White Paper

Enhancing Security and Scalability for APIs in Open Banking

Table of Contents

Introduction

Open banking opens customer data to external third-party providers (TPP) via application programming interfaces (APIs) that are designed to spur innovation and increase competition. In most modern applications, composed of functions and services, developers rely on APIs to communicate between applications and their components, to share data and to drive functionality. These applications are mobile and distributed, and they have instances in the cloud and on-premise. Gaining a consolidated view of their configuration and security parameters is challenging at best. Many of these applications change frequently and may include open-source modules. In many cases, security becomes an afterthought.

According to Radware, in 89% of organizations, the information security team does not own the budget for security solutions. In this white paper, we examine the implications of open-banking APIs on application security and identify best-practice recommendations for securing these APIs in both cloud and on-premise deployments.

Open banking, driven largely by regulation, opens closed and proprietary deposit-taking banking customer data to external third-party providers (TPPs) securely through publicly available APIs.

In traditional banking, all customer data is controlled by the parent bank. In open banking, the customers own their data, which is securely exposed to TPPs via APIs if consent is provided by the customer. The TPPs use these publicly exposed APIs to provide financial technology (fintech) services traditionally not available through the customer's own bank.

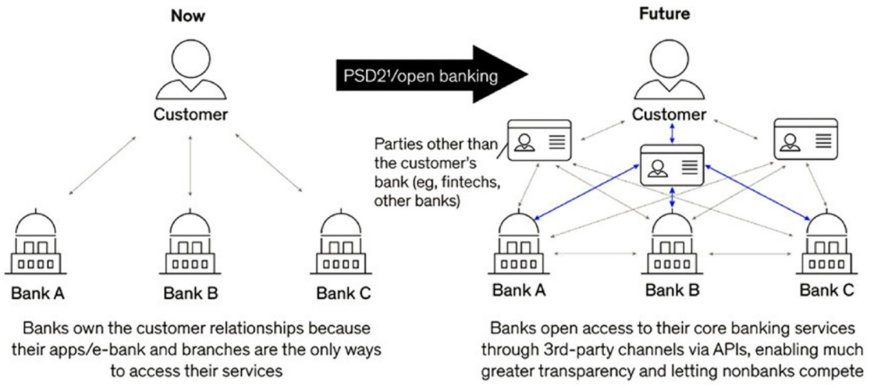
What Is Open Banking?

Prior to open banking, many innovative fintech providers used screen scraping to gain access to customer data, including user credentials, without knowledge of the parent bank. Open-banking APIs move to streamline the legal implications of sharing customer credentials and information through APIs, consent, and regulatory authority.

Open banking allows for the secure transmission of account data authorized by the customer to a TPP. Technically, this access is provided as a collection of REST APIs. Access to these APIs is available in the public domain for subscription through a certifying authority.

Figure: 1

The EU's second Payment Services Directive.


Now
Customer
Bank A
Bank B
Bank C
Banks own the customer relationships because their apps/e-bank and branches are the only ways to access their services
PSD2¹/open banking
Future
Customer
Parties other than the customer's bank (eg, fintechs, other banks)
Bank A
Bank B
Bank C
Banks open access to their core banking services through 3rd-party channels via APIs, enabling much greater transparency and letting nonbanks compete

[1] The EU's second Payment Services Directive.
Source: McKinsey analysis; UK Open Banking Implementation Entity

According to a 2018 Celent study, the number of U.S. financial institutions that have open-banking portals to facilitate TPP access to consumer financial and other data is expected to grow from 20 to more than 200 by the end of 2021. As of the first quarter of 2020, there were more than 300 TPPs registered under Payment Services Directive 2 (PSD2) in the U.K. Other countries, such as India and Australia, have followed the EU's approach and have a thriving openbanking ecosystem.

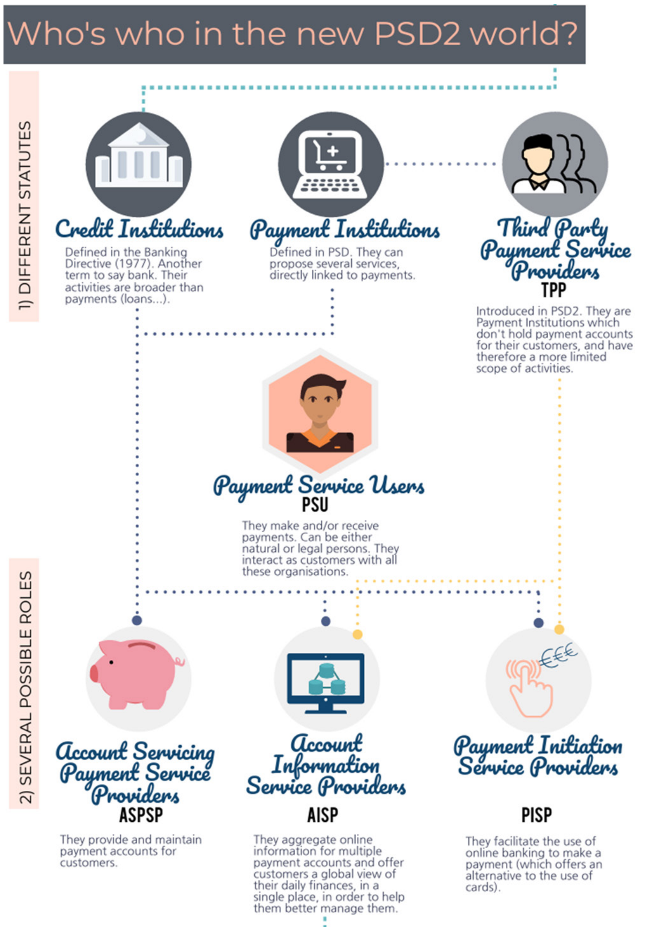
Who Are the Participants in Open Banking?

