OWASP Top 10 2021

What's New?

Shain Singh, Principal Security Architect, F5

Zhen Yu Chew, BFSI Security Solutions Lead, F5

Our Speakers

Shain Singh

F5

Principal Security Architect

@shainsingh

Chew Zhen Yu

F5

BFSI Security Solution Lead

Agenda

OWASP Top 10 2021 Overview

Key Themes and Changes

The Bigger Picture

Attack Demo

Sophisticated Threats

Automated Attack Demo

The 2021 OWASP Top 10

A01
Broken Access Control

A02
Cryptographic Failures

A03
Injection

A04
Insecure Design

A05
Security Misconfiguration

A06
Vulnerable and Outdated Components

A07
Identification and Authentication Failures

A08
Software and Data Integrity Failures

A09
Security Logging and Monitoring Failures

A10
Server-Side Request Forgery (SSRF)

OWASP Top 10 2021 Key Changes

2017		2021
Focus on traditional web applications	→	Shift to modern architectures
Small data set (prescribed subset of 30 CWEs)	→	Data-driven process with 400 CWEs
Variety of risk factors, technical/business impacts	→	Recategorization around symptoms and root causes
Injection top risk for over 20 years	→	New wave of risk: insecure design and implementation

The Bigger Picture of OWASP

OWASP Top 10 2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

API Security Top 10 2019
API1:2019 Broken Object Level Authorization
API2:2019 Broken User Authentication
API3:2019 Excessive Data Exposure
API4:2019 Lack of Resources & Rate Limiting
API5:2019 Broken Function Level Authorization
API6:2019 Mass Assignment
API7:2019 Security Misconfiguration
API8:2019 Injection
API9:2019 Improper Assets Management
API10:2019 Insufficient Logging & Monitoring

