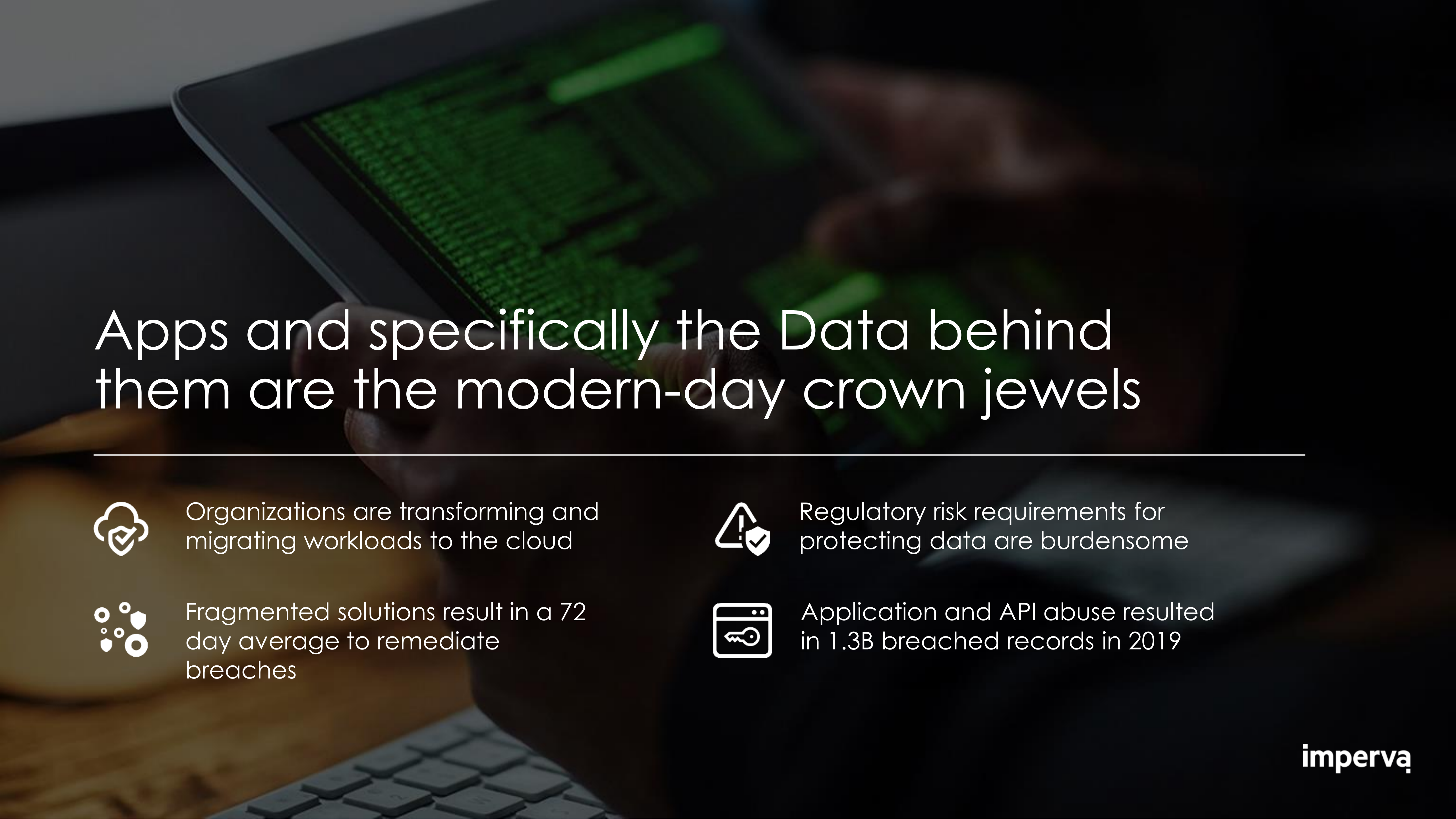
THALES
Building a future we can all trust