Regulatory Authority

This includes policymakers that regulate banking and promote competition, data sharing and security. For example, in Europe the Financial Conduct Authority (FCA) maintains a register of companies authorized for open banking and issues eIDAS certificates under its Strong Customer Authentication Regulatory Technical Standards (SCA-RTS). These TPPs must adhere to the General Data Protection Regulation (GDPR) as well.

Figure: 2

Who's who in the new PSD2 world?



Defined in the Banking Directive (1977). Another term to say bank. Their activities are broader than payments (loans...).

Defined in PSD. They can propose several services, directly linked to payments.

Introduced in PSD2. They are Payment Institutions which don't hold payment accounts for their customers, and have therefore a more limited scope of activities.

They make and/or receive payments. Can be either natural or legal persons. They interact as customers with all these organisations.

2) SEVERAL POSSIBLE ROLES
€€€
Account Servicing Payment Service Providers
ASPSP

They provide and maintain payment accounts for customers.

They aggregate online information for multiple payment accounts and offer customers a global view of their daily finances, in a single place, in order to help them better manage them.

They facilitate the use of online banking to make a payment (which offers an alternative to the use of cards).

Payment Service User

This describes a consumer initiatinga transaction. **Account Information Service Providers (AISPs)**. These are registered account aggregators that are authorized by the customer to use (but not modify) their bank account data.

Payment Initiation Service Providers (PISPs)

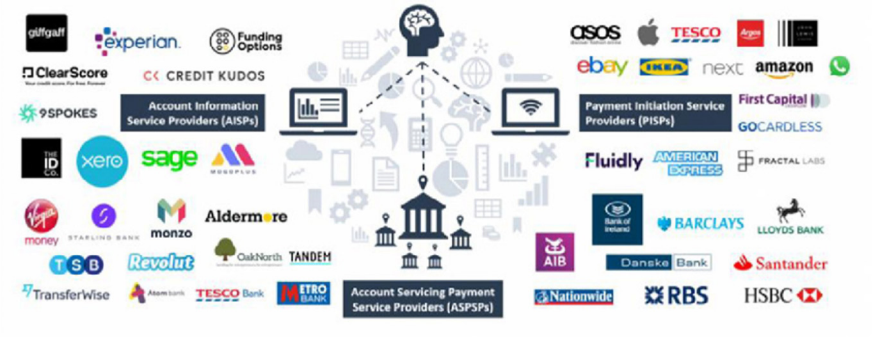
These are registered providers that are allowed by the consumer to initiate payments directly from a customer bank account.

Account Servicing Payment Service Providers (ASPSPs)

These are banks that are responsible for making APIs available to TPPs, allowing them to initiate payments or gain access to customer bank-transaction information.

Figure: 3

The Open Banking Ecosystem.



Financial institutions collaborate with TPPs and use APIs to enable new services and connect financial institutions' applications to merchants, consumers and companies. Data aggregators collect data and feed it into TPP apps such as Venmo, Betterment and Chime. For example, Plaid delivers an API platform for TPPs to connect to financial institutions for account access and authentication, while Finicity provides access to financial data in real time. UK, one of the leaders in open banking, currently lists 300+ regulated providers, 230+ TPPs and 80+ account providers, including Plum, Moneybox, Currensea and many others.

What's Driving Open Banking?

Open banking is a trend driven by regulation, the pace of innovation in financial technology and consumer demand for more control over how their data is used. Open-banking regulations are disrupting the conventional way of doing business for traditional financial institutions by forcing them to open access to their customer data to third parties via APIs. Open banking is one of the biggest threats traditional banks face, but interestingly, it is also one of their biggest opportunities. Many nimble and innovative fintech companies with access to customer data are enabling new and innovative products to offer more choice to the consumer.

Regulatory

In 2015, the European Union mandated open-banking APIs under its PSD2 and GDPR to govern data protection and privacy for all EU residents. PSD2 requires financial institutions to provide third-party providers with access to customer data via open APIs. It also mandates that financial institutions and their TPPs implement related data security controls.