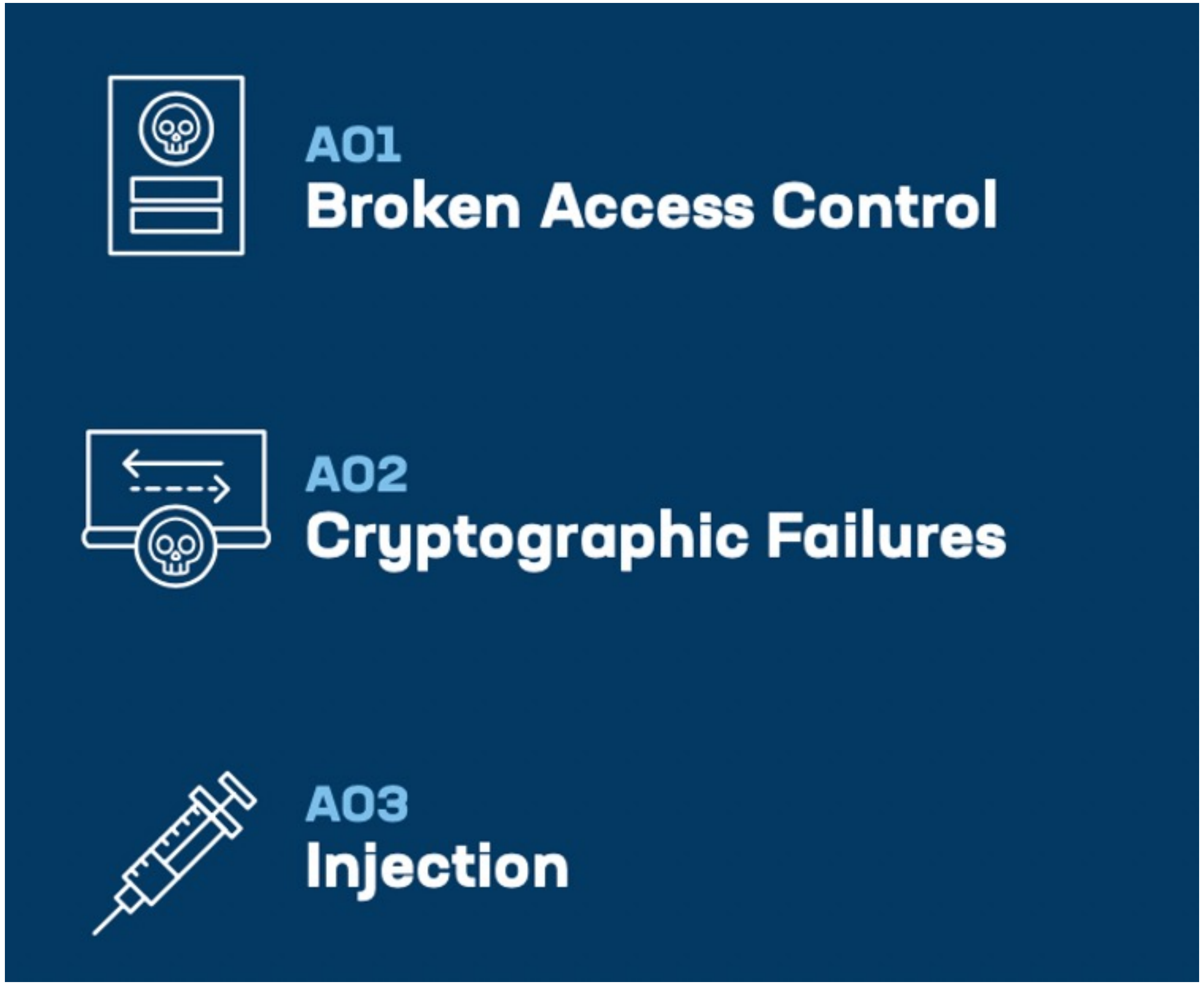
Bot Protection

OWASP Automated Threats
OAT-008 Credential Stuffing
OAT-015 Denial of Service

app app

API Protection

Act I: Break on Through (to the Other Side)



A01
Broken Access Control

A02
Cryptographic Failures

A03
Injection

F5 Labs Research

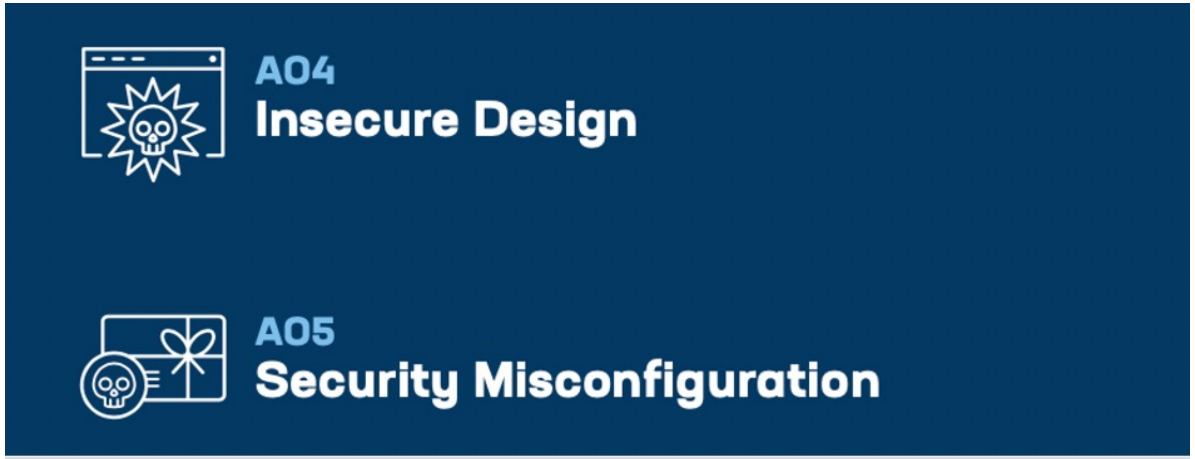
- 12 instances of specific clouds being compromised were due to a lack of access control
- Despite widespread TLS 1.3 adoption, old and vulnerable protocols are being left enabled
- The most common web app exploit reported was SQLi

F5 Solutions		
Full Proxy Architecture	*Custom SSL/TLS Stack*	*Attack Signatures*
Integrated AAA	*Secure Options (HSTS)*	*Metacharacter and parameter restrictions*
Secure Tokens	*FIPS*	*Evasion Detection*

