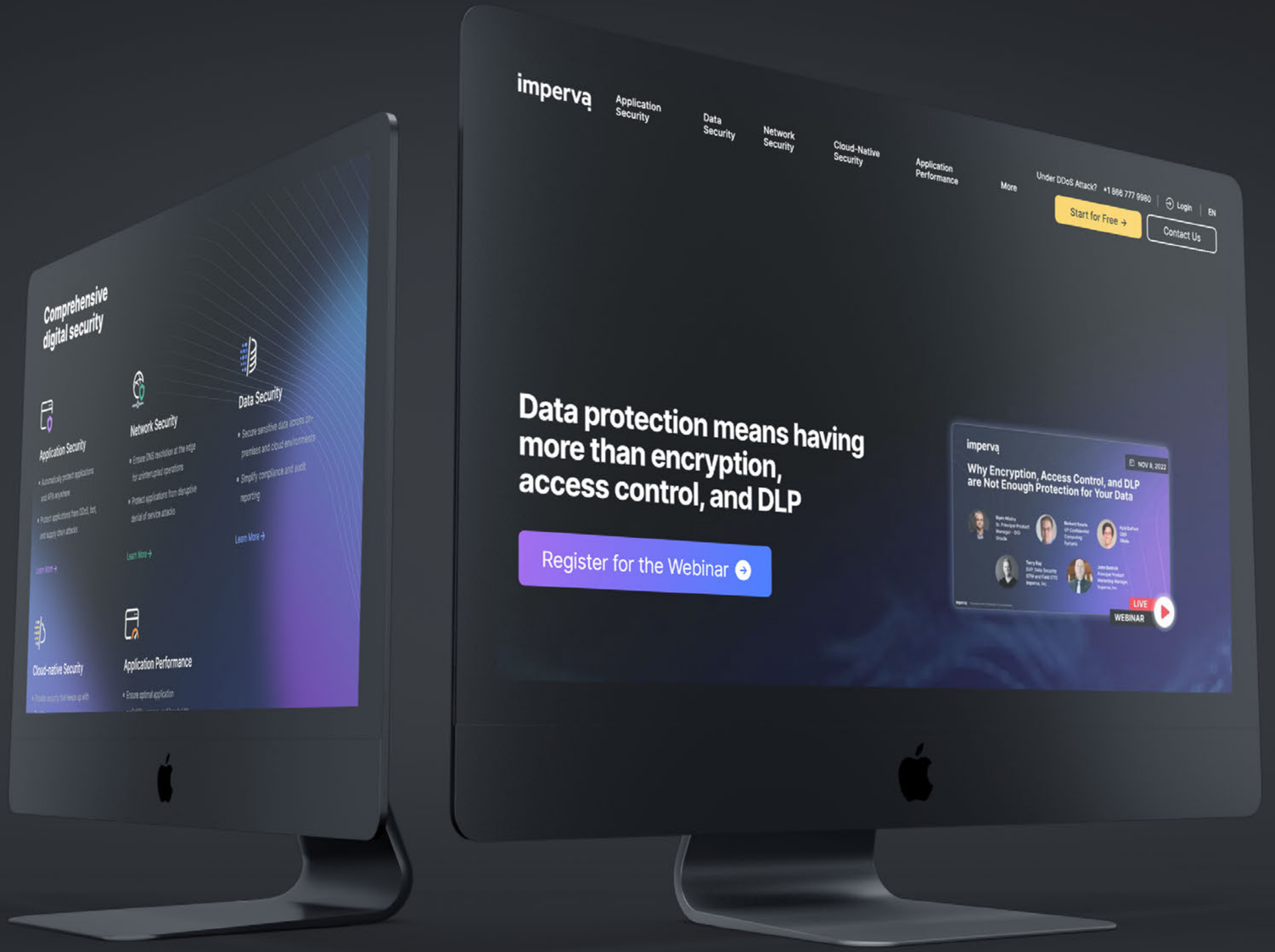