Innovative and Competitive

The pace of innovation and ease of use for the consumer are big drivers of open banking. Companies such as Venmo, Currensea, Plum, Betterment and Rocket Mortgage offer customers easy ways to make payments, spend, invest and understand their finances and get approved for a loan. Marketable

Europe (and the UK in particular) is an early indication of the open-banking revolution. There, TPPs have grown from approximately 100 to more than 450 in under two years, and their focus has expanded from payments and transactional retail banking to encompass the entire financial value chain.

According to Accenture, built on data sets covering 20 of the largest economies responsible for over 75% of global GDP, as much as US$416 billion in revenue will be at stake as the open-banking data wave arrives.

Technological

While interfaces are nothing new, more modern formats such as JSON and RESTful APIs are lighter, more flexible and require less bandwidth – making them ideal for a mobile-first world. Traditional banks are also modernizing and rearchitecting their applications to compete against neobanks and fintechs.

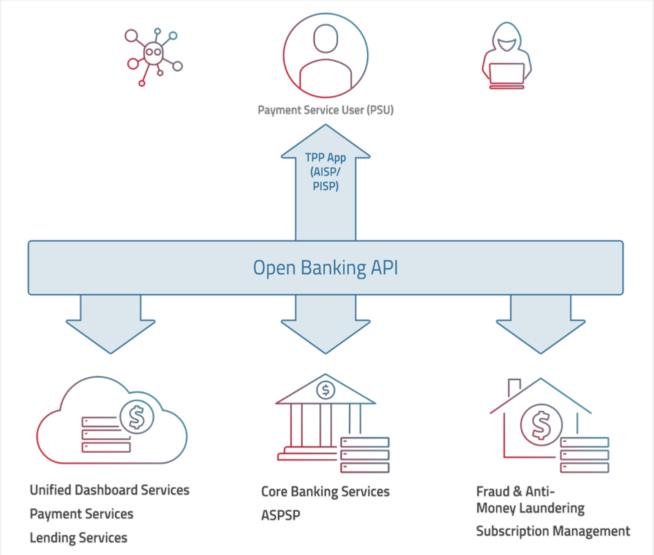
Dynamic

COVID-19 has affected nearly every business, some rather dramatically. Many sectors, including finance and banking, are still adjusting operations. The pandemic has accelerated remote workforces and driven the demand for a contactless economy. This is driving network and application rearchitecture as well as adoption of and transition to the cloud while increasing the use of open APIs for many services, including open-banking APIs for financial services.

Building Blocks of Open Banking

Figure: 4

Open Banking API.



In open banking, to use an API for sharing customer data, financial institutions must obtain the customer's consent for data sharing and allow the customer to select the data they want to share. Consent and data selection occur through an API, using the OAuth 2.0 protocol.

What's an API?

An API is a software interface that allows the creation of applications that connect and communicate with each other.

The developer defines the APIs, which are then implemented in software on the web or on an application server. Then, these APIs are exposed to the external world, which allows TPP applications and end users to communicate with it. One of the purposes of APIs is to decouple and hide internal details and implementation from an external consumer so that it may change at a later date without affecting the consumer.

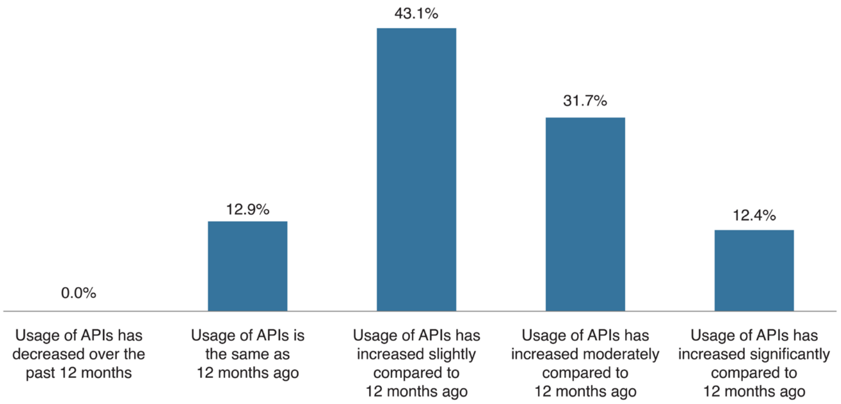
Security Implications of Open Banking

Easy-to-build and easy-to-consume APIs accelerate application development while enabling sharing of sensitive data between systems. According to a survey by Radware, more than half of applications in nearly two out of five organizations are exposed to the internet or third-party services via APIs. Organizations see API security as an area of growing concern. Fifty-five percent call it a "top priority," while 59% say they want to "invest heavily" in it during 2021.

A new Radware survey, Application Security In A Multi-Cloud World 2023, found that 87.2% of organizations are increasingly developing and using APIs as an essential element of their modern application strategy. 42% of organizations expect APIs to be inextricably linked to business success in a year—up from just 2% a year ago.

Figure: 5

Source: Osterman Research (2023).



