

OWASP Top 10 API security risks for 2023

A. Singh, T. Richabadas

An aerial photograph of a rugged coastline. The left side shows dark, turbulent ocean waves crashing against a rocky shore. A road runs along the right side of the image, with a small red car visible on it. The overall scene is dark and moody, with the text overlaid on the left side.

What's new with the OWASP Top 10 API Threats?

What's changed in the OWASP Top 10 API Threats

OWASP Top 10 API Threats 2019

Broken Object Level Authorisation

Broken User Authentication

Excessive Data Exposure

Lack of Resources & Rate Limiting

Broken Function Level Authorisation

Mass Assignment

Security Misconfiguration

Injection

Improper Assets Management

Insufficient Logging & Monitoring

OWASP Top 10 API Threats 2023

Broken Object Level Authorisation

Retained

Broken Authentication

Updated

Broken Object Property Level Authorisation

Updated

Unrestricted Resource Consumption

Updated

Broken Function Level Authorisation

Retained

Server-Side Request Forgery

New

Security Misconfiguration

Retained

Lack of Protection from Automated Threats

New

Improper Assets Management

Retained

Unsafe Consumption of APIs

New



What's changed?

Authorisation is the largest challenge for API Security

- Broken Object Level Authorisation (BOLA)
- Broken Object Property Level Authorisation (BOPLA)
 - Combines Excessive Data Exposure and Mass Assignment
- Broken Function Level Authorisation (BFLA)

New: Server-Side Request Forgery

- Also shows up on the new Top 10 Web Threats List

Automated Threats (Bots) are new introduced to the list

Unsafe consumption of APIs

Poll Question

An aerial photograph of a rugged coastline. The ocean is dark blue with white foam from waves crashing against dark, rocky cliffs. A paved road with yellow and white lane markings runs along the edge of the cliffs. A small red car is visible on the road, driving away from the viewer. The overall scene is dramatic and scenic.

An aerial photograph of a dark, heavily cracked and textured surface, likely asphalt or a similar material. The cracks are irregular and deep, creating a complex pattern across the entire frame. In the bottom right corner, a small white car is visible, driving along a road that runs vertically. The overall tone is dark and moody, with a focus on the texture and the small vehicle providing a sense of scale.

Examples of recent breaches



Eight T-Mobile breaches since 2019

- Two in 2023 alone so far
- Multiple breaches due to unprotected APIs

Latest API breach revealed in Jan 2023

- Data of 37M customers breached
- Attack started in November 2022

Actual attack method is unknown

- Likely issues that led to breach
 - Lack of API visibility
 - Lack of API governance
 - BOLA & Automated attacks
 - Unrestricted resource consumption
 - AuthN & AuthZ failures



API breached in September 2022

- Testing API exposed on the Internet
- No AuthN or AuthZ on the API
- No other protection on the API, including logging/monitoring

Multiple OWASP Top 10 vulnerabilities

- BOLA
- Broken Authentication
- Broken Object Property Level Authorisation
- Unrestricted Resource Consumption
- Improper Assets Management



API vulnerability discovered in 2021

- Unauthenticated API access
 - Allowed viewing of sensitive info of all users
 - View live class statistics
 - Show all the info even if user was in private mode
- Single request could show id's of all users in a class
 - IDs could be used to view sensitive info of a user
- Unauthenticated GraphQL endpoints

OWASP vulnerabilities

- BOLA
- Security Misconfiguration
- Unrestricted Resource Consumption
- Lack of protection from automated threats



GraphQL query batching vulnerability

- Query batching is a feature
- Ability to send as many GraphQL queries as you want in one request, and declare dependencies between the two

Can be used to bypass rate limits

- Multiple login attempts in a single request
- Multiple MFA tokens in a single request

OWASP vulnerabilities

- Broken authentication
- Unrestricted Resource Consumption

Poll Question



An aerial photograph showing a dark, winding road that curves along the edge of a dense green forest. To the right of the road is a large, calm body of water, likely a lake or a wide river. The water's surface is dark and reflects the surrounding environment. The text "API use has grown drastically, but they are drastically unprotected" is overlaid in white, serif font across the middle of the image, spanning both the road and the water.

API use has grown drastically, but
they are drastically unprotected

An aerial photograph of a dark, winding road that curves through a dense, green forest. The road is visible on the left side of the frame, curving towards the bottom left. The trees are thick and cover the majority of the landscape.