Application and API Security

Sachin Thombre
AppSec Specialist
Sachin.thombre@thalesgroup.com

www.thalesgroup.com

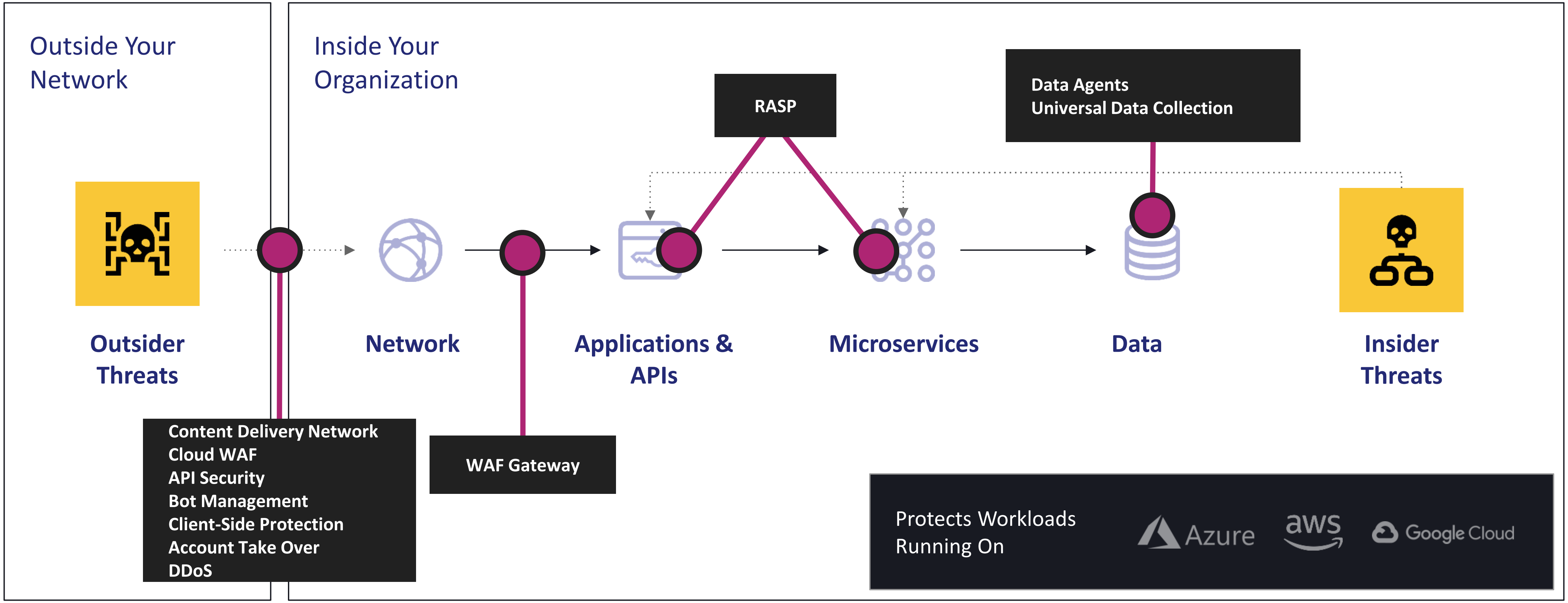


Apps and specifically the Data behind them are the modern-day crown jewels

- Organizations are transforming and migrating workloads to the cloud
- Regulatory risk requirements for protecting data are burdensome
- Fragmented solutions result in a 72 day average to remediate breaches
- Application and API abuse resulted in 1.3B breached records in 2019

imperva

What is Thales Application Security?



Outside Your Network

Inside Your Organization

Outsider Threats

Network

Applications & APIs

Microservices

Data

Insider Threats

RASP

Data Agents
Universal Data Collection

Content Delivery Network
Cloud WAF
API Security
Bot Management
Client-Side Protection
Account Take Over
DDoS

WAF Gateway

Protects Workloads Running On

Application Security: Imperva Cloud WAF

Always-on protection address how 90,000 web applications are still attacked every day

WAF pre-tuned to immediately block

- Zero false positives
- <90% customers in blocking mode

Automation makes better use of resources

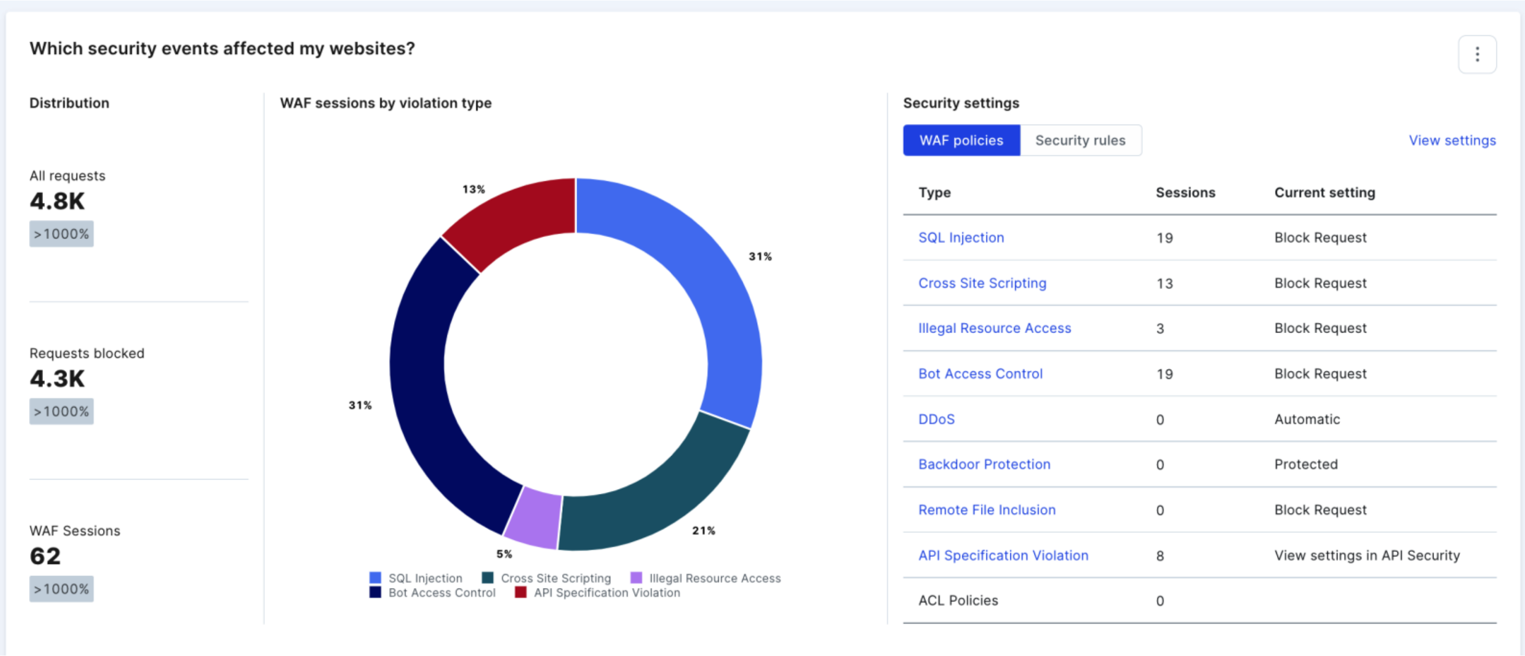
- Combats less accurate manual controls

Security that operates at the speed of DevOps

Allows using third-party code without risk

- 70% of a web application is risky, third-party code

PCI compliance



Which security events affected my websites?