In this survey, 74.3% of organizations said that they are not confident that their APIs can withstand security threats

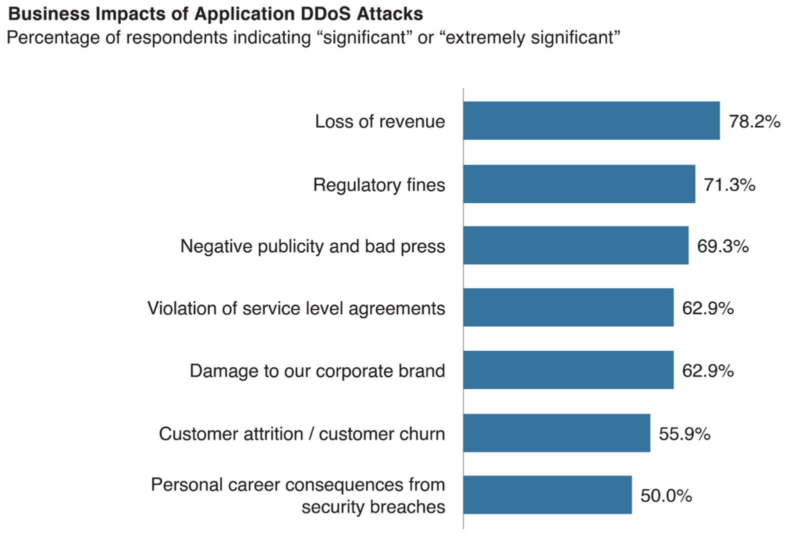
Open-banking APIs are also used for mobile banking and fintech applications. A large proportion of organizations do not maintain the same security practices for mobile applications as they do for web applications. Only 36% of mobile apps have integrated security fully into their mobile application development lifecycle, and a large proportion either have no security (22%) or only "bolted-on" security (42%).

While APIs bring tremendous benefits, they also introduce availability and security concerns.

Service disruption: Dependence on third-party APIs and components may lead to unintended service disruptions if API services are unavailable due to security, network and application configuration errors, API denial-of-service (DoS) attacks or application or authentication infrastructure outages.

Figure: 6

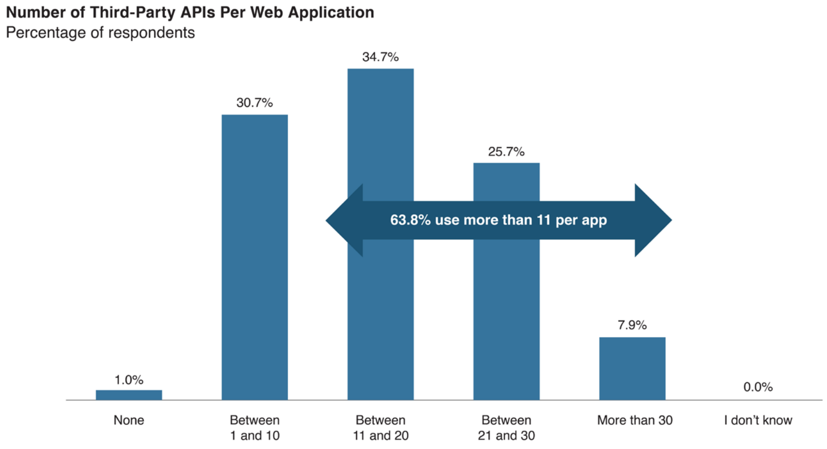
Source: Osterman Research (2023).



The survey, Application Security In A Multi-Cloud World 2023, found that organizations use an average of 15.9 third-party APIs in each of their web applications. 99% of organizations make extensive use of third-party APIs, with 68.3% of organizations using more than 11 third-party APIs for each of their web applications. On average, organizations use 15.9 third-party APIs that are executed directly in the user's browser in each of their web applications.

Figure: 7

Source: Osterman Research (2023).

