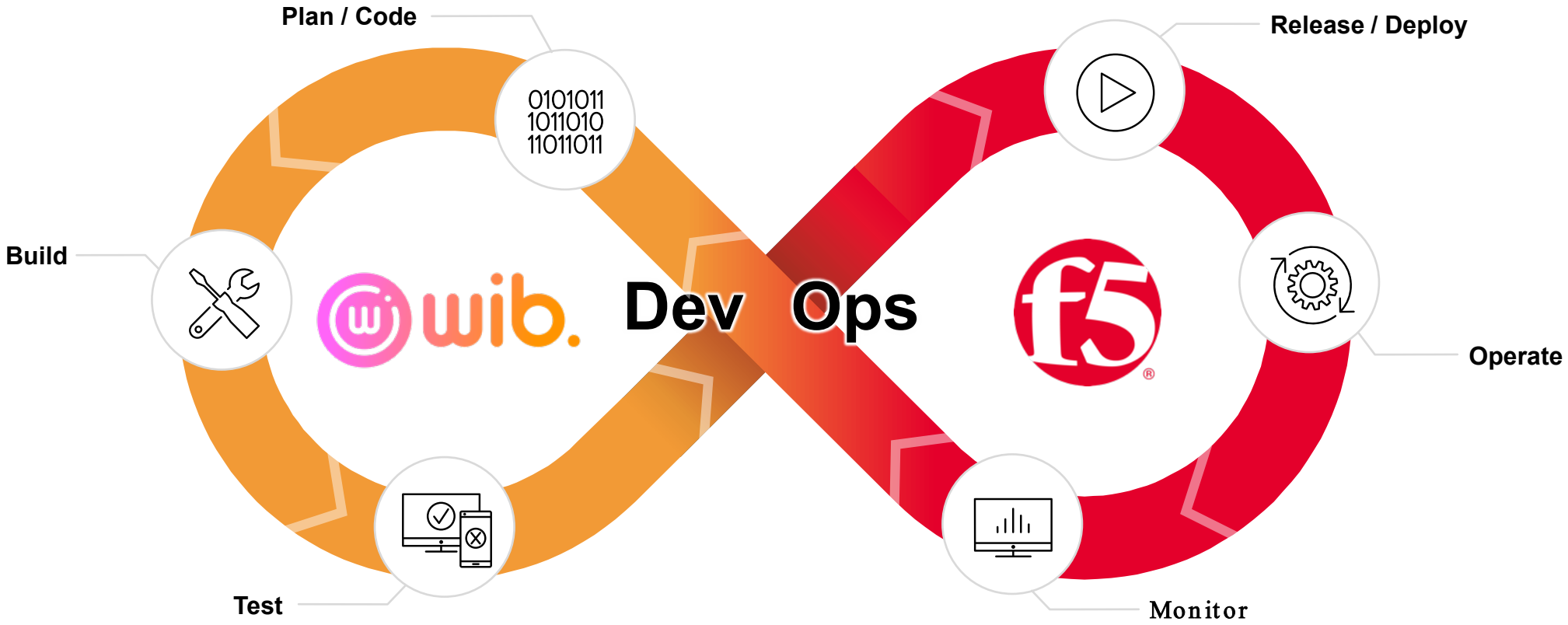
APIに特化した、APIの脆弱性に対して開発段階から対処するためのサービス・ツール

- API Discovery/Protection
- APIに特化した SAST/DAST、脆弱性診断、侵入テスト
- OWASP API TOP10対応

wib.