Distribution

All requests
4.8K
>1000%

Requests blocked
4.3K
>1000%

WAF Sessions
62
>1000%

WAF sessions by violation type

Security settings

WAF policies | Security rules | View settings

Type	Sessions	Current setting
SQL Injection	19	Block Request
Cross Site Scripting	13	Block Request
Illegal Resource Access	3	Block Request
Bot Access Control	19	Block Request
DDoS	0	Automatic
Backdoor Protection	0	Protected
Remote File Inclusion	0	Block Request
API Specification Violation	8	View settings in API Security
ACL Policies	0	

Application Security: Imperva CDN (Content Delivery Network) - App Delivery

Content Delivery Network and Load Balancing, included in Cloud WAF

Full-featured API

- Built- in Content Delivery Network (**CDN**) integrates security and delivery rules for no perf impact

Instant, flexible cache purge

- Supports fast changing content
- Soft, wildcard and global – in milliseconds

Rapid config changes

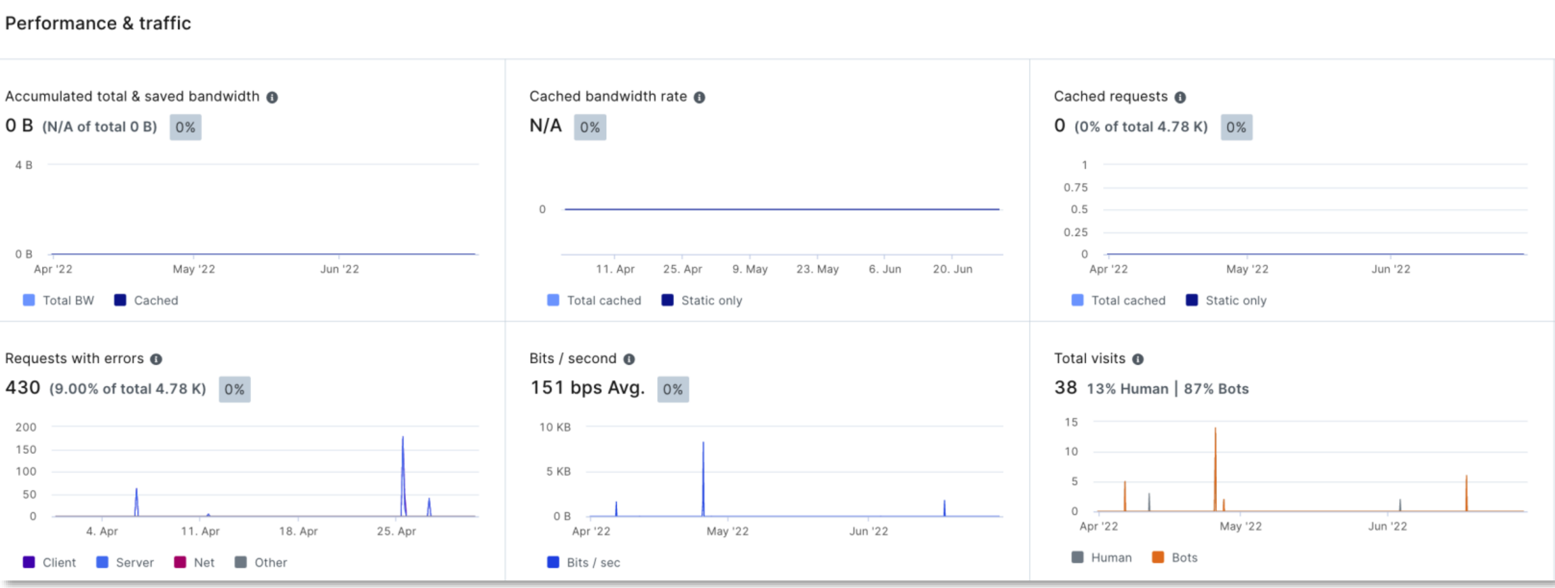
- Deploy globally in seconds

Load balancer

- Real-time health monitoring

Dev-friendly

- Cache tags



Performance & traffic

Accumulated total & saved bandwidth

0 B (N/A of total 0 B) 0%

Cached bandwidth rate

N/A 0%

Cached requests

0 (0% of total 4.78 K) 0%

Requests with errors

430 (9.00% of total 4.78 K) 0%

Bits / second

151 bps Avg. 0%

Total visits

38 13% Human | 87% Bots

Application Security:
On-premise Imperva WAF Gateway

Flexible solution protects applications and APIs

- Supports hybrid environments (on-prem and cloud)
- Deploy as appliance or virtual machine