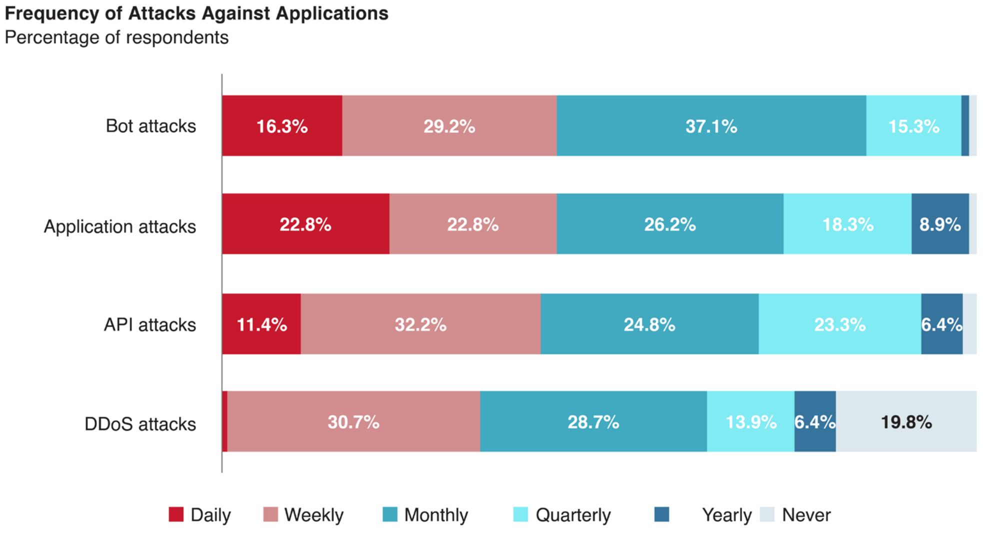


Trust issues: Many solutions for open banking are built on cloud-only or hybrid infrastructure. However, according to a Radware survey, migration to public clouds creates trust issues. Only 27% "completely trust" the security offered by their cloud provider(s). Of those that have already migrated to the public cloud, 47% are using more than one infrastructure provider for hosting their production apps. Trust issues include incompatibility of security solutions, configuration challenges across different environments, misconfigurations and issues around application security policies and profiles.

Increased Attack Surface: API attacks of various types are fairly common. Figure 5 lists the top attacks against applications reported by respondents.

Figure: 8

Source: Osterman Research (2023).



Data Theft: Many APIs process sensitive personally identifiable information (PII). The combination of sensitive and confidential information, coupled with a lack of visibility into how these APIs and third-party applications operate, is a security nightmare in case of a breach.

Undocumented but published APIs: Undocumented APIs may accidently expose sensitive information if not tested and may be open to API manipulations and vulnerability exploits.

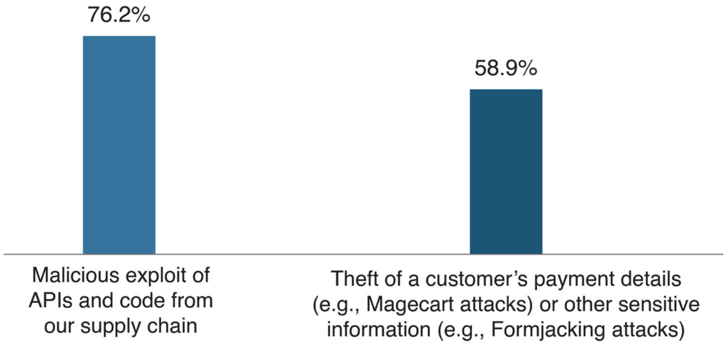
Client-Side Threats: When building applications, organizations complement their internally developed APIs with APIs to third-party web applications. These third-party APIs are executed directly in the user's browser (hence also known as client-side APIs). 99% of organizations make extensive use of third-party APIs, with 68.3% of organizations using more than 11 third-party APIs for each of their web applications. On average, organizations use 15.9 third-party APIs that are executed directly in the user's browser in each of their web applications. In our survey, Application Security In A Multi-Cloud World 2023, 76.2% of organizations expressed concerns about software supply chain threats.

Figure: 9

Source: Oterman Research (2023).

Concerns About Various Types of Malicious Exploits

Percentage of respondents indicating "concerned" or "extremely concerned"



Because threats vary, API security requires a combination of security controls to enforce:

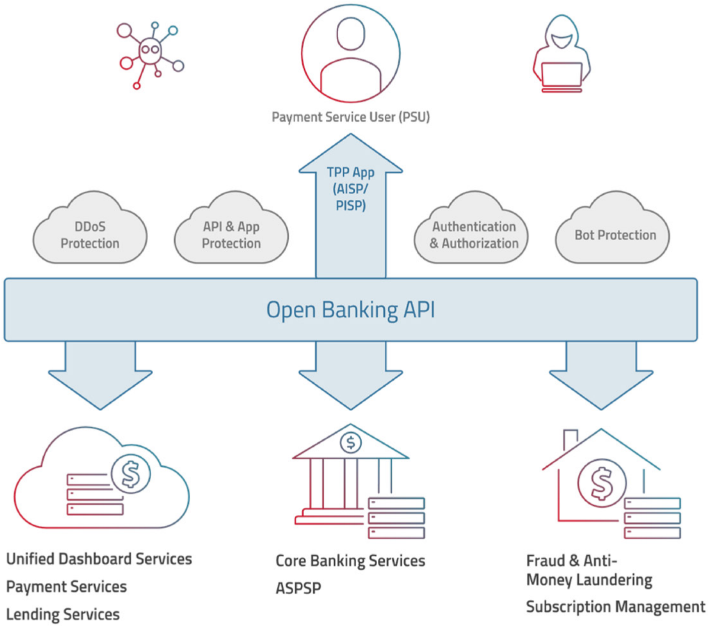
- API access controls for authentication, authorization and access management.
- Protection against excessive permissions, entitlements and malicious activity.
- Prevention of bot attacks on APIs.
- Detection and prevention of API manipulations.
- Protection from distributed denial-of-service (DDoS) and availability attacks.
- Protection from embedded attacks.
- Protection from API vulnerabilities.
- Prevention of PII data leakage and excessive data exposure.
- Protection from fraud and phishing scams.
- Client-side protections from compromised embedded third-party APIs.