New risk vectors created by accelerated digital transformation

New deployment models, including multi-cloud and hybrid deployments

- Use of Containers/Kubernetes, Serverless & allied development methodologies

New technology stacks & protocols

- REST APIs with XML, JSON and GraphQL
- Protocols like WebSocket, HTTP/2, gRPC, HTTP/3...
- Low-Code/No-Code versus “traditional” LAMP/JAM



APIs growth is
exploding in
businesses

98%

Using or planning to use internal APIs

94%

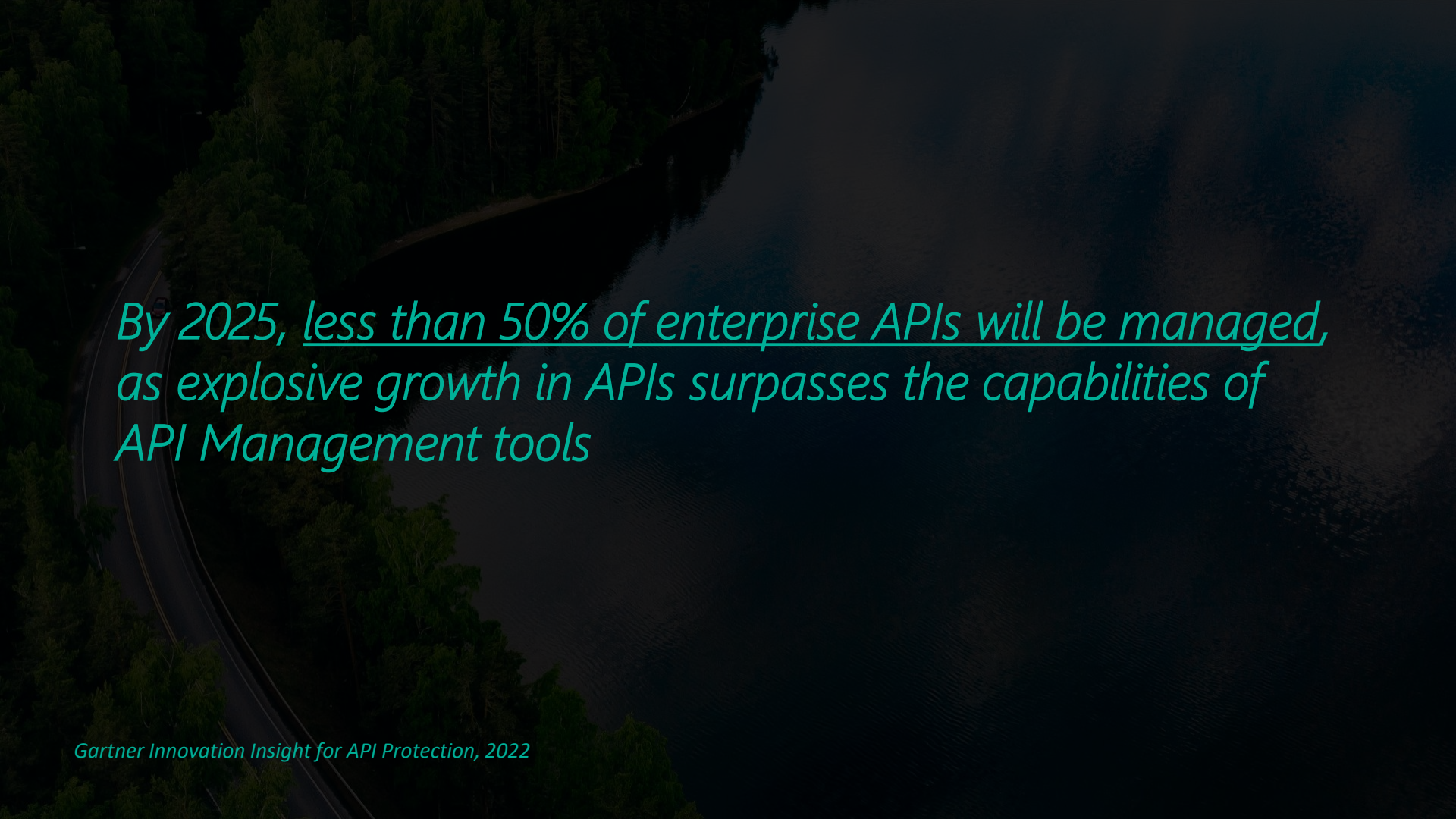
Using or planning to use Public APIs

90%

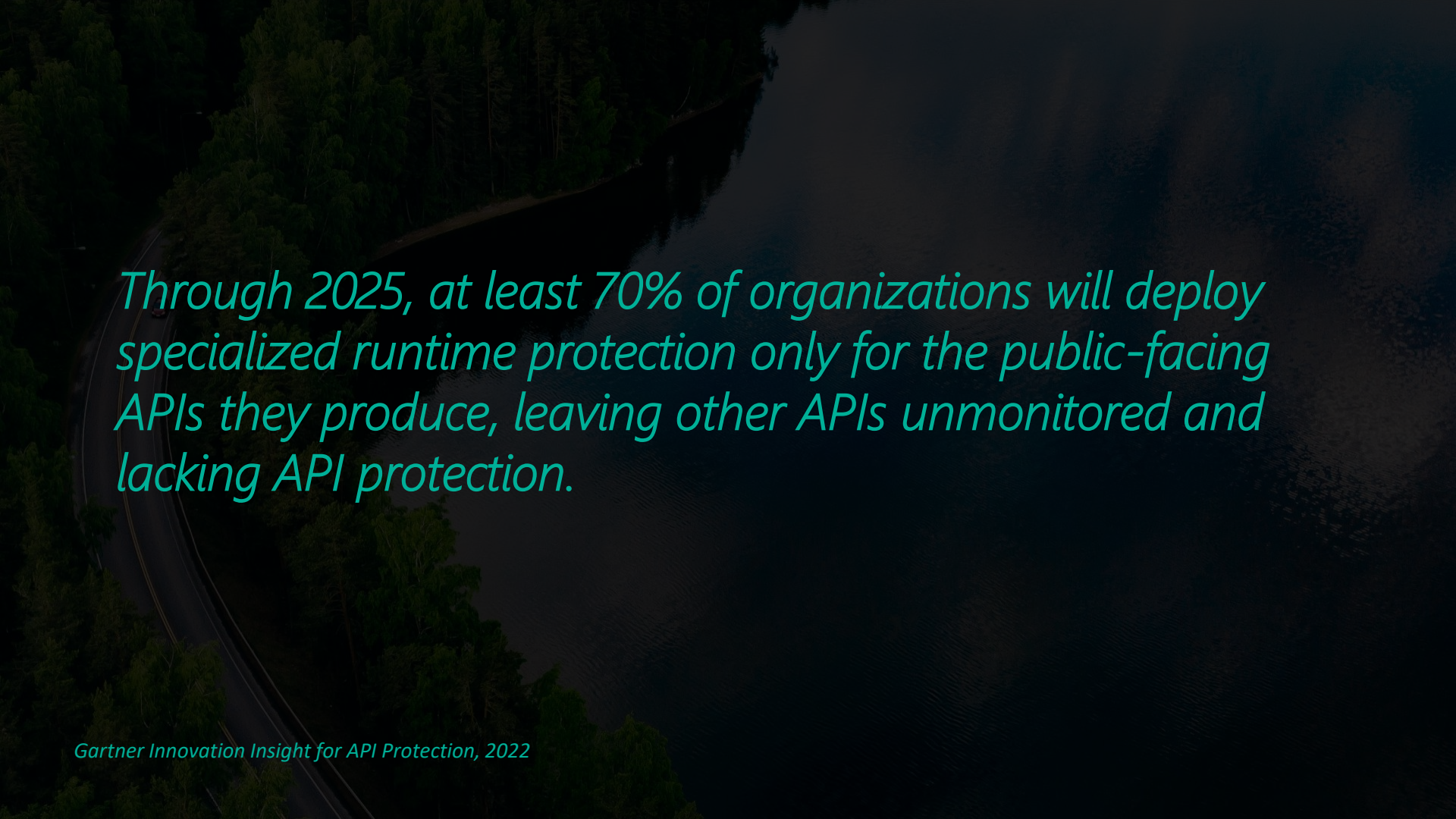
Using or planning to use private APIs
from Partners