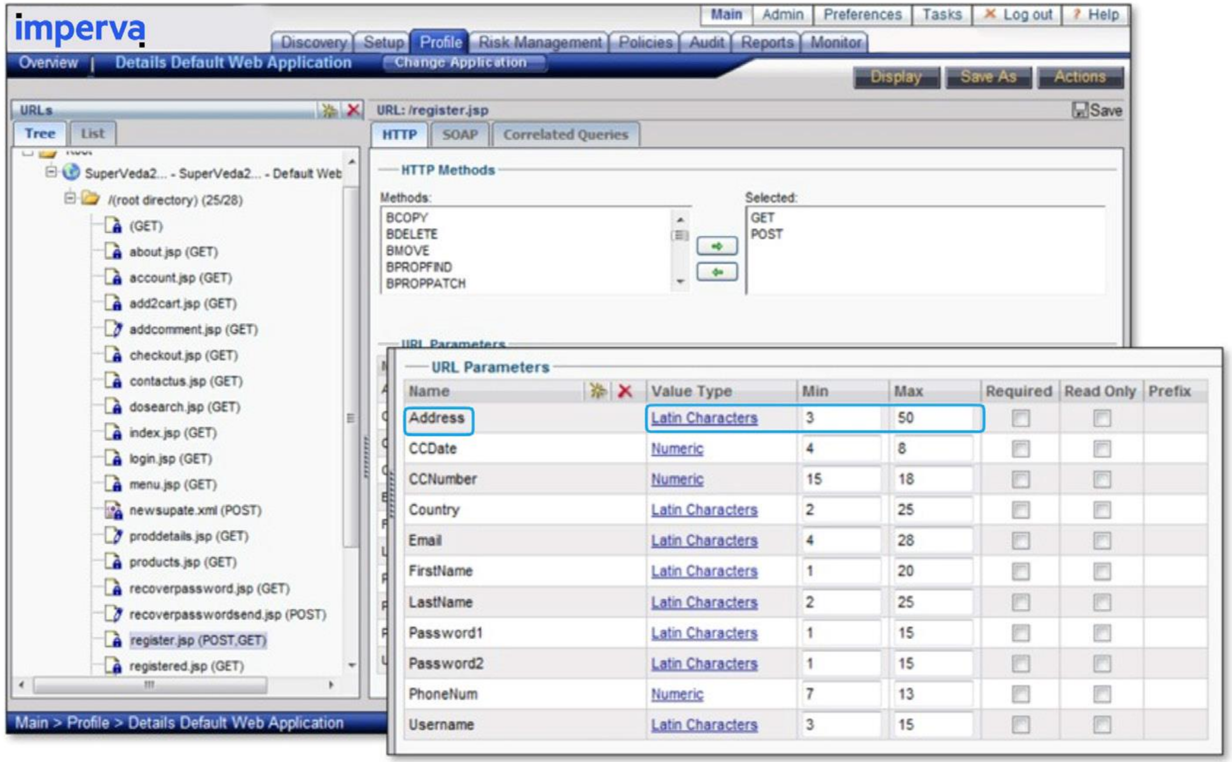
Highly configurable

- Tight protection for specific applications
- Implement as a bridge or reverse proxy engine
- Near zero false positives

Uncompromised security

- Positive security - block anomalies and illegal traffic
- Automated virtual patching
- Integration with Reputation Services

Simplified event investigation with Attack Analytics



URL: /register.jsp

SuperVeda2... - SuperVeda2... - Default Web
/(root directory) (25/28)
(GET)
about.jsp (GET)
account.jsp (GET)
add2cart.jsp (GET)
addcomment.jsp (GET)
checkout.jsp (GET)
contactus.jsp (GET)
dosearch.jsp (GET)
index.jsp (GET)
login.jsp (GET)
menu.jsp (GET)
newsupate.xml (POST)
proddetails.jsp (GET)
products.jsp (GET)
recoverpassword.jsp (GET)
recoverpasswordsend.jsp (POST)
register.jsp (POST,GET)
registered.jsp (GET)

Methods:
BCOPY
BDELETE
BMOVE
BPROPFIND
BPROPPATCH

Selected:
GET
POST

Name	Value Type	Min	Max	Required	Read Only	Prefix
Address	Latin Characters	3	50	□	□	
CCDate	Numeric	4	8	□	□	
CCNumber	Numeric	15	18	□	□	
Country	Latin Characters	2	25	□	□	
Email	Latin Characters	4	28	□	□	
FirstName	Latin Characters	1	20	□	□	
LastName	Latin Characters	2	25	□	□	
Password1	Latin Characters	1	15	□	□	
Password2	Latin Characters	1	15	□	□	
PhoneNum	Numeric	7	13	□	□	
Username	Latin Characters	3	15	□	□	

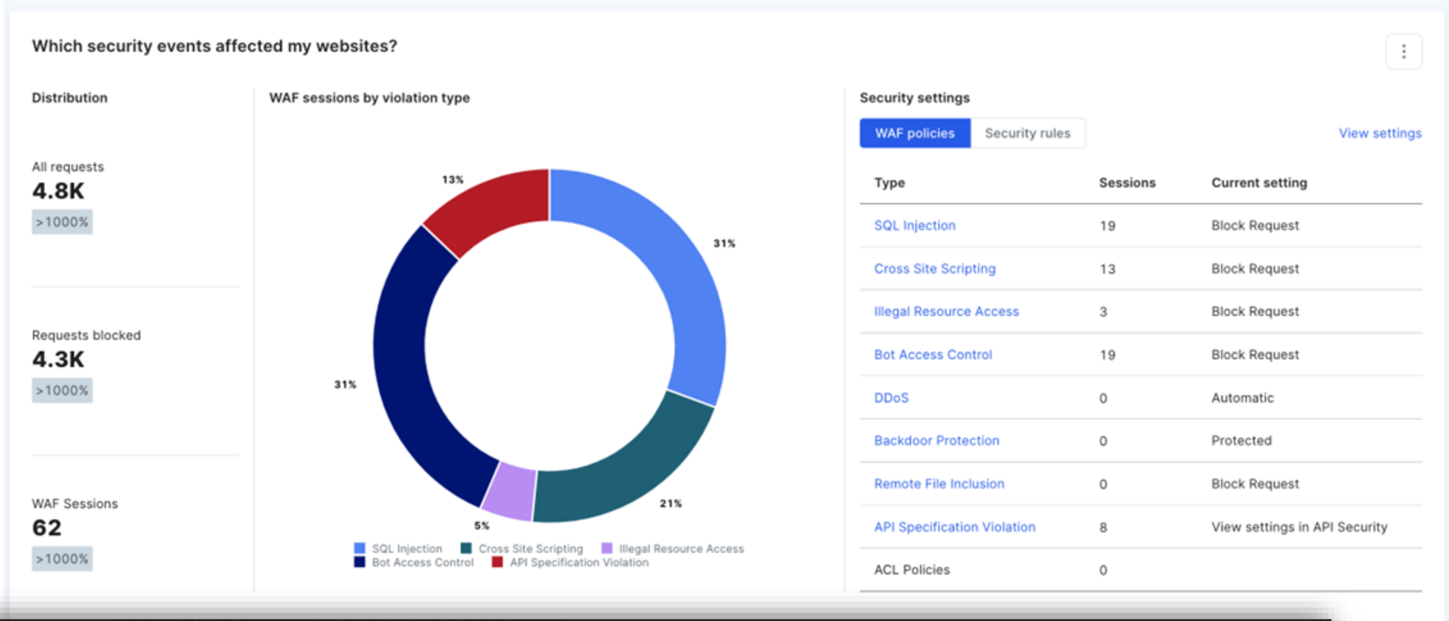
Main > Profile > Details Default Web Application

Application Security: Imperva Elastic WAF

Deploying WAF in Devops Environnent, managed in Cloud WAF

Benefits

- Natively embedded in cloud native environment
- WAF not in the critical path of the data
- Also protects East-West traffic
- It supports blocking
- Leverages the Imperva SaaS ecosystem for threat protection
- Provides visibility into web infra attacks
- Allows for centralized management of the on-prem WAF deployment via the Cloud Security Console
- Offers a singular WAF experience for both Cloud WAF & On-prem WAF environments
- Natively integrates security into CI/CD



Which security events affected my websites?