Designing a Secure Open-Banking API Environment

Gartner predicted that by 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications. The API security challenge requires threat coverage, easy integration and complete visibility for both documented and undocumented APIs. In a new research, according to Gartner, more than 30% of the increase in demand for application programming interfaces (APIs) will come from AI and tools using large language models (LLMs) by 2026.

Figure: 10

Must-Have Requirements for Protecting Open-Banking APIs.



Traditionally, DDoS protection, web application firewalls (WAFs) and API gateways have been the primary inline security tools used for API protection.

However, APIs are also exposed to bot attacks. According to Forrester, more than a quarter of all web requests originate from bad bots. These bots were observed attempting automated attacks – such as account takeover, denial of service, payment data abuse and denial of inventory – targeting APIs. Protecting APIs against automated attacks is different than protecting web and mobile applications simply because the bot behaviors, navigation flow and indicators are different.

The lack of dedicated bot management tools in most organizations puts these organizations at greater risk for potential bad actors launching successful attacks – such as credential stuffing, Brute Force and scraping attempts – through APIs.

While API gateways offer API management and integration with authentication and authorization features, their API security, bot protection and web application protection capabilities are either limited or absent. On the other hand, most WAFs do not understand the differences between APIs and regular web applications. Even if they do, they do not inspect or detect the real security risks related to APIs.

Security measures must be applied to enforce security policy on documented and undocumented APIs.

To secure APIs, a web application and API protection (WAAP) security solution must discover the undocumented APIs, enumerate API endpoints for both documented and undocumented APIs to be secured, and then enforce the appropriate security measures, blocking API calls that attempt any of the following violation indicators:

- Accessing restricted or unauthenticated APIs.
- Business logic attacks.
- Client-side attacks using compromised third-party API calls.
- Using undefined or disallowed HTTP methods for an API endpoint.
- Containing unrecognized and nonvalid parameters.
- Containing out-of-expected-range parameter values.
- Embedding web attacks in JSON payloads or parameters.
- Excessively utilizing the APIs.
- Extracting sensitive data through the API including using AI-agents and AI-assisted attack tools.
- Attempting to take advantage of API vulnerabilities.
- Attempting to break the API authentication process through an account takeover attack.

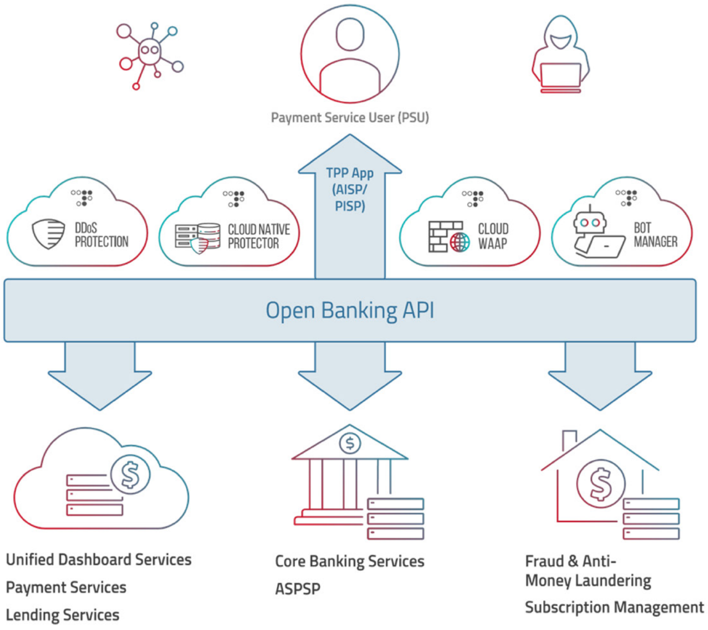
Securing Open-Banking APIs with Radware

Radware's application protection solution is designed to secure APIs from hackers and nation-state attacks. The solution protects application APIs from DDoS, application and bot attacks; protects APIs against vulnerabilities, manipulations, excessive permissions, entitlements and malicious user activity; and prevents service disruptions while addressing trust and security concerns of customers migrating to a multi-cloud or hybrid deployment.

In the multi-layered defense, you have different **enforcement points**. We integrate with these enforcement points to apply security policies, signatures, and rules in a uniform manner regardless of where the application resides.

Figure: 11

Radware Solution Components for Protecting Open-Banking APIs.



By combining positive and negative security models, Radware, a leader in API security, secures APIs from known and zero-day attacks as part of its flexible and scalable web application security solution and is recommended by NSS Labs and ICSA Labs across on-premise, cloud, virtual, stand-alone or integrated, and inline and out-of-path deployments.

DDoS Protection

APIs may be attacked using a flood of requests to slow or disrupt service or to gain access to databases. Many attacks, frequently using SSL, focus on rendering the web application layer unreachable, causing a denial-of-service state. A maliciously designed HTTP request can lead the web or application server to execute many internal requests that can consume all its resources.

