





Cloud-Native Security

Legacy security tools lack the visibility and control needed to protect modern infrastructure. Improve insights into cloud-native technology to protect your business with expanded cloud operations.

[Get more info >](#)

Proven Leadership
We're a leader in the industry. We've been recognized by Gartner for 14 years.

85% data repository coverage
We protect 85% of your data repository with our cloud-native technology.

Customer testimonials
"We've seen a significant increase in our security posture since we implemented this solution." - John Smith, CISO

New infrastructure attack opportunities

The massive diversity of technology options for digital infrastructure has brought more security challenges across an expanding attack surface. Infrastructure has changed from servers remaining online for hours to containers redeployed every second.

- **Understanding risk, changes with cloud**
Infrastructure has changed from servers remaining online for hours to containers redeployed every second.
- **Security is less connected to developers**
Many configurations are managed by developers who bypass IT operations and security processes.
- **Legacy security doesn't help here**
In the DevOps model, traditional security tools don't pick up from the decommission of the operating system.
- **Pervasive characteristics of APIs**
Not only are APIs growing in volume, but also ever-changing nature.

Protection for modern infrastructure

Improve defense security within DevOps tooling to protect modern cloud-native functions and Database-as-a-Service (DBaaS).

- **Built into modern technology**
Improve your protection by deploying into existing workflow and technology stack.
- **Advanced visibility for DevOps cultures**
Risks are automatically discovered and identified for developers to remediate.
- **Protection against innovative attacks**
Stop attacks that evade detection and identified for developers to remediate authorization (SOA).
- **Comprehensive security at DevOps speed**
Streamlined protection with continuous data availability and automated API classification based on compliance.



imperva

Protecting your data
and all paths to it

There are more opportunities to **steal data** today than ever before



Organizations are transforming and moving workloads to the cloud



APIs and applications are the primary vector for accessing data



20% of internet traffic is from bots pretending to be humans



Regulatory risk requirements for protecting data are burdensome

imperva

A **modern** approach



Run Anywhere

Protect critical workloads and sensitive data on-prem and in the cloud



DevOps Ready

Pre-built libraries and integrations to provision and scale visibility and security