Distribution

All requests
4.8K
>1000%

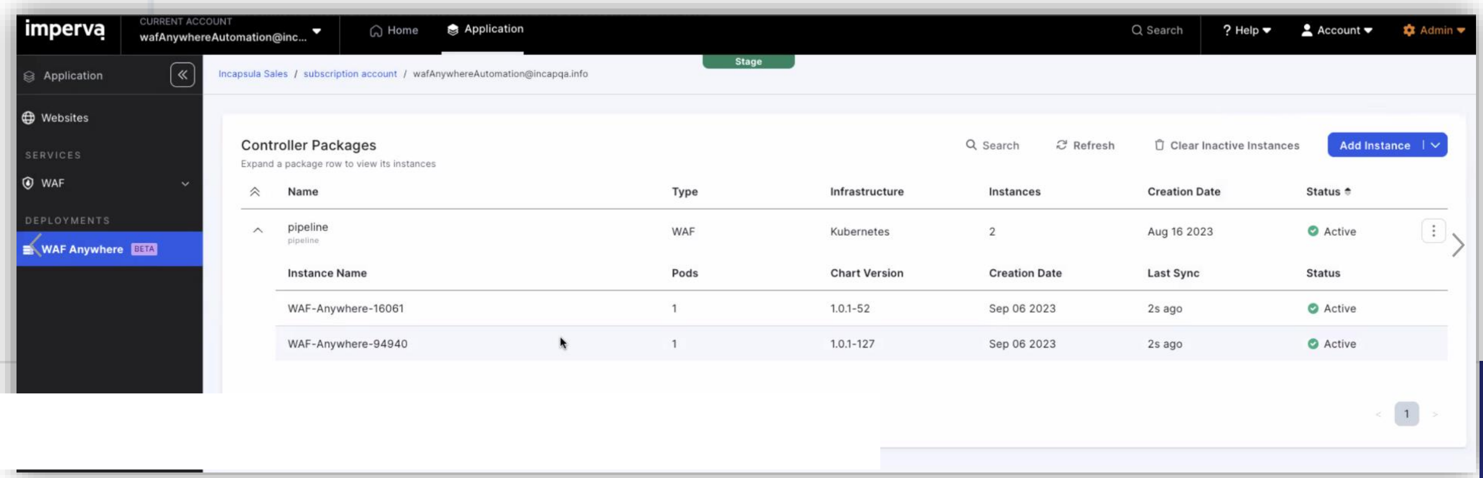
Requests blocked
4.3K
>1000%

WAF Sessions
62
>1000%

WAF sessions by violation type

Security settings

Type	Sessions	Current setting
SQL Injection	19	Block Request
Cross Site Scripting	13	Block Request
Illegal Resource Access	3	Block Request
Bot Access Control	19	Block Request
DDoS	0	Automatic
Backdoor Protection	0	Protected
Remote File Inclusion	0	Block Request
API Specification Violation	8	View settings in API Security
ACL Policies	0	



Incapsula Sales / subscription account / wafAnywhereAutomation@incapqa.info

Controller Packages

Expand a package row to view its instances

Name	Type	Infrastructure	Instances	Creation Date	Status
pipeline pipeline	WAF	Kubernetes	2	Aug 16 2023	Active

Instance Name	Pods	Chart Version	Creation Date	Last Sync	Status
WAF-Anywhere-16061	1	1.0.1-52	Sep 06 2023	2s ago	Active
WAF-Anywhere-94940	1	1.0.1-127	Sep 06 2023	2s ago	Active

Application Security: Imperva API Security

Positive Security Model generated automatically from your OpenAPI specification file

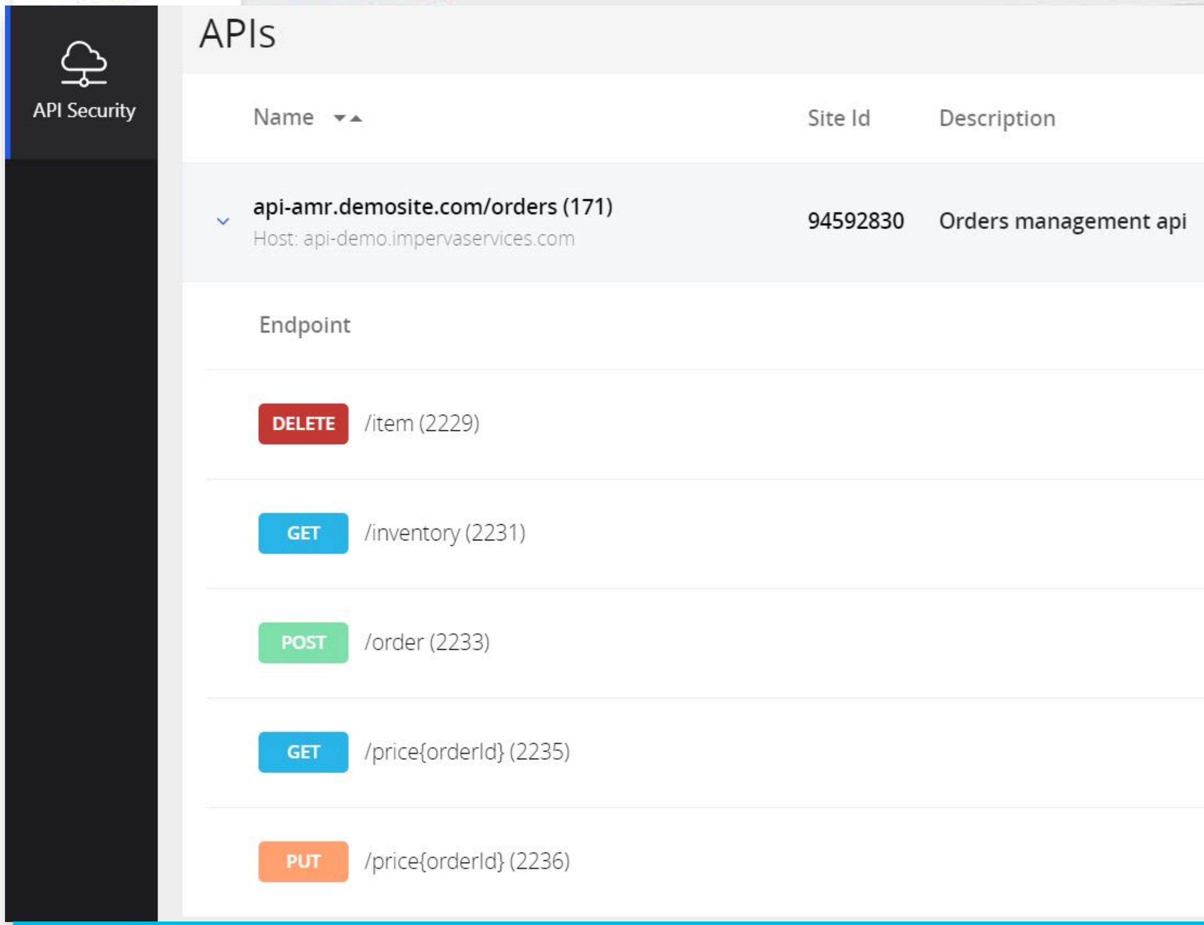
- Automatic enforcement of OPENAPI specification
- Changes updated automatically