Radware's DefensePro or Cloud DDoS Protection Service

These guard from evolving cyber threats with comprehensive, automated DDoS protection that continuously adapts to offer the fastest threat detection and mitigation.

Cloud Security Posture Management (CSPM) & Cloud Infrastructure Entitlement Management (CIEM):

Migrating application workloads to the public cloud creates new threat surfaces that can be exploited by attackers and lead to theft of customer data. Radware's Cloud Native Protector (CNP) secures the cloud environment against identity and access abuse, protects against malicious user behavior and secures the overall security posture of the public cloud environment.

Reverse Proxy or Application Delivery Controller (ADC)

In an API-driven world, ensuring application service-level agreements is critical for ensuring the digital experience. ADCs are the foundation for keeping applications and their environments secure, scalable and available. Radware's Alteon Multi-Cloud Solution allows organizations to decouple user connections from applications to individually scale them while reducing both access latency and operational cost for scaling applications.

WAAP

Radware provides an API and application protection solution suite for every environment, with automated security policy generation. Radware's WAAP solution is available integrated with Radware's Alteon (integrated WAF) as a managed cloud service (CWAF) or as a solution in Kubernetes environments (KWAF) to easily integrate with common software provisioning, testing and visibility tools in the continuous integration and continuous delivery (CI/CD) pipeline.

Radware Bot Manager

Radware Bot Manager defends APIs against automated attacks and ensures that only legitimate users and devices can access the APIs while blocking any attempt to reverse engineer mobile SDKs. It uses intent-based deep behavior analysis behind an API request to block malicious activity.

Compliance

Radware's solution ensures PCI DSS 4.0, DORA, NIS2, and GLBA compliance by addressing the requirement to detect and protect against API, application, and network threats. Our AI-driven engine continuously auto-discovers APIs and learns their business logic in real-time, providing immediate detection and mitigation of malicious API calls.

Deployment Topology in the Public Cloud (AWS)

The figure below shows Radware's solution recommendation for open-banking reference architecture on Amazon Web Services (AWS).

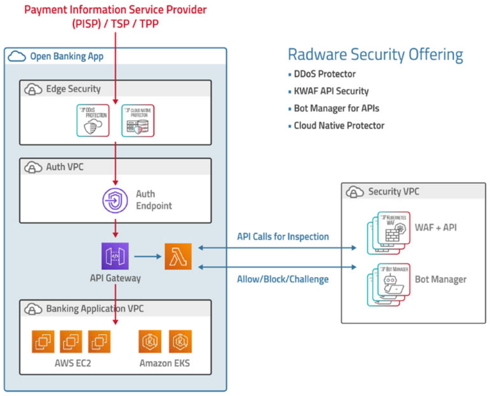


Figure: 12

Radware Solution Components in a Public Cloud Deployment.

When customers deploy their applications and APIs purely on a public cloud such as AWS:

- Radware Cloud DDoS Protection Service or Radware DefensePro running as a virtual machine in a virtual private cloud provides edge security for applications and APIs against denial of service.
- Radware's Cloud Native Protector, available as a cloud-native solution, provides multilayered protection for cloud-native application infrastructure and workloads against identity and access abuse and malicious user behavior.
- Radware's WAAP – available as a cloud service, as a virtual machine integrated with Radware's Alteon, or as a solution for Kubernetes – provides:
  - A strong positive security model with API security for documented and undocumented APIs.
  - Integrated bot mitigation for comprehensive protection of APIs from bots through intent analysis, fingerprinting and so on to protect against all forms of account takeover.
  - Protection from API manipulations, embedded attacks and API vulnerabilities and prevention of sensitive data leakage.
  - Best-of-breed protection for API access controls and management through integration with leading API gateways.
- For reverse proxy, customers have the option to use native load balancers in the cloud, deploy Radware's Alteon through the marketplace or utilize Radware's unique and cost-effective bring-your-own-license model called Alteon Global Elastic License (Alteon GEL).
- Radware Bot Manager is available as a cloud software-as-a-service (SaaS) application.

Deployment for Hybrid Topology

Many customers are in the process of either transitioning to the cloud or maintaining a hybrid topology spanning a mix of private, public and on-premise infrastructure.

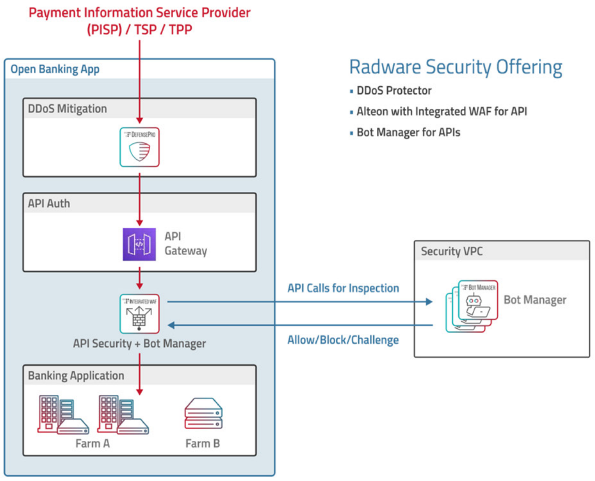


Figure: 13

Radware Solution Components in a Hybrid Deployment.