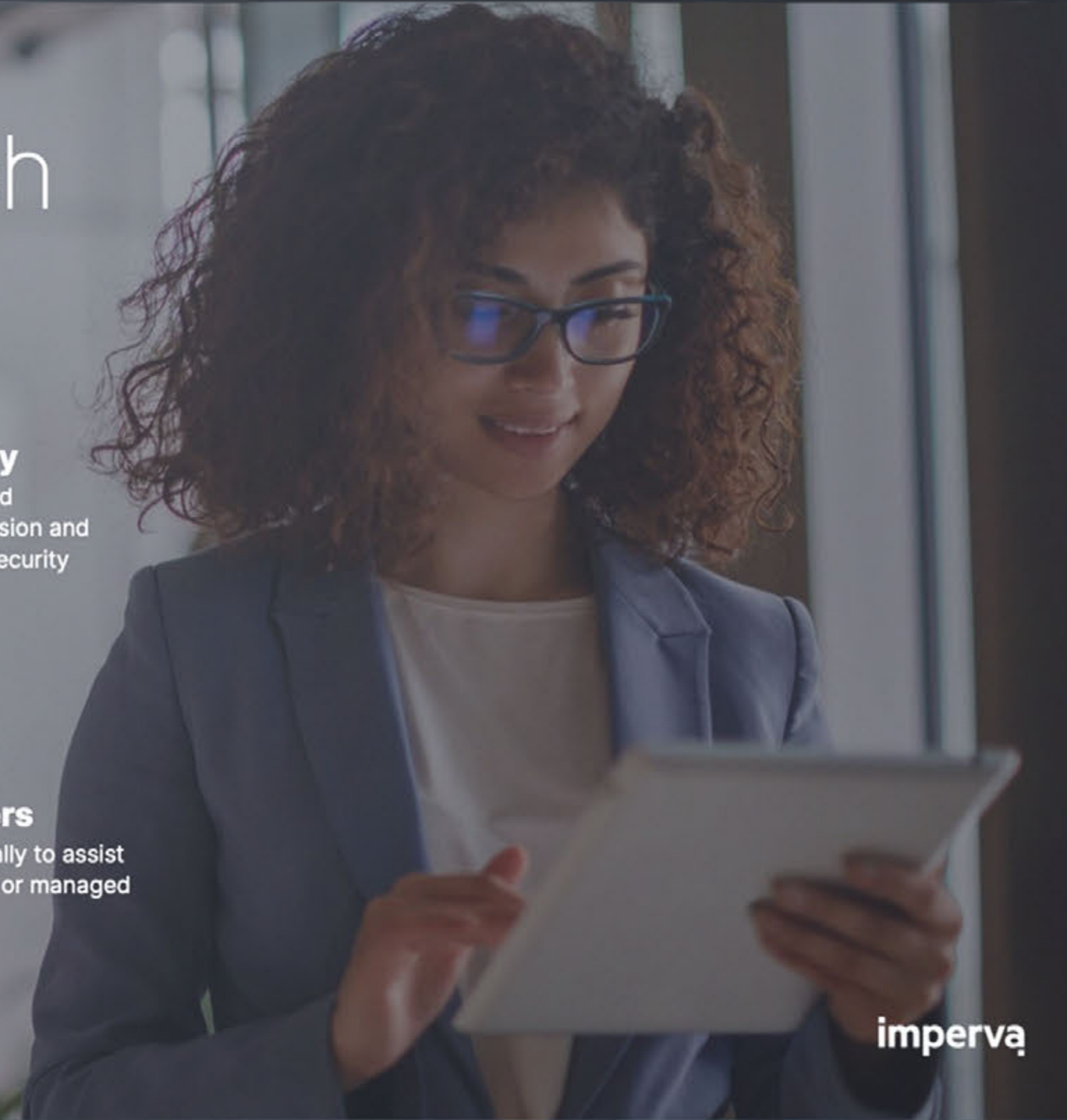
Ecosystem

Out of the box integrations with SIEMs, response automation tools, etc.