Single stack to protect both websites and APIs

- Attack Analytics includes API security events
- Build on the existing capabilities of our Cloud WAF, CDN, Load Balancing and Layer 3/4 DDoS protection

Seamless integration with leading API management vendors

- Removes load from API application
- Supports AWS, Azure & Red Hat 3scale



APIs

Name	Site Id	Description
api-amr.demosite.com/orders (171) Host: api-demo.impervaservices.com	94592830	Orders management api

Endpoint

- DELETE /item (2229)
- GET /inventory (2231)
- POST /order (2233)
- GET /price{orderId} (2235)
- PUT /price{orderId} (2236)

Application Security: Imperva Advanced Bot Protection

Stop Advanced Persistent Bots

Block the Most Sophisticated Bots

- Before it ever reaches your site.
- Via real-time classification and machine learning.
- Without affecting the flow of business-critical traffic.

Protect all Attack Vectors (Web, Mobile, API)

- Deploy in any environment to protect against automated attacks.

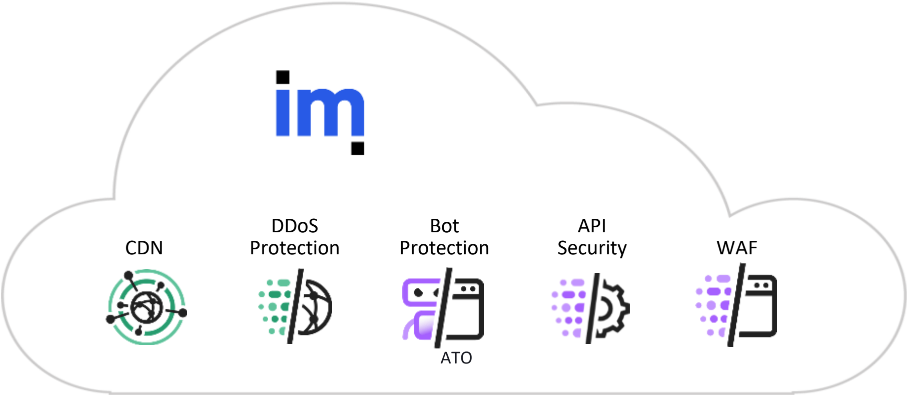
Manage with Precision

- Eliminate friction for legitimate users; false positive reporting, tuning.

Vigilant Service

- The most experienced bot experts in the world.

Integrated in Imperva Cloud App Security



Stand Alone Connectors

Deploy into existing environment

Connector for AWS — aws

Connector for F5 — f5

Connector for Cloudflare — CLOUDFLARE

Connector for NGINX — NGINX

Connector for Fastly — fastly

Application Security: Imperva Client-Side Protection (CSP)

Prevents data theft through client-side attacks like formjacking, digital skimming, supply chain, and Magecart.

Discovery

- Visibility into 3rd-party JavaScript Services on website

Insights

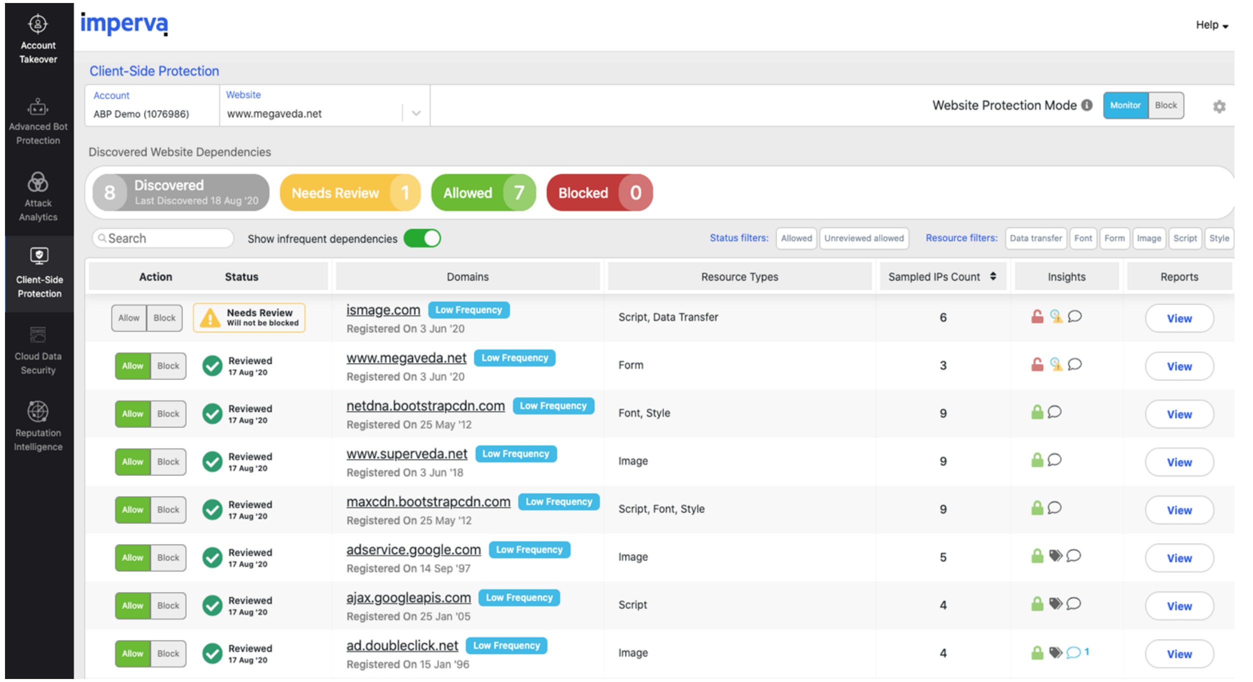
- Help makes security decisions about any discovered services