Shift-left

Shift-left & Shield-right の実現

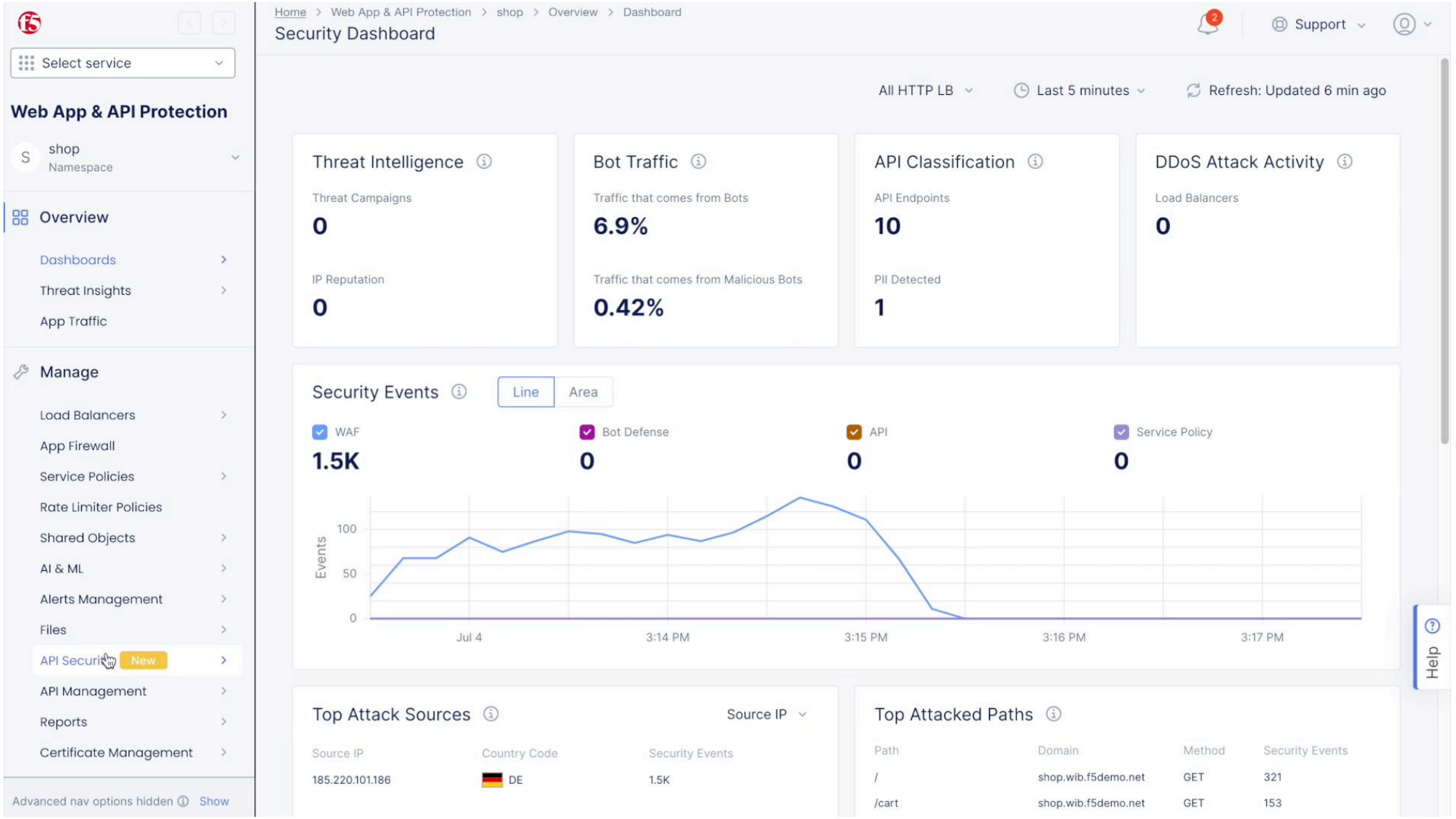


SHIFT LEFT | **SHIELD RIGHT**

Web/API scanning and testing	API code analysis	Web/API discovery and traffic analysis	Runtime protection and enforcement

Devとの連携を実現し、アプリ自体のセキュリティも高めることが可能に

Shift-left & Shield-right の実現 – デモ




```
  },
  "query":"mutation deleteReports($siteId: ID!, $reportKeys: [String]!) {
    {
      deleteReports(reportKeys: $reportKeys)
    }
  }"
}
```

指定された ID を持つ文書はそれ以上の権限チェックなしで削除されるため、ユーザーは他のユーザーの文書を削除できてしまう可能性があります。

防止方法

- ユーザーポリシーとヒエラルキーに依存する適切な認可メカニズムを実装します。
- クライアントからの入力を使用してデータベースのレコードにアクセスするすべての関数で、ログインしているユーザーがそのレコードに対してリクエストしたアクションを実行するためのアクセス権を持っているかどうかを、認可メカニズムを使用して確認します。
- レコードの ID にはランダムで予測不可能な値を GUID として使用することを推奨します。
- 認可メカニズムの脆弱性を評価するテストを作成します。テストが不合格となるような変更をデプロイしてはいけません。