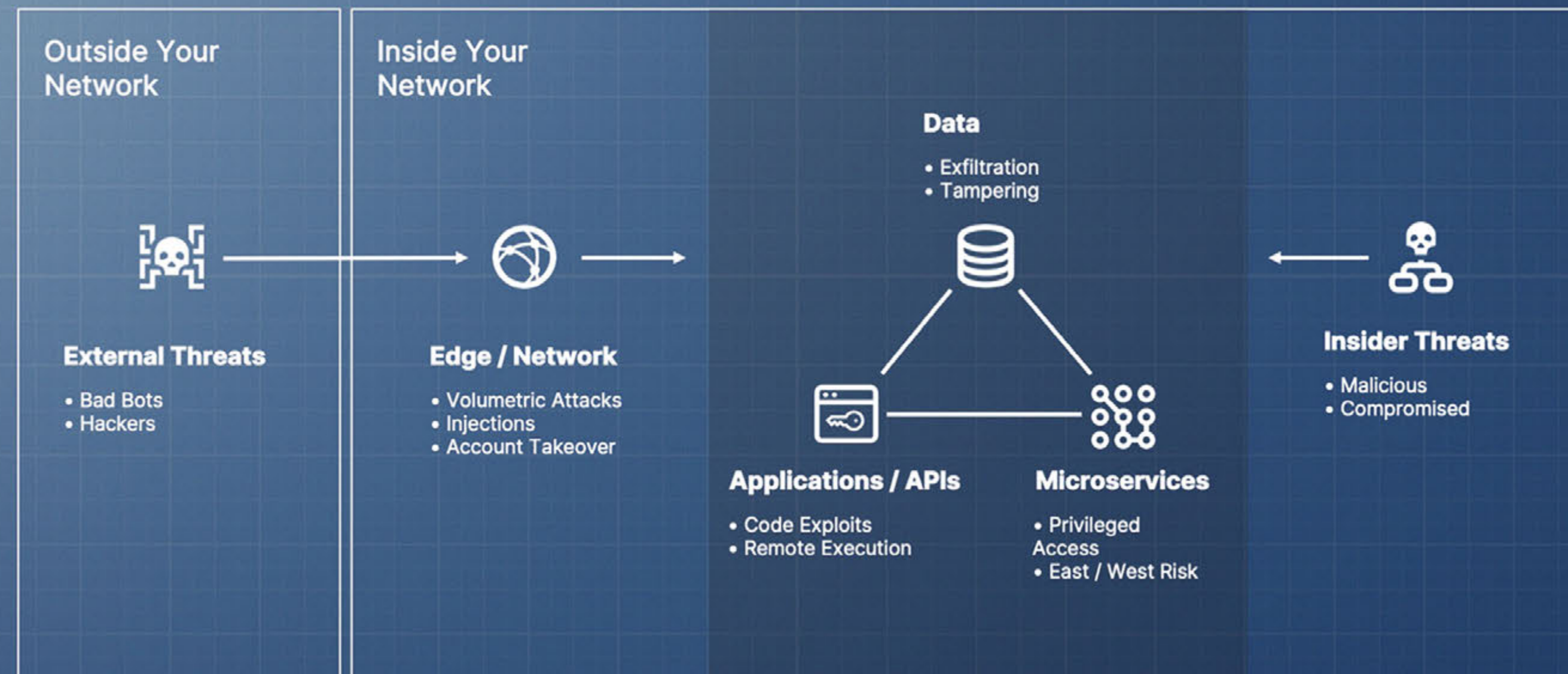
Global Partners


500+ partners globally to assist with getting started or managed



imperva

Today's Threat Model





We now spend less time on issues
such as software changes and
can direct more energy on
protecting our **members' data**
and **company information**

Sharon Black
Sr. Manager of Information Security
BlueCross BlueShield of Tennessee

imperva

imperva

DATA SHEET

ImpervaONE

What is ImpervaONE?

ImpervaONE is the environment and insights from a combination of Imperva Cloud Web Application Firewall (WAF), Runtime Application Self Protection (RASP), and Database Activity Monitoring (DAM) and Discovery and Assessment (DAS) security and assessment offerings. This integration and combination of products provides the ability to track users' activity and interactions with sensitive data from the edge, through applications and APIs to back-end databases. Additionally, these enriched audit events are connected to the results of DAS scans identifying if the data is sensitive, determine who has access to it, and if the database is vulnerable. ImpervaONE supports both legacy and modern application stacks, and can work in any customer managed environment including on-premises and in the cloud.

What challenges does ImpervaONE solve?

There is currently a blind-spot when monitoring access to sensitive data in database traffic as it pertains to security applications. When a user logs into the front-end of an application or an API, the database audit only sees the account in the connection. Today, there is no simple method to derive who is accessing sensitive data (by role, etc), or where users came from (app or browser, internal or external, job or not, geo, etc). ImpervaONE solves this by scanning requests from the various disparate tiers in a distributed environment, and correlating the logs to reconstruct a single, comprehensive, and operational view of the sensitive data access.