Attack Demo

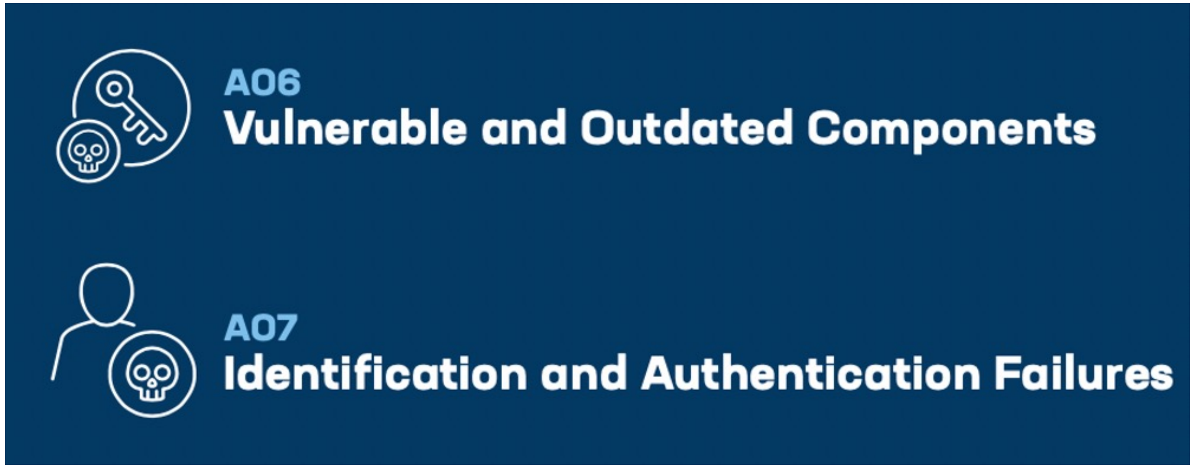
Protected by F5 Distributed Cloud Web App and API Protection

Act II: Weaknesses and *Inherent* Vulnerabilities



A04
Insecure Design

A05
Security Misconfiguration



A06
Vulnerable and Outdated Components

A07
Identification and Authentication Failures

F5 Labs Research

- ❖ *Cloud breaches occur most frequently through misconfigurations*
- ❖ *79% of libraries are never updated*
- ❖ *Average time to discover credential spill is 327 days*
- ❖ *Authentication attacks are the most frequent cause of breaches*

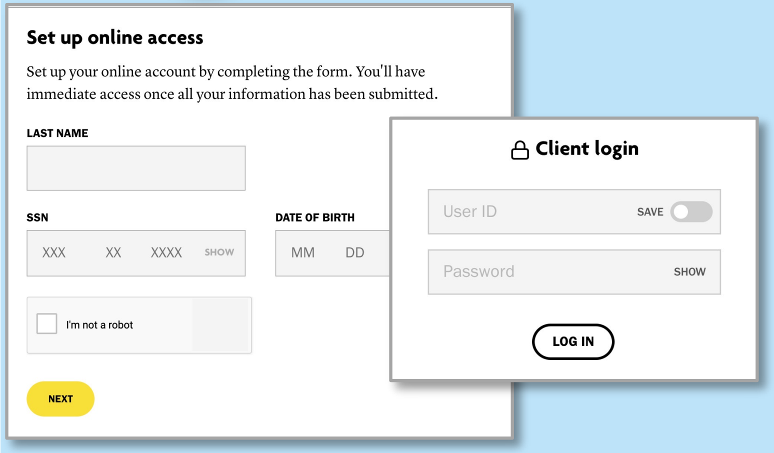
F5 Solutions

Zero-Trust Proxy	*Consistent Enforcement*	*Dynamic API Discovery*	*Tampering Prevention*
CI/CD Pipeline Integration	*Allowed URLs and Filetypes*	*DAST Integration*	*User Behavior Analysis (UBA)*
Bot Defense	*Flow Enforcement*	*ML-Based Assessment*	*Anomaly Detection*

These Attacks Impact Security, Risk, and Digital Teams

Security

Secure the application



Set up online access

Set up your online account by completing the form. You'll have immediate access once all your information has been submitted.