When customers deploy their applications and APIs in a hybrid topology:

- Radware DefensePro, available as an appliance or a virtual machine, provides edge security for applications and APIs against denial of service. Customers also have the option to use Radware Cloud DDoS Protection Service.
- For reverse proxy, customers can utilize Radware's Alteon as an appliance or virtual machine available as a perpetual or subscription license. The license allows customers to transition their applications to a public or private cloud in the future.
- Radware's WAAP, available as a virtual machine integrated with Radware's Alteon and as a solution for Kubernetes, provides:
  - A strong positive security model with API security for documented and undocumented APIs.
  - Integrated bot mitigation for comprehensive protection of APIs from bots through intent analysis, fingerprinting and so on to protect against all forms of account takeover.
  - Protection from API manipulations, embedded attacks and API vulnerabilities and prevention of sensitive data leakage.
  - The Integrated ERT Active Attackers Feed for protection against DDoS attacks, scanners, anonymous proxies, IoT botnets, and web application attacks by identifying and blocking, in real time, known IP addresses with bad reputations that were recently involved in attacks.
  - Best-of-breed protection for API access controls and management through integration with leading API gateways.
- Radware Bot Manager is available as a cloud SaaS application and is integrated with Radware's Alteon using Radware's WAAP.

The Radware Advantage

Radware's solution portfolio for open banking provides full support for the OWASP Top 10, bot management, comprehensive API security, DDoS protection, solution scalability and availability and threat intelligence.

Radware's WAAP provides unique advantages that include the following.

Continuously Adaptive Security

Continuously detect changes in the application and acceptable user behavior to keep application and API protection current:

- AI-assisted and machine learning algorithms to automatically generate policies.
- API mapping to detect new and/or changes to existing web applications.
- Accurate protection lowering false positives.
- Automatic threat analysis covering the OWASP Top 10 and more than 150 attack vectors.
- Automatic policy activation for adding tailored app rules and optimizing for best accuracy.
- Policy generation with automatic optimization for out-of-the-box rules to minimize false positives.

Multi-Layered Detection and Mitigation of Business Logic Attacks

Continuous Real-Time Learning of the APIs' Business Logic: Learns directly from real-time transactions, unlike others that rely on historical logs, allowing for immediate and accurate detection of malicious API calls.

- Immediate Mitigation: Automatically generates and applies security policies in real time to block business logic attacks as they occur.
- Accurate Bad Actor Identification: Goes beyond simple IP blocking to surgically identify and block the specific malicious user or client responsible for the attack. This prevents false blocking of legitimate users sharing the same IP.
- Unmatched detection and mitigation accuracy: Uses real-time AI-driven context analysis of security policies to ensure only the most reliable policies are applied and significantly enhances the protection accuracy.

Real-time Automated Protection for Any Type of API Attack

Broad support for API security includes:

- TCP termination.
- Parsing, decoding and normalizing traffic.
- JSON and XML parsing, validity check and key-value extraction.
- Embedded attack detection in JSON and XML parameters.
- Schema enforcement and access control lists for API endpoints according to the OpenAPI Specification (formerly the Swagger Specification), including endpoints, methods, structures and more.
- Behavioral protections via invocation context and API flow of API calls to prevent API abuse.
- Leakage prevention for sensitive data parameters and PII in API responses.
- API vulnerabilities involving data manipulation such as XML External Entity (XXE).
- Protection against bot account-takeover attacks on API authentication.
- Quota management policy to validate that APIs are not abused.
- Geolocation policy enforcement on APIs.
- Protection against availability attacks.

Flexible Deployment for Any Architecture and Platform

- **Advanced automation:** Integrates into CI/CD pipeline to facilitate security provisioning of new services and applications, with a local management and reporting interface.
- **Scalability and elasticity:** Grows and scales application security along with Kubernetes pods, including learned policies and configuration settings, assuring high availability.
- **Visibility:** DevSecOps and security visibility through integration with common tools and platforms.
- **Extensive application security:** Only vendor to combine positive and negative application and API security models for all deployments, including Kubernetes.
- **DevOps friendly:** Only vendor to provide NSS Labs–recommended and ICSA Labs–certified application and API protection technology, with full automation and actionable analytics for microservices running within a Kubernetes environment.
- **Cross-platform support:** Grows and scales application security for all environments, from Kubernetes to managed deployments for on-premise and cloud environments.

Conclusion

Although open banking is still in its infancy, it is growing rapidly. Open banking opens customer data to external third-party providers via APIs to deliver innovative services. However, this also means a broader threat surface that needs to be protected against abuse and malice. Banks and fintech that thrive in this environment will deliver solutions that encourage customer trust through secure solutions.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.