Enforcement

- Control over malicious or unauthorized JavaScript services

Compliance

- Meet PCI, GDPR, CCPA



Client-Side Protection

Account: ABP Demo (1076986)

Website: www.megaveda.net

Website Protection Mode: Monitor | Block

Discovered Website Dependencies

8 Discovered — Last Discovered 18 Aug '20 | Needs Review 1 | Allowed 7 | Blocked 0

Search | Show infrequent dependencies | Status filters: Allowed, Unreviewed allowed | Resource filters: Data transfer, Font, Form, Image, Script, Style

Action	Status	Domains	Resource Types	Sampled IPs Count	Insights	Reports
Allow | Block	Needs Review Will not be blocked	ismage.com Low Frequency Registered On 3 Jun '20	Script, Data Transfer	6	🔓 ⚠ 💬	View
Allow | Block	Reviewed 17 Aug '20	www.megaveda.net Low Frequency Registered On 3 Jun '20	Form	3	🔓 ⚠ 💬	View
Allow | Block	Reviewed 17 Aug '20	netdna.bootstrapcdn.com Low Frequency Registered On 25 May '12	Font, Style	9	🔒 💬	View
Allow | Block	Reviewed 17 Aug '20	www.superveda.net Low Frequency Registered On 3 Jun '18	Image	9	🔒 💬	View
Allow | Block	Reviewed 17 Aug '20	maxcdn.bootstrapcdn.com Low Frequency Registered On 25 May '12	Script, Font, Style	9	🔒 💬	View
Allow | Block	Reviewed 17 Aug '20	adservice.google.com Low Frequency Registered On 14 Sep '97	Image	5	🔒 🏷 💬	View
Allow | Block	Reviewed 17 Aug '20	ajax.googleapis.com Low Frequency Registered On 25 Jan '05	Script	4	🔒 🏷 💬	View
Allow | Block	Reviewed 17 Aug '20	ad.doubleclick.net Low Frequency Registered On 15 Jan '96	Image	4	🔒 🏷 💬 1	View

Application Security: Imperva Account Take Over (ATO)

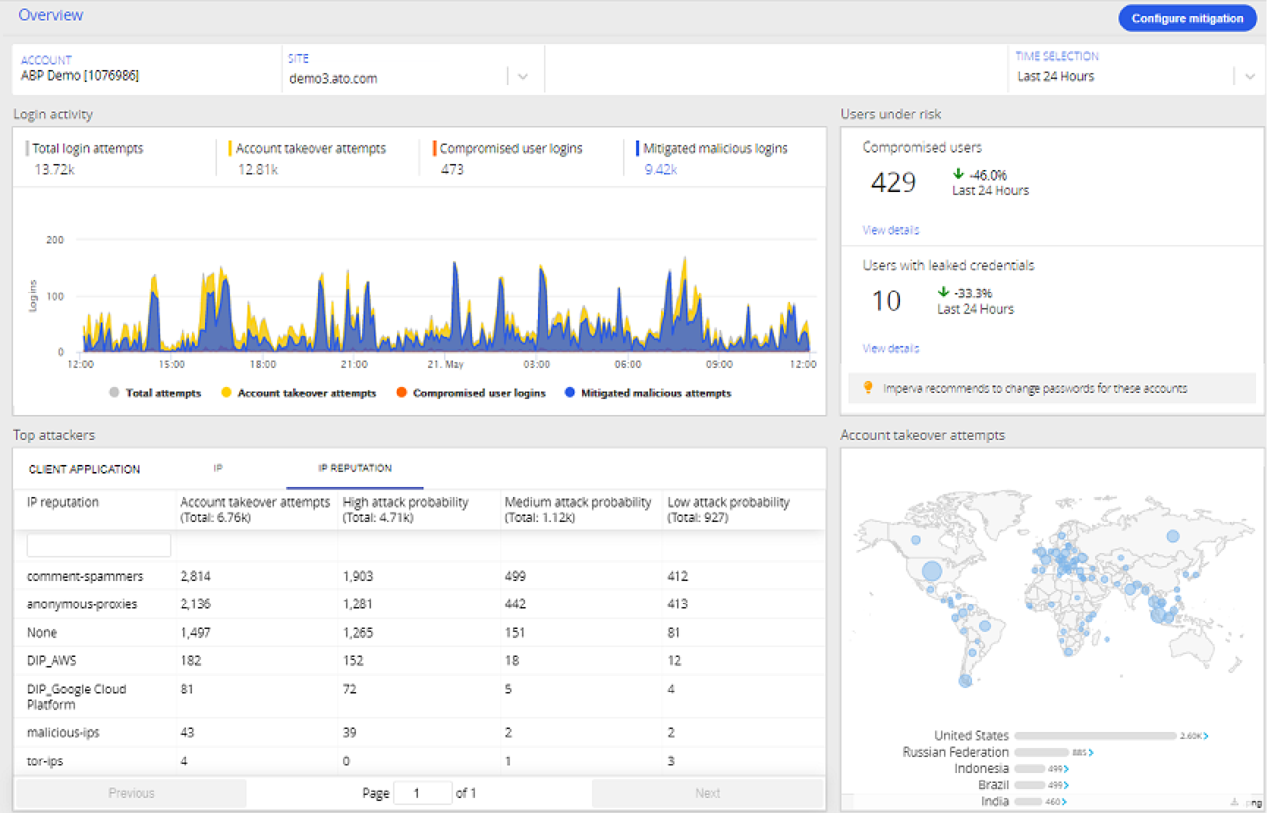
ATO Protection detects and mitigates account takeover attempts, protecting your web applications against volumetric and low and slow ATO attacks.