LAST NAME

SSN

XXX XX XXXX SHOW

DATE OF BIRTH

MM DD

□ I'm not a robot

NEXT

Client login

User ID SAVE

Password SHOW

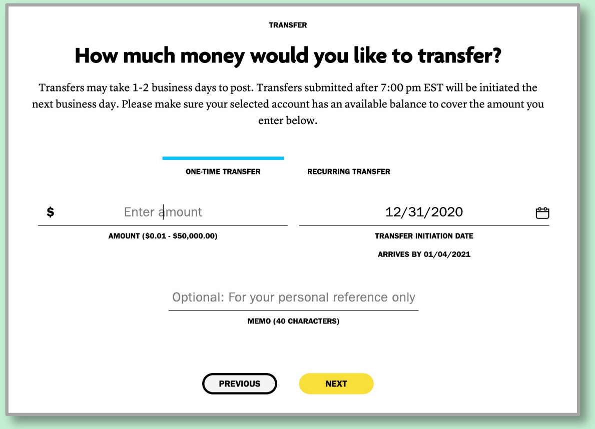
LOG IN

Web application firewall; Bot detection; API security, App Security, Access control, DDoS…

Data breaches, Credential Stuffing, Brand Damage

Risk

Protect the business



TRANSFER

How much money would you like to transfer?

Transfers may take 1-2 business days to post. Transfers submitted after 7:00 pm EST will be initiated the next business day. Please make sure your selected account has an available balance to cover the amount you enter below.

ONE-TIME TRANSFER RECURRING TRANSFER

$ Enter amount

AMOUNT ($0.01 - $50,000.00)

12/31/2020

TRANSFER INITIATION DATE

ARRIVES BY 01/04/2021

Optional: For your personal reference only

MEMO (40 CHARACTERS)

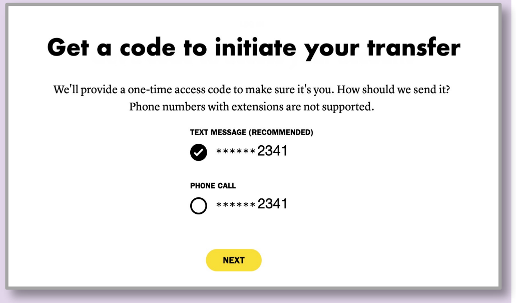
PREVIOUS NEXT

Identity Proofing; Social Engineering; Account Protection; Payment Protection; Abuse; Behavior...

Fraud Loss, Trust & Safety, Customer friction

Digital

Remove friction



Get a code to initiate your transfer

We'll provide a one-time access code to make sure it's you. How should we send it? Phone numbers with extensions are not supported.

TEXT MESSAGE (RECOMMENDED)