ImpervaONE - Data Sheet

Source IP	Destination IP	Operation	Account	Database
85.79.104.78	172.28.42.17	SELECT	ADMIN	PROD
85.79.104.78	172.28.42.17	SELECT	ADMIN	PROD
85.79.104.78	172.28.42.17	SELECT	ADMIN	PROD
172.28.4.159	172.28.42.17	SELECT	ADMIN	PROD
172.28.4.159	172.28.42.17	SELECT	ADMIN	PROD
172.28.4.159	172.28.42.17	SELECT	ADMIN	PROD

imperva.com

imperva
DATA SHEET

Runtime Application Self-Protection (RASP)

Securing applications by default

Applications are prime targets for cyber attacks as they handle flows of personally identifiable information, intellectual property, financial information, and other critical data. Many traditional application security tools fail to protect organizations from attacks because they mostly rely on signatures and rules that are heavy to maintain, cause performance degradation, suffer from high false positive rates, struggle to stop zero-day attacks, and lack the real-time context and visibility Imperva believes that securing applications requires radical thinking: applications must defend themselves.

Imperva RASP

Imperva RASP fits the security gaps that leave applications vulnerable to attack with a single plugin that protects both legacy and modern applications. The RASP plugin is compatible with on-premise, in the cloud, and in containers. Imperva RASP secures applications by protecting themselves using an industry-leading, lightning fast attack detection architecture in Language ThreatSec Security (LATH2SEC). LATH2SEC understands how payloads will execute within the context of a given environment and recognizes known and zero-day attacks. The result is applications that avoid otherwise inevitable attacks.

RASP integrates security into application development lifecycle, augmenting the traditional vulnerability management approach to AppSec. Because RASP not only reports the vulnerabilities, it neutralizes attack even before exploits - down to the exact line of code - but also secures applications despite those vulnerabilities, organizations can patch vulnerabilities on their own schedule, minimizing disruption.



Runtime Application Self-Protection - Data Sheet

KEY CAPABILITIES

- Secures applications no matter where or how they are deployed, on-prem, in the cloud or via containers
- Fast time to value with no build, no change, with no network mode
- Simple deployment via existing signatories, with no network calls
- Secures latent vulnerabilities in original or third-party software
- Zero-day protection

Imperva RASP at a glance

Benefits of Imperva Runtime Application Self-Protection

RASP-protected applications in production are secure by default, no matter where or how they are deployed. RASP requires no signatures, updates or learning mode, no external network calls, and negligible CPU and memory consumption while an application under attack by leveraging patented LATH2SEC techniques, leading to fast time to value and low total cost of ownership (TCO). RASP buys you time to fix and patch vulnerabilities because your applications are secure regardless of latent vulnerabilities in original or third-party software.

A new context-enriched perspective of security from the inside of your apps with unprecedented visibility into application attacks, events & flows.

Deployments that scale with DevOps

RASP deploys natively and safely via automated plugins that live inside applications, no matter where or how they are deployed. Because RASP leverages LATH2SEC - which combines high detection accuracy with very low performance overhead - deployment is unobtrusive, allowing critical business functions to continue as usual, without disrupting user experience.

Imperva RASP supports the following application runtimes:

- Java
- Microsoft .NET
- node
- NET

Imperva RASP protects against

- Command Injection
- Clickjacking
- Cookie-Side Scoping (CSC)
- Cookie-Side Request Forgery (CSRF / XSS)
- Database Access Location (DAL)
- HTML Injection
- HTTP Method Tampering
- HTTP Response Splitting
- Invalid Cookies
- Invalid Transport
- JSON Injection
- Large Payloads
- Logging Sensitive Information
- Malformed Content Types
- OSINT Injection
- Path Traversal
- SQL Injection
- Logging Sensitive Info
- Intensity Transport Protocol
- Unauthenticated Network Activity
- Uncaught Exceptions
- Unvalidated Templates
- Vulnerable Dependencies
- Weak Authentication
- Weak Browser Cache Management
- Weak Cryptography & Ciphers
- XML Injection
- And more...