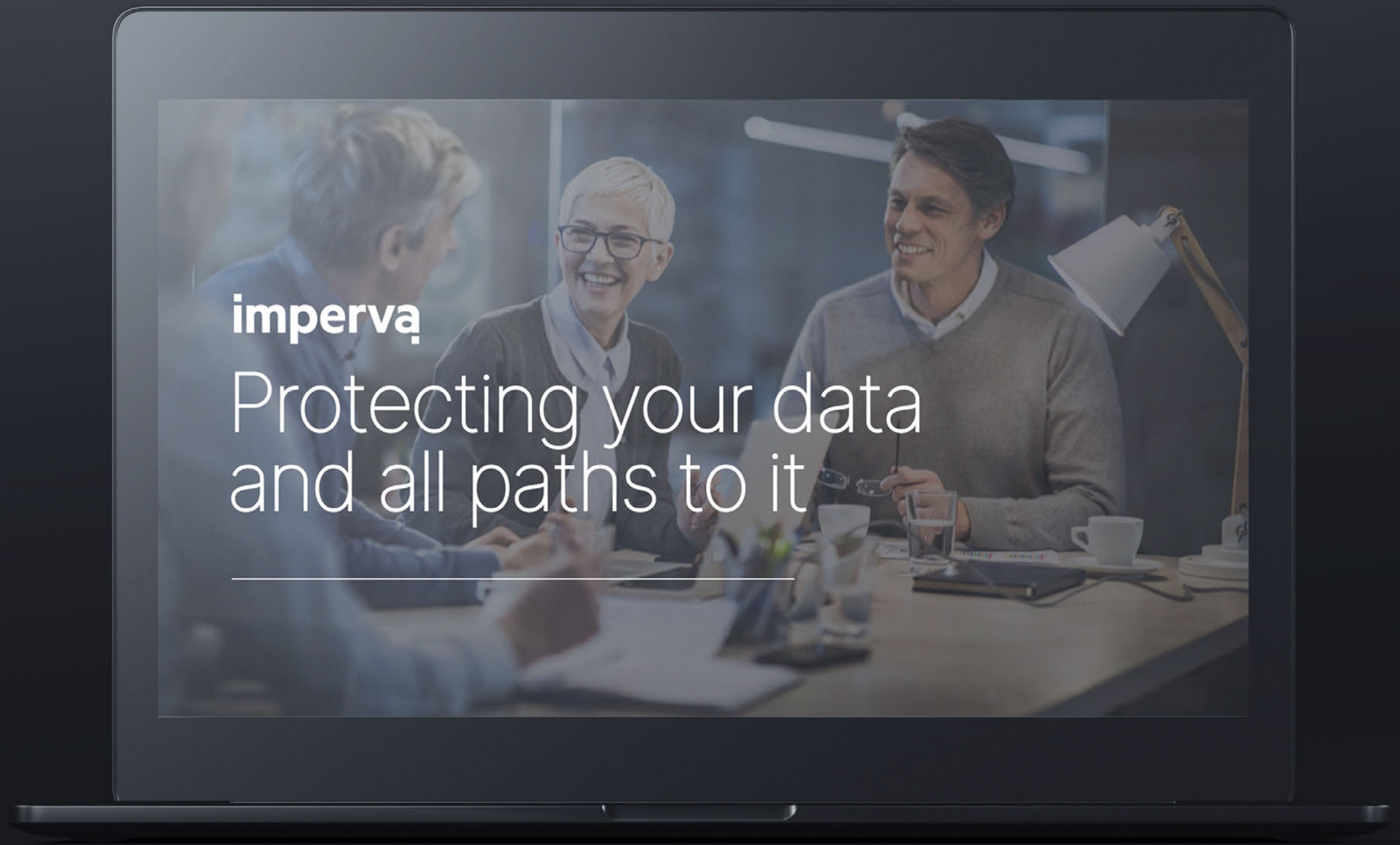
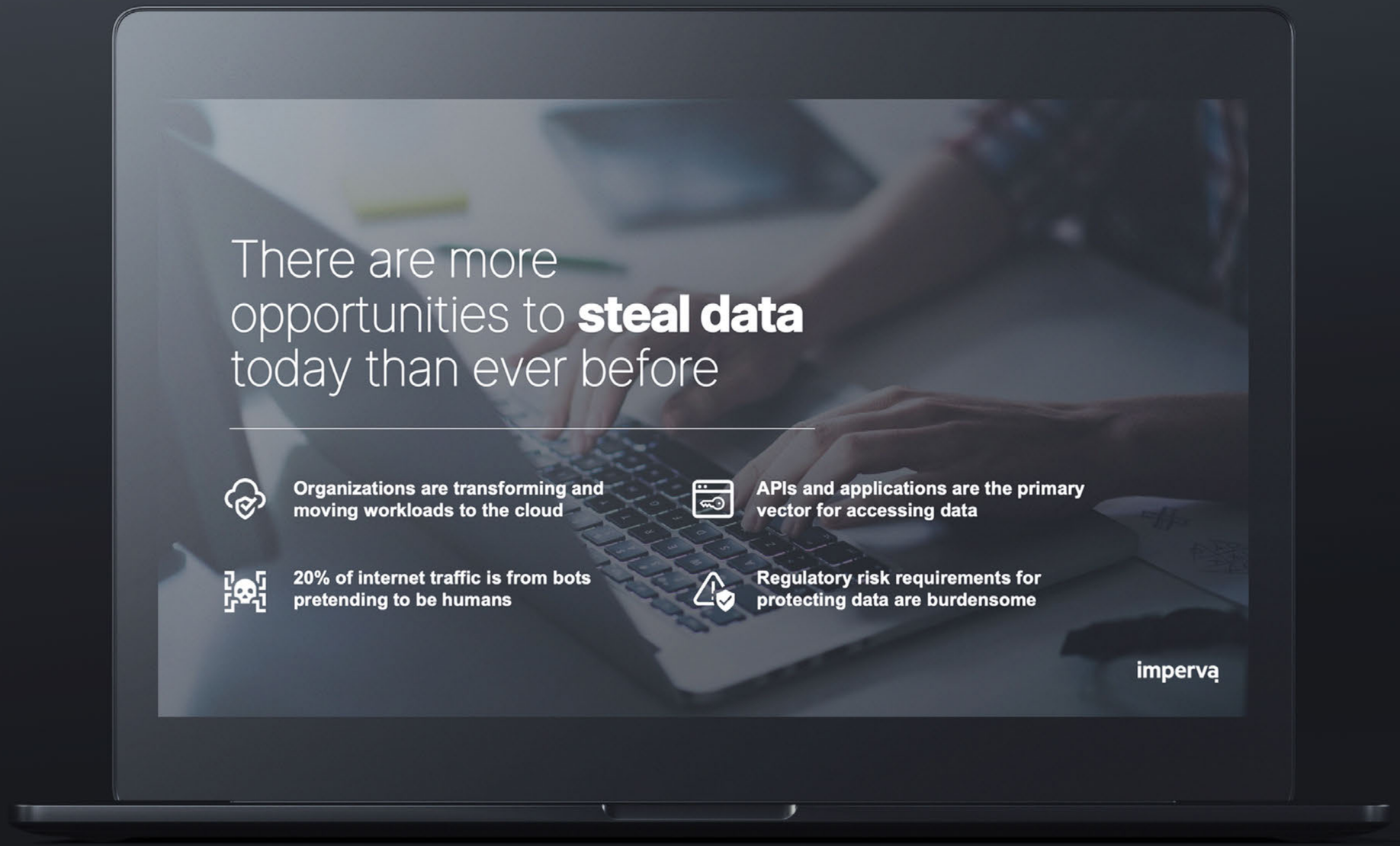