● ******2341

PHONE CALL

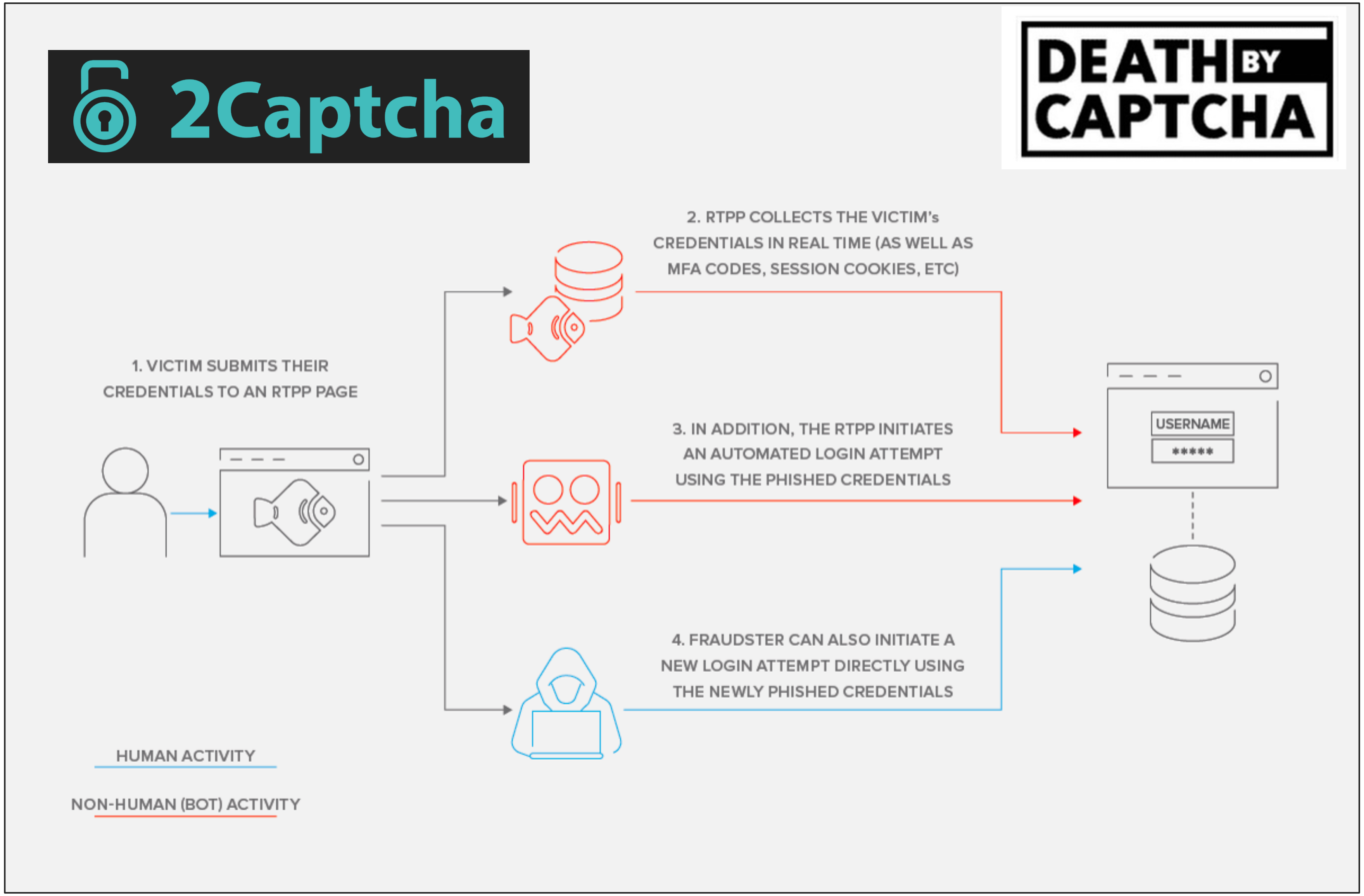
○ ******2341

NEXT

2FA; MFA; Cookies…

Acquistion & Growth

Sophisticated Attackers can Bypass MFA and CAPTCHA



1. VICTIM SUBMITS THEIR CREDENTIALS TO AN RTPP PAGE

2. RTPP COLLECTS THE VICTIM's CREDENTIALS IN REAL TIME (AS WELL AS MFA CODES, SESSION COOKIES, ETC)

3. IN ADDITION, THE RTPP INITIATES AN AUTOMATED LOGIN ATTEMPT USING THE PHISHED CREDENTIALS

4. FRAUDSTER CAN ALSO INITIATE A NEW LOGIN ATTEMPT DIRECTLY USING THE NEWLY PHISHED CREDENTIALS

HUMAN ACTIVITY

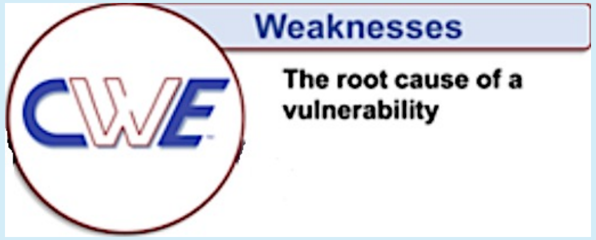
NON-HUMAN (BOT) ACTIVITY

OWASP and Automated Attacks

OWASP TOP 10

A07:2021-Identification and Authentication Failures

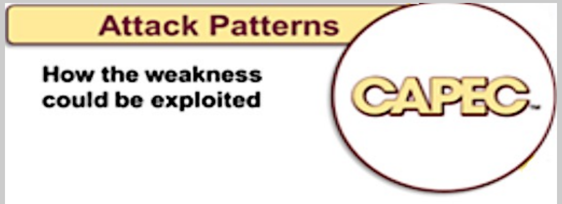
Groups weaknesses as high-level awareness