参考資料

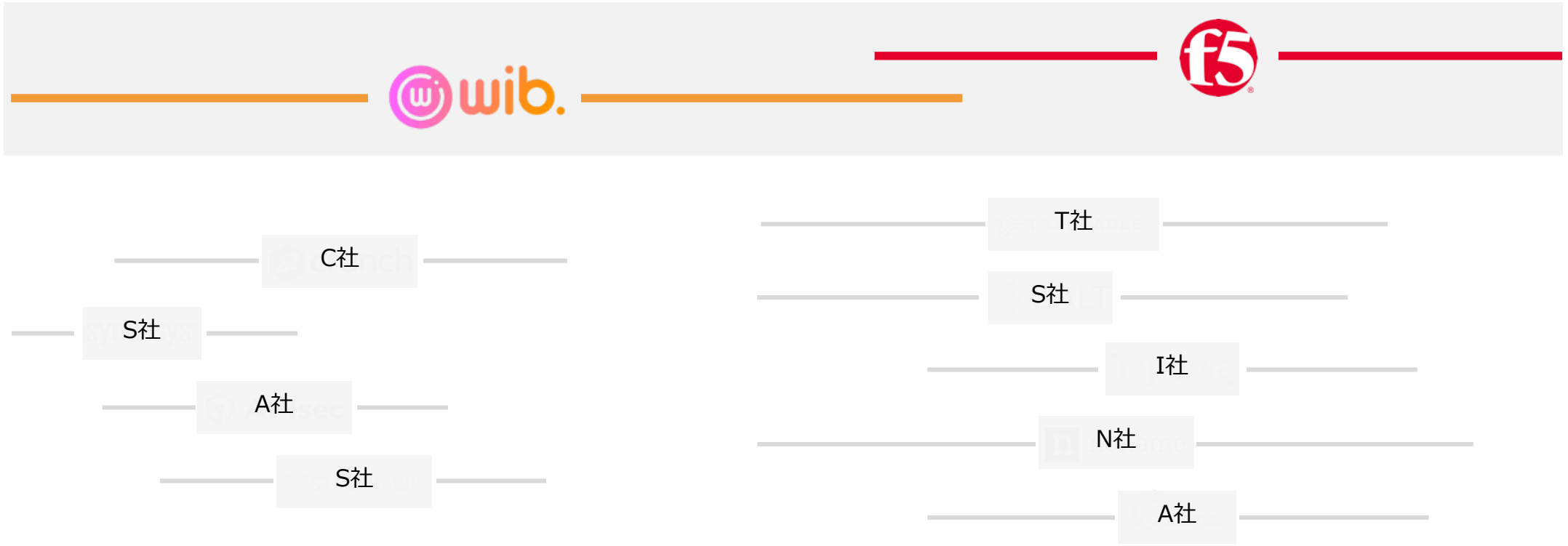
OWASP

- Authorization Cheat Sheet
- Authorization Testing Automation Cheat Sheet

その他

- CWE-285: Improper Authorization
- CWE-639: Authorization Bypass Through User-Controlled Key

API Security で最も広い範囲をカバー



まとめ

まとめ

API Securityって何やったらいいの？何から始めたらいいの？

1. まずは **API Discovery** から始めましょう。
   APIエンドポイントを可視化し、どこから対策していくか、優先順位を検討しましょう。

2. 対策としては、対象のAPIアプリに対して**WAAPを適用**し、APIアプリの**スキャンや侵入テスト等を実行**し、**リスクスコアを確認**しましょう。
   １つ１つ対策を実施し、セキュリティレベルをあげていきます。
   この際に、**OWASP API Security TOP10をベース**に、それぞれの脅威に対する対策や開発ガイドラインを作成することでほとんどのAPI脅威に対応できると考えられます。

3. 対策を実行したら常にスキャンやテスト、監視を行い、**常にAPIアプリをセキュアに**保っていきましょう。
   残念ながらセキュリティに終わりはありません。**簡単に継続運用できる仕組み**を構築し、対策していく必要があります。

F5 API Security で皆様のご支援ができますと幸いです。


App
World
2024