IMPERVA APPLICATION SECURITY

RASP is a key component of Imperva Application Security, which reduces risk while providing an optimal customer experience. The solution safeguards applications on-premises and in the cloud by:

- Providing actionable security insights
- Protecting against DDoS attacks
- Mitigating botnet attacks
- Monitoring all data activity
- Providing WAF protection
- Blocking cyber-attacks that target APIs
- Ensuring optimal content delivery

Learn more about Imperva Application Security at +1 800 925 4678 or online at www.imperva.com

Imperva is an analyst-recognized cybersecurity leader championing the fight to secure data and applications wherever they reside.



Forrester's research uncovered a market in which Prevoty (now Imperva RASP) leads the pack.

The Forrester New Wave™ Runtime Application Self-Protection Q1 2019. Download the full Forrester report [here](https://www.forrester.com).

imperva.com

imperva

CAPABILITY BRIEF

Attack Analytics

Uncover attacks hiding in an avalanche of security alerts

Security teams are often overwhelmed with the volume and sophistication of emerging threats and relentless data breaches. Ideally they want to receive alerts when a potential risk is seen, and be able to take action based on a clear understanding of the context. Instead they labor under a massive overhead of security events, making it almost impossible to connect the dots and determine where to spend their time. The situation only gets worse as applications are moved to the cloud, presenting new security challenges related to cloud-specific or hybrid environments and a greater need for enterprise-wide visibility.

IT organizations looking for a way to decisively respond to and resolve security events, while avoiding alert fatigue and wasting valuable time chasing down false positives need a smart, analytics tool. One with built-in artificial intelligence would enable them to evaluate large volumes of alerts instantaneously and find commonalities and correlations. Machine learning algorithms would be extremely useful in finding patterns and identifying true security events from among the constant barrage of security alerts.

Imperva Attack Analytics

Imperva Attack Analytics correlates and distills thousands of security events into a few distinct readable narratives. Through sophisticated use of artificial intelligence and machine learning, it takes the mystery out of investigating application security events and enables IT organizations to mitigate and respond to real security threats quickly and decisively. Attack Analytics sorts and groups security events into clusters of narratives, assigning each a severity level so teams can quickly investigate.