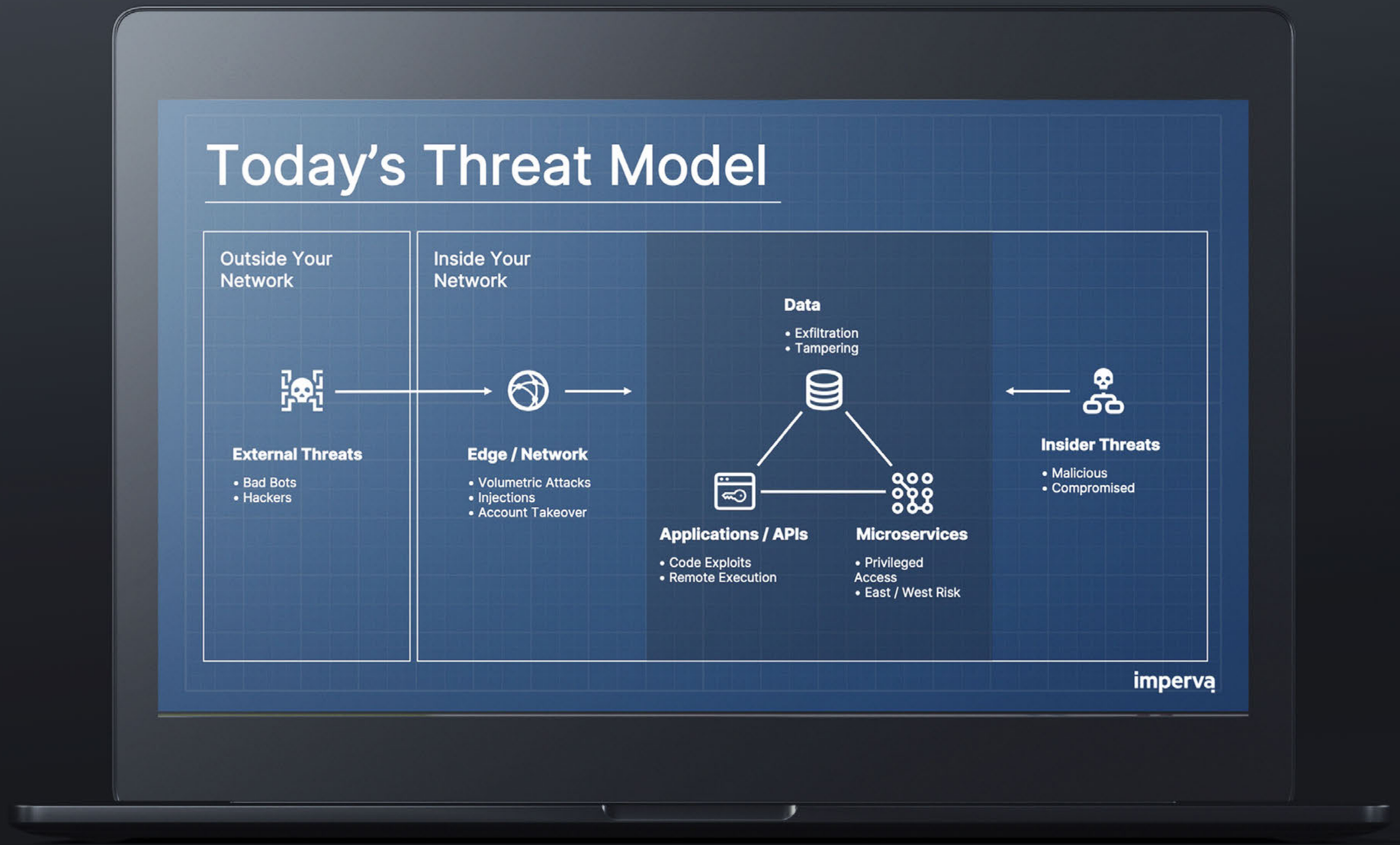