Class : CWE-287: Improper Authentication

Base : CWE-309: Use of Password System for Primary Authentication

Leads to potential attack patterns



CAPEC-600: Credential Stuffing

Leads to different offensive techniques

Automated Attack Demo

Protected by F5 Distributed Cloud Bot Defense

Act III: Unintended Risk

A08
Software and Data Integrity Failures

A09
Security Logging and Monitoring Failures

A10
Server-Side Request Forgery (SSRF)

F5 Labs Research

- *"If DevSecOps is enforced properly, it would be very difficult to cheat the system and deploy things that bypass the pipeline"*
- *Insufficient logging and monitoring is a significant subset of API security incidents*
- *The risk of third-party breaches emerging for cloud customers is significant*

F5 Solutions

Attack Signatures (deserialization)	*Universal Visibility*	*SSRF Violation Protections*
CI/CD Pipeline Integration	*Remote High-Speed Logging*	*Allowed URLs/Filetypes*
JSON/XML/HTTP validation	*Sensitive Log Masking*	*URL/Parameter Flow Enforcement*

F5 Distributed Cloud Web App and API Protection

Effective Security

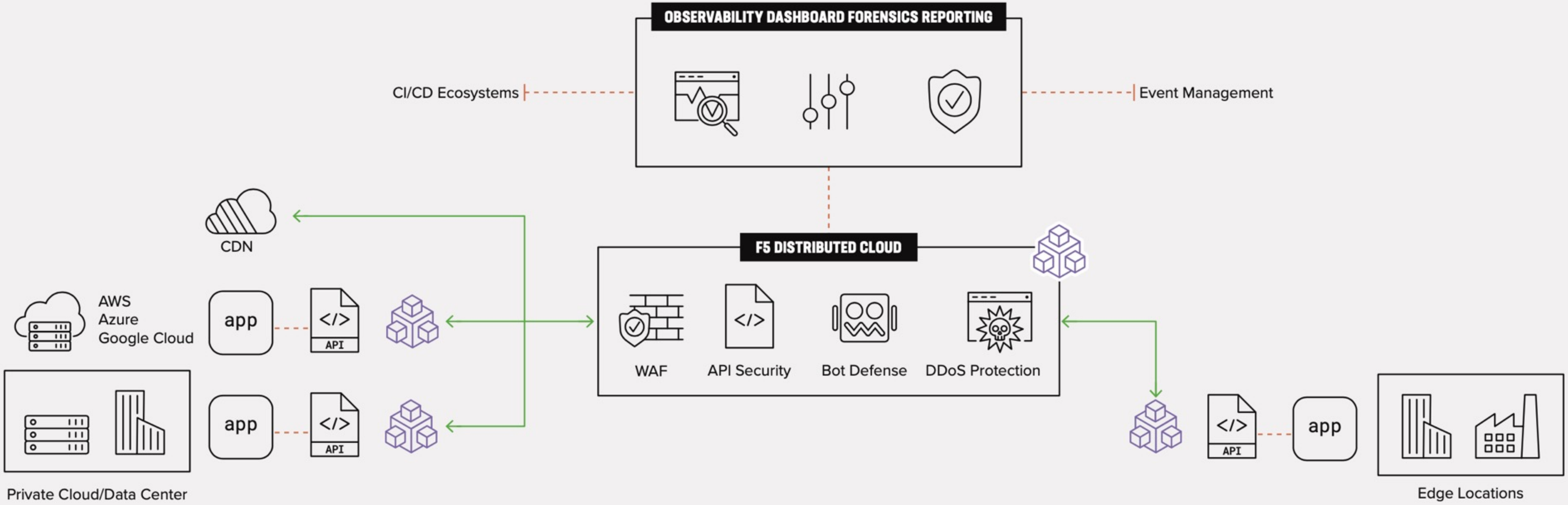
Maintains resilience with minimal customer friction and false positives