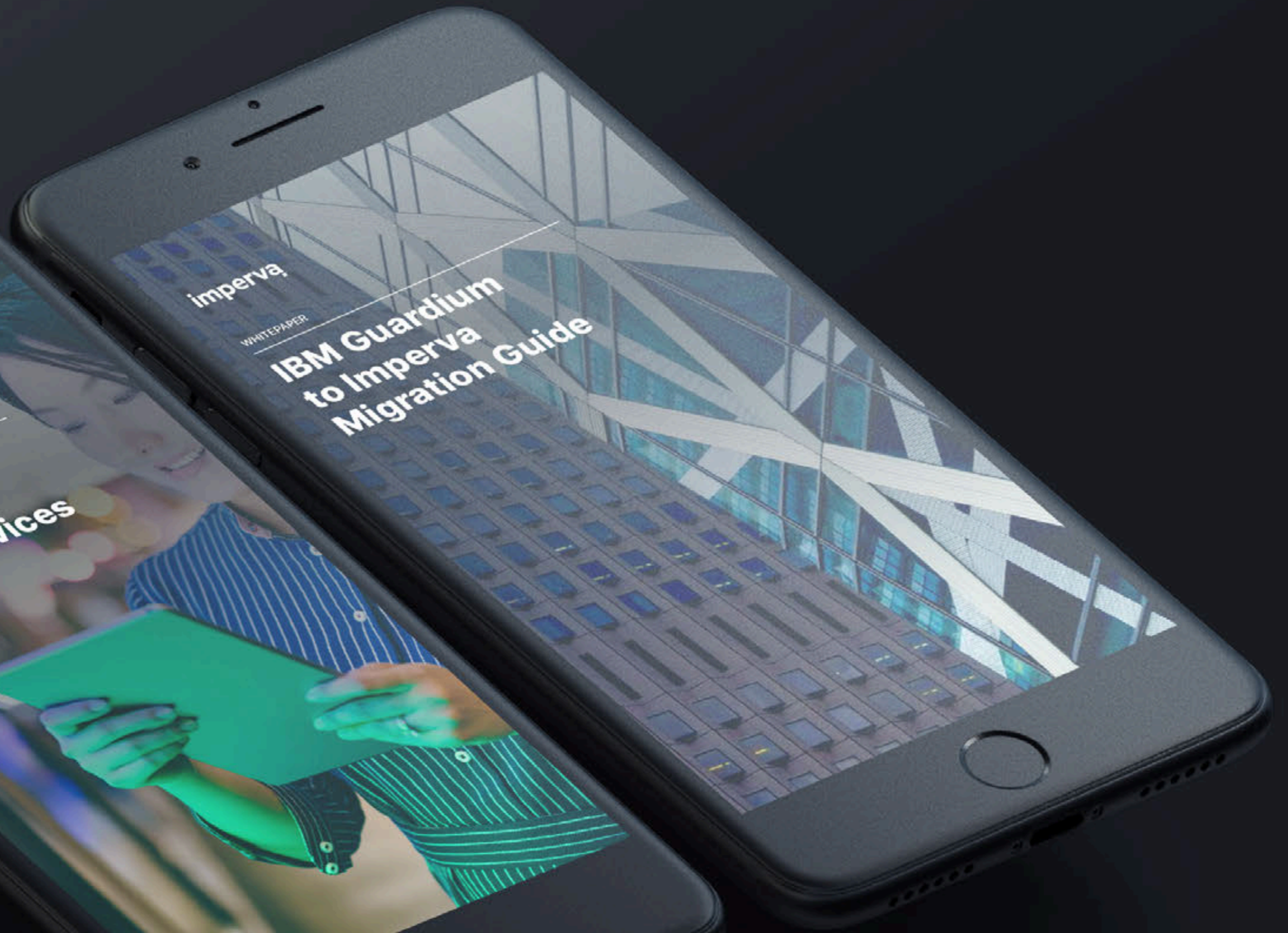
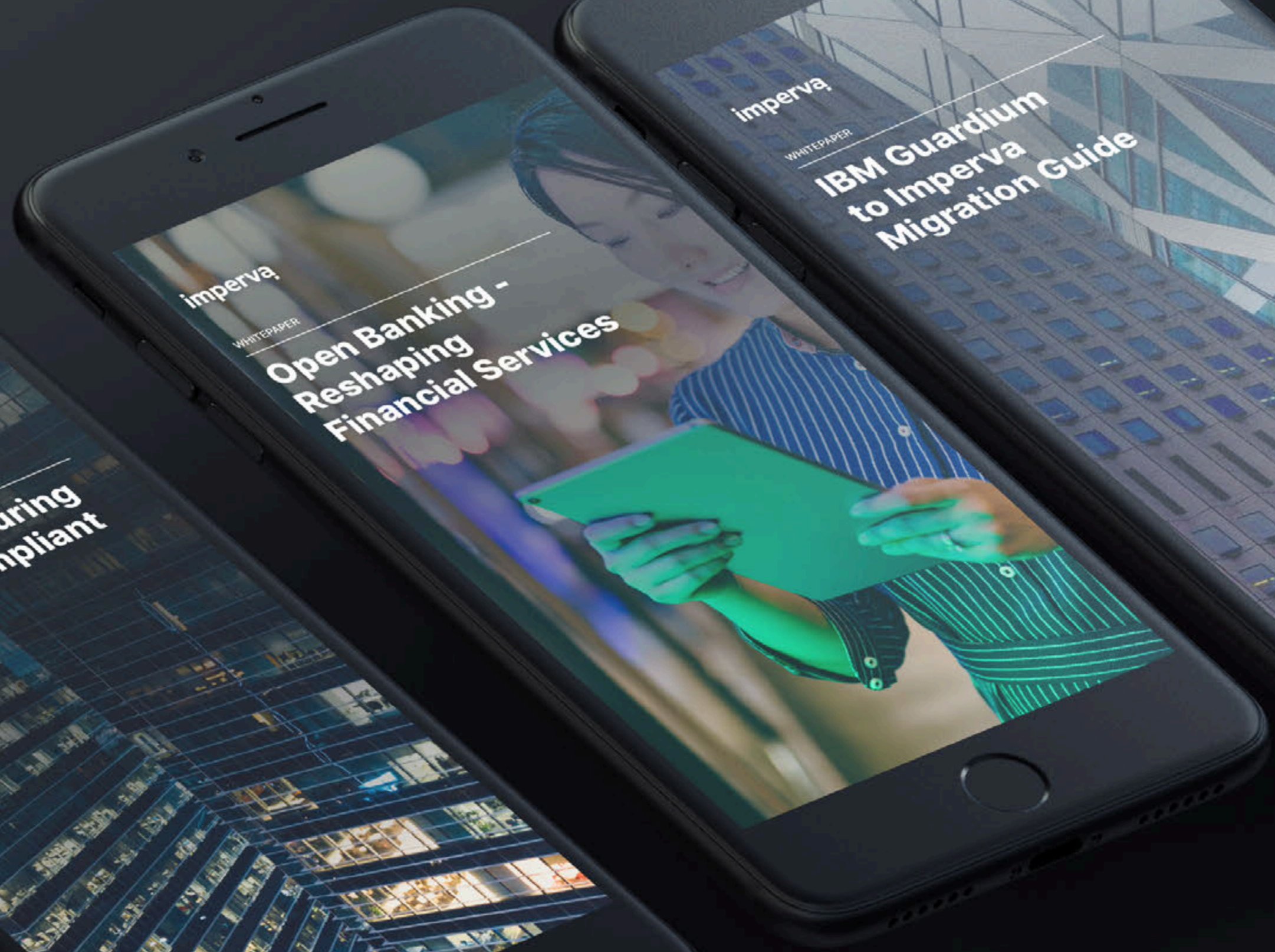
KEY CAPABILITIES