Comprehensive digital security
Application Security
Network Security
Data Security
Cloud-native Security
Application Performance
imperva
Application Security
Data Security
Network Security
Cloud-Native Security
Application Performance
More
Under DDoS Attack? +1 866 777 9980
Login
EN
Start for Free
Contact Us
Data protection means having more than encryption, access control, and DLP
Register for the Webinar
imperva
NOV 9, 2022
Why Encryption, Access Control, and DLP are Not Enough Protection for Your Data
LIVE
WEBINAR


Cloud-Native Security
Legacy security tools lack the visibility and control needed to protect modern infrastructure. Imperva integrates into cloud-native technology to protect your business as it expands cloud operations.
Get more info >
Proven leadership
65+ data repository coverage
Customer testimonials
New infrastructure attack opportunities
Understanding risk changes with cloud
Securify is less connected to developers
Legacy security doesn't help hers
Pervasive characteristics of APIs
Protection for modern infrastructure
Built into modern technology
Advanced visibility for DevOps cultures
Protection against innovative attacks
Comprehensive security at DevOps speed


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
Outside Your Network
Inside Your Network
Data
• Exfiltration
• Tampering
External Threats
• Bad Bots
• Hackers
Edge / Network
• Volumetric Attacks
• Injections
• Account Takeover
Insider Threats
• Malicious
• Compromised
Applications / APIs
• Code Exploits
• Remote Execution
Microservices
• Privileged Access
• East / West Risk
imperva