80%

Provide or plan to provide publicly
exposed APIs

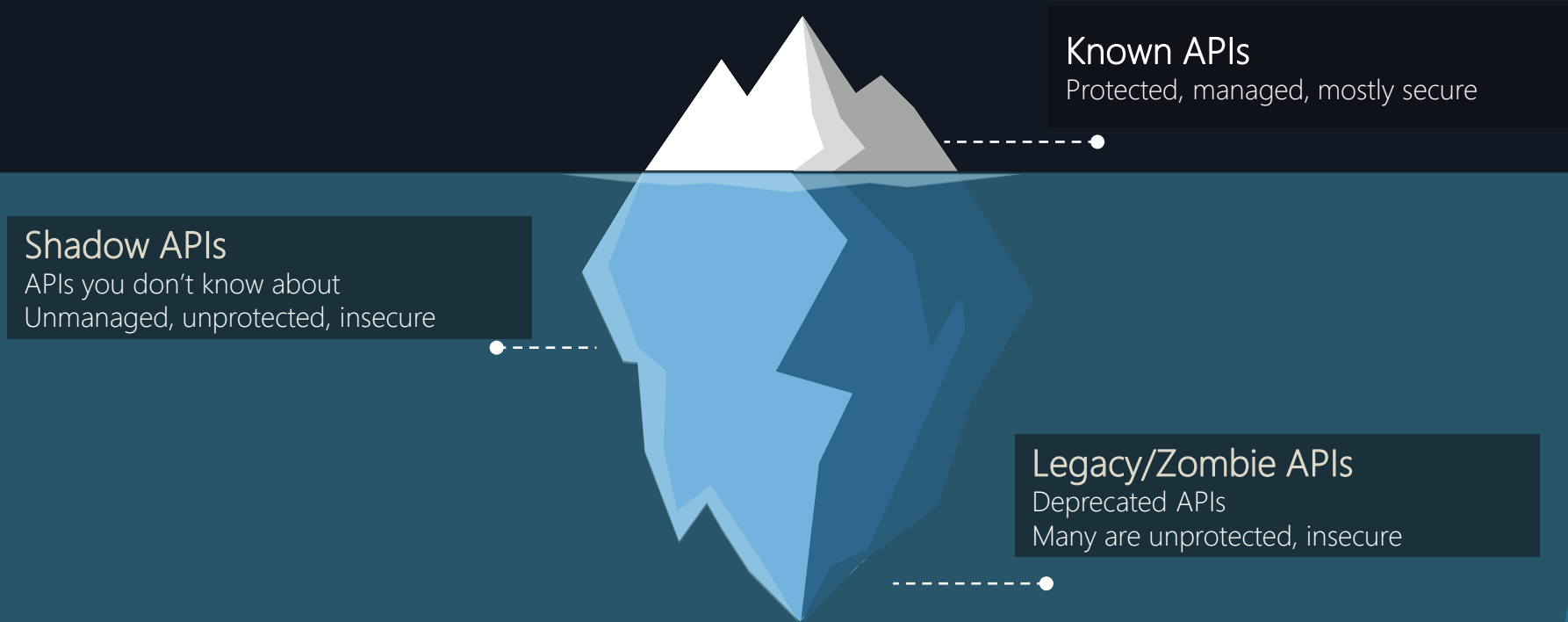
An aerial photograph of a dark, winding road that curves along the edge of a calm lake. The road is bordered by a dense forest of tall, thin trees. The water in the lake is dark and reflects the surrounding greenery. The overall scene is serene and somewhat somber due to the dark tones.

*By 2025, less than 50% of enterprise APIs will be managed,
as explosive growth in APIs surpasses the capabilities of
API Management tools*

An aerial photograph of a dark, winding road that curves along the edge of a calm lake. The road is flanked by a dense forest of tall, thin trees. The water in the lake is dark and reflects the surrounding greenery. The overall scene is serene and somewhat somber due to the dark tones.

Through 2025, at least 70% of organizations will deploy specialized runtime protection only for the public-facing APIs they produce, leaving other APIs unmonitored and lacking API protection.