- Correlates and distills thousands of security events into actionable insights
- Cloud-based for easy deployment
- Unified monitoring of cloud and on-premises environments
- Collective intelligence from across the organization
- Expertise that understands the root problem better than anyone else



Attack Analytics distills thousands of security events into a few readable narratives.

imperva.com



Open banking around the world

"What started with PSD2 regulation in Europe in 2018, open banking is now being adopted in various regions around the world."

- The Digital Banker 2020

Open banking in UK

The UK has been somewhat of a trailblazer in terms of open banking adoption. Following an investigation by the Competition and Markets Authority (CMA) into the supply of retail banking services to personal current account customers and to small and medium-sized enterprises (SMEs), open banking was one of a number of changes proposed to improve competition in retail banking and financial services. Trading 4x Open Banking Limited (OBL) was set up by the CMA in 2018 to deliver open banking in the UK.

Open banking was launched in the UK in January 2020, with the five biggest banks and building societies, also known as the CMA5, first to be included in the Open Banking Directory. However, despite the goals with which open banking was introduced in 2020, a number of delays, extensions, and complications were required in 2020. Only now only the CMA5 have been obliged to comply, although some smaller newcomers such as Monzo, Revolut, and Starling Bank, have taken up the challenge willingly.

CMA 5 in the UK

- Hill Street UK (Building as First Trust Bank in Northern Ireland)
- Bank of Ireland (Ireland)
- Barclays Bank
- HSBC Group (Providing First Open and WAP)
- Lloyds Banking Group (Including Bank of Scotland and Halifax)
- Nationwide Building Society
- Northern Bank Limited (Banking as Danske Bank)
- The Royal Bank of Scotland Group (Including Halifax and State Bank)
- Santander UK

The UK is also a leader when it comes to regulation, ensuring that all open banking providers must be regulated by the FCA, and imposing a strict ISO standard designed to enable a well-functioning ecosystem, in which there are no barriers to entry.