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 enrichment and insights from a combination of Imperva's 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 sen
applications. When a user logs into the front-end of an application or an API, the database audit only se
account in the connection. Today, there is no simple method to derive who is accessing sensitive
role, etc.), or where user's came from (app or browser, internal or external, hop or not, geo, etc.).
sensitive information is ok. The infrastructure, processors and resources required by
anonymous request from the various disparate tiers in a distributed environment
ineffective.


imperva
DATA SHEET
Runtime Application Self-Protection (RASP)
Securing applications by default
Imperva RASP
KEY CAPABILITIES
Imperva RASP at a glance
Benefits of Imperva Runtime Application Self-Protection
Deployments that scale with DevOps
Imperva RASP supports the following application runtimes:
Java
.NET
node
Imperva RASP protects against
IMPERVA APPLICATION SECURITY
"Forrester's research uncovered a market in which Prevoty (now Imperva RASP) leads the pack."
imperva.com
Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.
imperva

imperva

CAPABILITY BRIEF

Attack Analytics

Uncover attacks hiding in an avalanche of security alerts

KEY CAPABILITIES

Correlates and distills thousands of security events into actionable insights

Cloud-based for fast deployment

Unified monitoring of cl… and on premises

Collecti… dicti…

…expertise that understands the bot problem better than anyone else

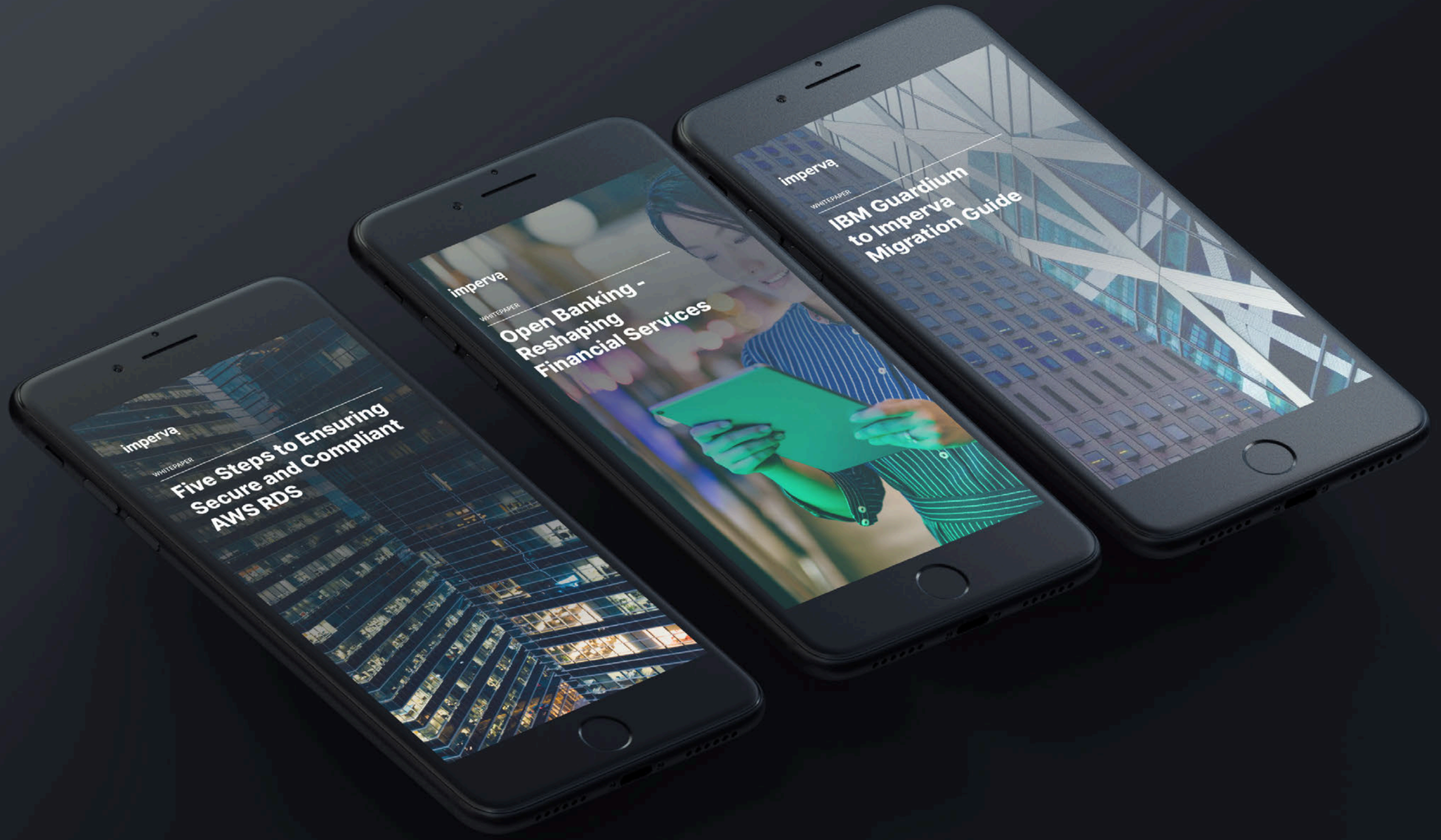
AI powered pattern recognition

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

imperva.com

Imperva Attack Analytics

Attack Analytics - Capability Brief


imperva
WHITEPAPER
Five Steps to Ensuring Secure and Compliant AWS RDS
imperva
WHITEPAPER
Open Banking - Reshaping Financial Services
imperva
WHITEPAPER
IBM Guardium to Imperva Migration Guide

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 nominee 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 is the Open Banking Limited, CMA was set up by the CMA in 2016 to deliver open banking in the UK.