You can only manage and secure the APIs you know about



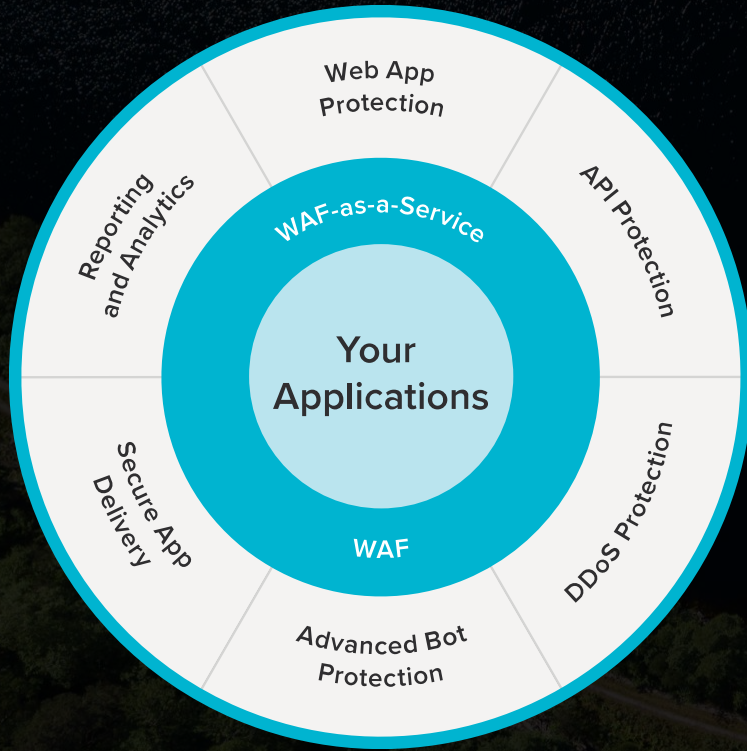
An aerial photograph showing a dark asphalt road with yellow double lines curving through a dense green forest. To the right of the road is a calm, dark blue lake that reflects the sky. A small dark car is visible on the road. The text "Poll Question" is overlaid in white serif font on the left side of the image.

Poll Question

An aerial photograph showing a wide, dark river flowing from the top right towards the bottom left. The river is bordered on the left by a dense, green forest. A narrow, light-colored path or road runs along the edge of the forest, following the curve of the river. The overall scene is captured in a high-contrast, slightly desaturated style, emphasizing the textures of the water and the foliage.

Barracuda Application Protection

Introducing Barracuda Application Protection



Protect all your apps and APIs with Barracuda Application Protection

- Comprehensive protection for web apps and APIs
- Easy to operationalise and manage
- Protect your apps everywhere
- Scale to secure any size of application

An aerial photograph of a winding coastal road. The road is light-colored and curves from the bottom left towards the top right. A small red car is visible on the road, near the bottom left. To the left of the road is a rocky coastline with waves crashing against the shore. To the right of the road is a dense green forest. The overall scene is a scenic coastal landscape.

API Protection with Barracuda Application Protection

Stop API attacks and prevent data breaches

Discover and secure your XML, JSON and GraphQL APIs

- Machine-Learning powered continuous API discovery to secure growing applications
- Stop bot and DDoS attacks, and improve API performance
- Secure API delivery for your critical applications
- Shift left without slowing down
- Gain full visibility into your applications and traffic.

An aerial photograph of a dry, winding riverbed with visible sand and silt patterns. A paved road with a dashed white line runs along the right edge of the frame. The overall image has a dark, muted color palette with a teal overlay on the left side.

The impact of the new OWASP Top 10 API threats list

Evolution rather than revolution

Moving to continuous monitoring and security

AuthN and AuthZ are broken (40% of the list)

API Management is complex and difficult (50% of the list)

Risk categories have been broadened

Broken Object Level Authorization	Broken Object Level Authorization	Retained
Broken Object Property Level Authorization	Broken Object Property Level Authorization	Updated
Excessive Data Exposure	Broken Object Property Level Authorization	Updated
Lack of Resources & Rate Limiting	Unrestricted Resource Consumption	Updated
Broken Function Level Authorization	Broken Function Level Authorization	Retained
Mass Assignment	Server-Side Request Forgery	New
Security Misconfiguration	Security Misconfiguration	Retained
Injection	Lack of Protection from Automated Threats	New
Improper Assets Management	Improper Assets Management	Retained
Insufficient Logging & Monitoring	Unsafe Consumption of APIs	New



An aerial photograph of a dry, winding riverbed with visible sand and silt patterns. A paved road with a dashed white line runs along the right edge of the frame. The text "About Barracuda Networks" is overlaid in white serif font on the left side of the image.