According to Sarah Kocotarski in her January 2020 blog 'Open banking 11 Years On', however, there has been frustration on both sides, with the big banks struggling to meet deadlines and move forward with their innovation, and the fintech providers with the need to develop the products and services limiting their ability to progress.

Open Banking - Reshaping Financial Services

Your role in database security and compliance in the cloud

How do you get your data in compliance with the security and compliance of your AWS RDS-powered app with these five essential:

1. Proven Success

Imperva's proven success is a result of our unique ability to identify and prevent threats before they reach your application. Our advanced threat prevention capabilities have been proven to prevent threats before they reach your application, resulting in a 99.9% uptime and a 99.9% success rate in preventing threats.

2. Laser focused on big data

Big data is a complex and challenging environment to secure. Imperva's advanced threat prevention capabilities are designed to protect your big data from threats, ensuring that your data is secure and compliant.

3. Unmatched knowledge and experience

Imperva has over 15 years of experience in protecting cloud environments. Our experts have helped thousands of organizations secure their cloud environments, ensuring that they are compliant and secure.

4. All threats covered - web, mobile and API

Imperva's advanced threat prevention capabilities cover all threats, including web, mobile, and API threats. This ensures that your application is protected from all threats, ensuring that your data is secure and compliant.

5. Imperva is an industry-recognized, cybersecurity leader fighting to secure data and applications wherever they reside.

DATA DISCOVERY & CLASSIFICATION

Discover your data in the cloud and ensure it is protected. Imperva's advanced threat prevention capabilities can help you discover and classify your data, ensuring that it is protected and compliant.

DATA CERTIFICATION & REPORTING

Ensure your data is certified and reported. Imperva's advanced threat prevention capabilities can help you certify and report your data, ensuring that it is compliant and secure.

UNIFIED POLICY ENFORCEMENT

Enforce a consistent security policy across all your cloud environments. Imperva's advanced threat prevention capabilities can help you enforce a consistent security policy across all your cloud environments, ensuring that they are secure and compliant.

Five Things You Must Do to Get AWS RDS Secure and Compliant

Introduction to Imperva Cloud Data Security

Address all data, web, and security challenges by using a cloud database program. Imperva's advanced threat prevention capabilities can help you address all data, web, and security challenges by using a cloud database program.

Holistic approach comprised of the most effective technology.

It's security professionals who fight to make sure that all critical digital assets are protected. Imperva's advanced threat prevention capabilities can help you protect your critical digital assets, ensuring that they are secure and compliant.

Imperva is an industry-recognized, cybersecurity leader fighting to secure data and applications wherever they reside.

1. Proven Success

Imperva's proven success is a result of our unique ability to identify and prevent threats before they reach your application. Our advanced threat prevention capabilities have been proven to prevent threats before they reach your application, resulting in a 99.9% uptime and a 99.9% success rate in preventing threats.

2. Laser focused on big data

Big data is a complex and challenging environment to secure. Imperva's advanced threat prevention capabilities are designed to protect your big data from threats, ensuring that your data is secure and compliant.

3. Unmatched knowledge and experience

Imperva has over 15 years of experience in protecting cloud environments. Our experts have helped thousands of organizations secure their cloud environments, ensuring that they are compliant and secure.

4. All threats covered - web, mobile and API

Imperva's advanced threat prevention capabilities cover all threats, including web, mobile, and API threats. This ensures that your application is protected from all threats, ensuring that your data is secure and compliant.

5. Imperva is an industry-recognized, cybersecurity leader fighting to secure data and applications wherever they reside.

Winner: 2017 Best Fraud Prevention Solution

Verdict: For monitoring the impact of bots on a network, this is the tool one needs.

Gartner

"The only anti-bot solution to be included in Gartner's Online Fraud Detection Market Guide three-years running."