Easy-to-Operate

Self-service deployment with low operational complexity

Distributed Platform

Universal visibility and consistent policy enforcement across architectures



Key Takeaways

- The OWASP Top 10 continues to provide key security guidance for protecting *all* web apps

- There is broad consensus within the security community that a combination of Web App, API and Automated Threat Protection solutions are needed

- F5 Distributed Cloud provides effective security in an easy-to-operate, distributed platform to protect web apps and APIs across clouds and architectures

Resources

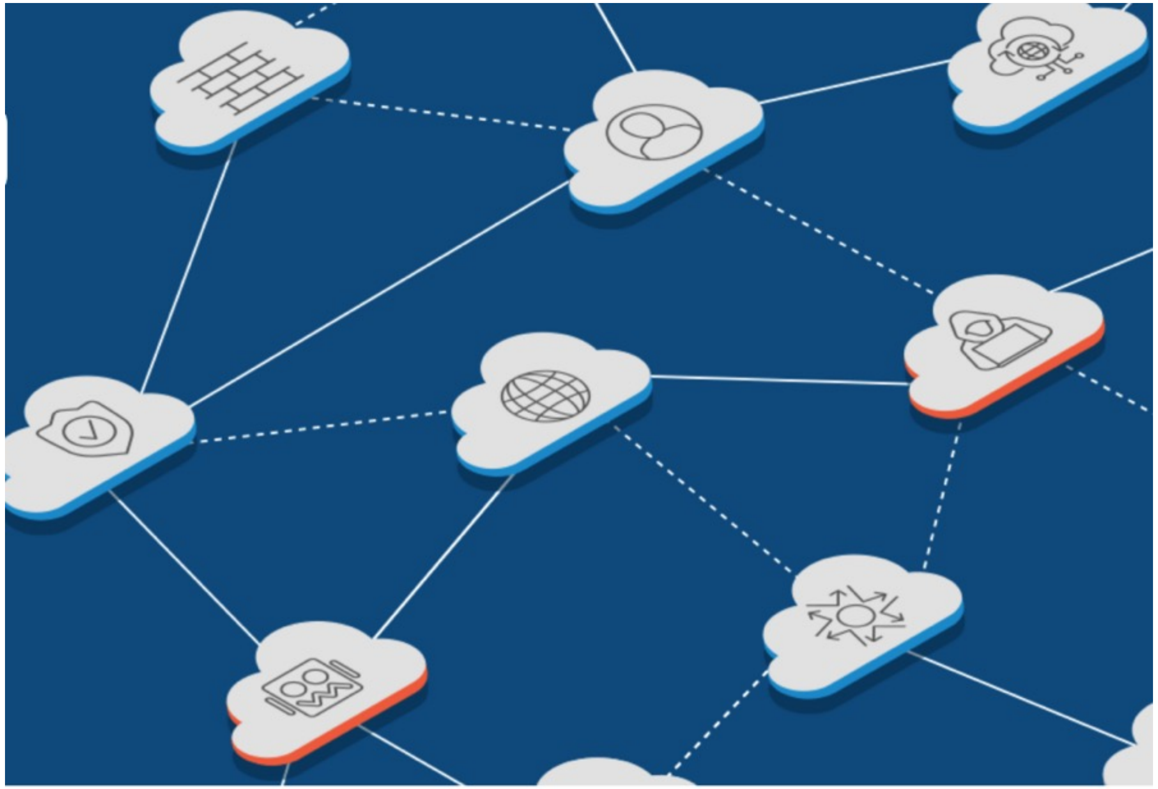
OWASP Top 10 2021 eBook

OWASP Top 10 2021 Lightboard Lesson Series

WAAP Buying Guide Digital Article

Choosing the WAF That's Right for You Guide

F5 Application Security Solutions



Thank you for listening!