Open banking was launched in the UK in January 2018 with the nine biggest banks and building societies, also known as the CMA9, first to be enabled in the Open Banking Directory. However, despite the push and clarification were required in 2018, some only a number of delays, extensions, and clarifications were required in 2019. Until now only the CMA9 have been obliged to comply, although some smaller newcomers such as Monzo, Revolut, and Starling Bank, have been up the challenge amongst

CMA 9 in the UK

- AIB Group UK (trading as First Trust Bank in Northern Ireland)
- Bank of Ireland (UK)
- Barclays Bank
- HSBC Group (including First Direct and M&S)
- Lloyds Banking Group (including Bank of Scotland and Halifax)
- Nationwide Building Society
- Northern Bank Limited (trading as Danske Bank)
- The Royal Bank of Scotland Group (including NatWest and Ulster Bank)
- Santander UK

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

According to Sarah Kochanski in her January 2020 blog Open Banking 2 Years On, however, there has been frustration on both sides, with the big banks still struggling to meet deadlines, and many brands who are not innovators, and the fintechs frustrated with the banks for delaying the process and blamed by existing their ability to progress.

Your role in database security and compliance in the cloud

How we get to your part in ensuring the security and compliance of your data (DB) clusters data with these five scenarios.

Figure 1: Your Role in database security and compliance in the cloud

DATABASE DISCOVERY - INVENTORY ALL YOUR DATABASES (CUSTOM/3RD PARTY)

ANOMALY DETECTION & RESPONSE

DATA CRITICALITY CLASSIFICATION

AUDIT READINESS REPORTING

UNIFIED POLICY ENFORCEMENT

5 Five Things You Must Always Do (but Still Don't) Secure and Compliant

imperva.com

Introduction to Imperva Cloud Data Security

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

Holistic approach comprised of the most effective technology.

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

Gartner

Ten essential bot management capabilities

1. Proven Success

2. Laser focused on bad bots

3. Unmatched knowledge and experience

4. API security covered: web, mobile and API

"Winner: 2017 Best Fraud Prevention Solution."

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

SC Awards