About Barracuda Networks

The background of the slide features five tall flagpoles with blue and white Barracuda flags flying against a dark, overcast sky. The flags are positioned in front of a building with a prominent, sloped, corrugated metal roof. In the distance, a dark, forested hillside is visible. The overall lighting is dim, creating a professional and serious atmosphere.

Barracuda protects the people, data, apps, and networks of more than 200,000 organizations worldwide by providing cloud-first security solutions that are easy to buy, deploy, and use

Delivering at scale

Emails archived
(per week)

1.3B

Malicious emails blocked
(per week)

158M

Application and bot attacks
blocked (per day)

200M

Cloud-to-Cloud Backup
data stored

53PB

RMM and Intronis
backup agents deployed

500K

Zero-day attacks blocked
(per day)

5M

Barracuda Application Protection

2003

First WAF
Sold

2/5

Top US
Banks Using
Barracuda

4K+

WAFs in
Largest
Deployment

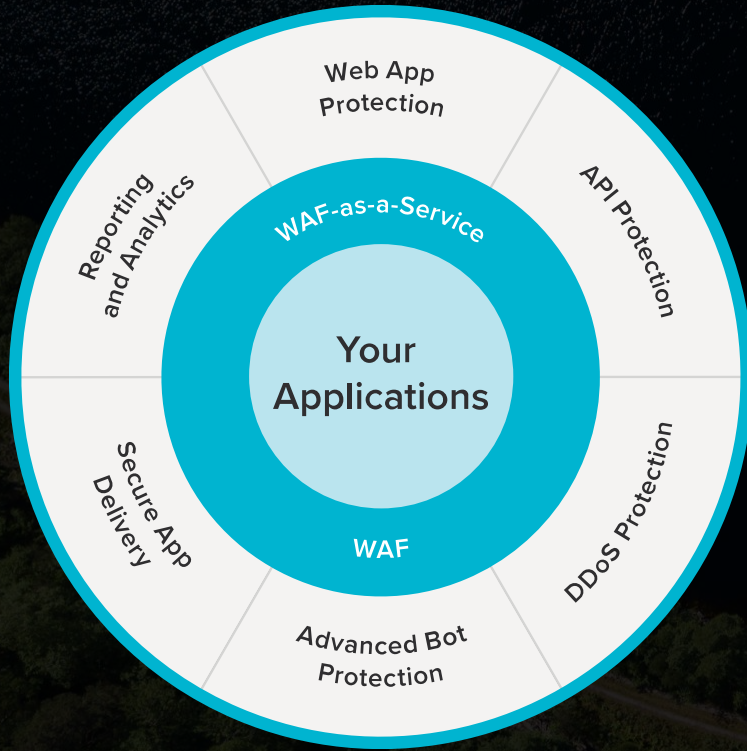
200M

App and Bot
attacks
blocked (per day)

An aerial photograph of a river flowing through a lush green forest. The river is dark and occupies the upper half of the frame. The forest is dense and green, covering the lower half. A dirt road or path runs along the edge of the forest, separating it from the river. The text "Barracuda Application Protection" is overlaid in white, serif font across the middle of the image.

Barracuda Application Protection

Introducing Barracuda Application Protection



Protect all your apps and APIs with Barracuda Application Protection

- Comprehensive protection for web apps and APIs
- Easy to operationalise and manage
- Protect your apps everywhere
- Scale to secure any size of application

An aerial photograph of a winding coastal road. The road is light-colored and curves from the bottom left towards the top right. A small red car is visible on the road, moving away from the viewer. To the left of the road is a rocky coastline with waves crashing against the shore. To the right of the road is a dense green forest. The overall scene is serene and scenic.

API Protection with Barracuda Application Protection

Stop API attacks and prevent data breaches

Discover and secure your XML, JSON and GraphQL APIs

- Machine-Learning powered continuous API discovery to secure growing applications
- Stop bot and DDoS attacks, and improve API performance
- Secure API delivery for your critical applications
- Shift left without slowing down
- Zero Trust for your APIs
- Gain full visibility into your applications and traffic.

Next Steps

Review our additional resources

- The New ABCs of Application Security – [Direct Link](#) (PDF)
- Threat Spotlights on our blog covering these vulns. & more - [Link](#)

Follow our blog to receive more insights, including Threat Spotlights - [Link](#)



Thank You