User Behavior Anomaly Detection

Real-time login protection with no added latency

Minimal user configuration and interaction

Clear visibility into attack attempts, users at risk, and compromised user accounts



ACCOUNT
ABP Demo [1076986]

SITE
demo3.ato.com

TIME SELECTION
Last 24 Hours

Login activity

Total login attempts	Account takeover attempts	Compromised user logins	Mitigated malicious logins
13.72k	12.81k	473	9.42k

Users under risk

Compromised users
429 -46.0% Last 24 Hours

Users with leaked credentials
10 -33.3% Last 24 Hours

Imperva recommends to change passwords for these accounts

Top attackers

IP reputation	Account takeover attempts (Total: 6.76k)	High attack probability (Total: 4.71k)	Medium attack probability (Total: 1.12k)	Low attack probability (Total: 927)
comment-spammers	2,814	1,903	499	412
anonymous-proxies	2,136	1,281	442	413
None	1,497	1,265	151	81
DIP_AWS	182	152	18	12
DIP_Google Cloud Platform	81	72	5	4
malicious-ips	43	39	2	2
tor-ips	4	0	1	3

Page 1 of 1

Account takeover attempts

Application Security: Imperva DDoS Protection

Most Comprehensive, Mature Services – Detailed Protection Matrix

DDoS for Websites	DDoS for DNS	DDoS for Networks	DDoS for Individual IPs
Websites / web applications Application / Network / Protocol attacks **(Layer 3/4/7)** **Always-on**	Domain name servers Application / Network / Protocol attacks **(Layer 3/4/7)** **Always-on**	Entire networks or subnets Any infrastructure asset: Email/ File/ Web/ Gaming/ VoiIP servers, any other IP-based app Network / Protocol attacks **(Layer 3/4)** **Always-on** or **On-demand**	Any online asset hosted in the cloud or on-prem When you don't own C Class range/networking equipment with BGP Migrating workloads to the cloud but still need to run apps on-prem (hybrid) Network / Protocol attacks (Layer 3/4) **Always-on**

Four DDoS Protection Offerings

An overview of our DDoS protection services

	DDoS for Web	DDoS for DNS	DDoS for Networks	DDoS for IPs
Asset	Websites	DNS servers	Class-C+ network	Individual IPs
Customer	With sites/apps	With DNS Infra	Enterprises with DCs	With cloud assets
Operation	Always On	Always On	AO + On-Demand	Always On
Method	DNS Update (A)	DNS Update (NS)	BGP advertising	DNS Update
Trafic	Ingress+Egress	Ingress+Egress	Ingress Only	Ingress+Egress
Protocole	HTTP	TCP, UDP	TCP, UDP	TCP, UDP
Connectivity	TCP Proxy	TCP Proxy	GRE, ECX, Peering	TCP Proxy, GRE, IPnP, IPinIP

Key Advantages: App/API Security Portfolio

Attack Analytics

Correlate and distill thousands of security events into a few readable security narratives

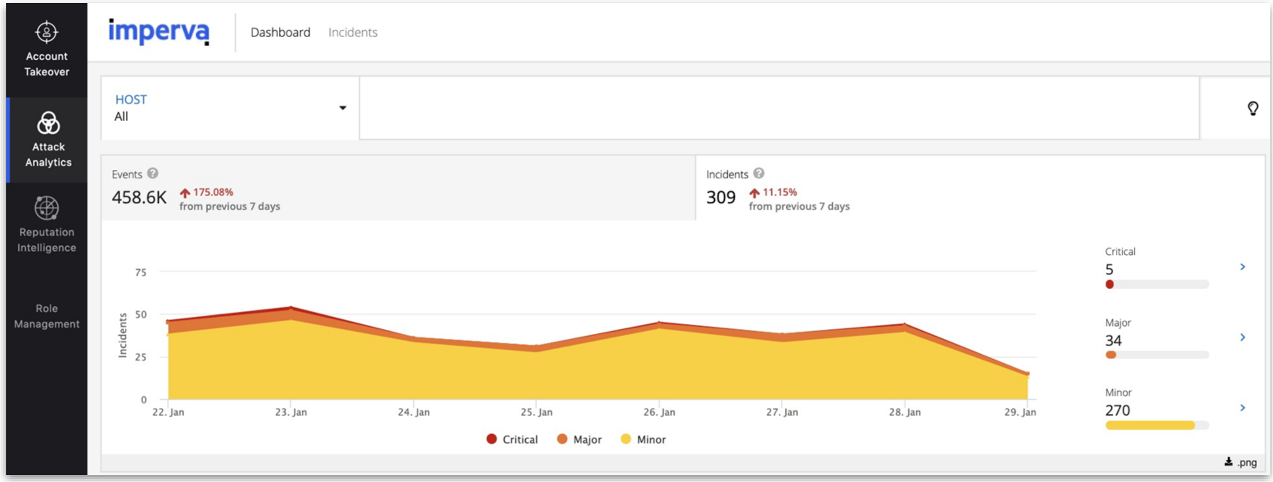
- Leverage threat information to provide unified and contextual insights
- Infinitely scalable

Single Stack approach to visibility

- Identify enterprise-wide attack campaigns
- Remove complexity of investigating security events

Seamless integration

- Cloud WAF, WAF Gateway, Adv. Bot Protection (incl. ATO Protection), DDoS Protection, and API Security attacks
- Easily share and distribute with SIEMs like Splunk



HOST
All

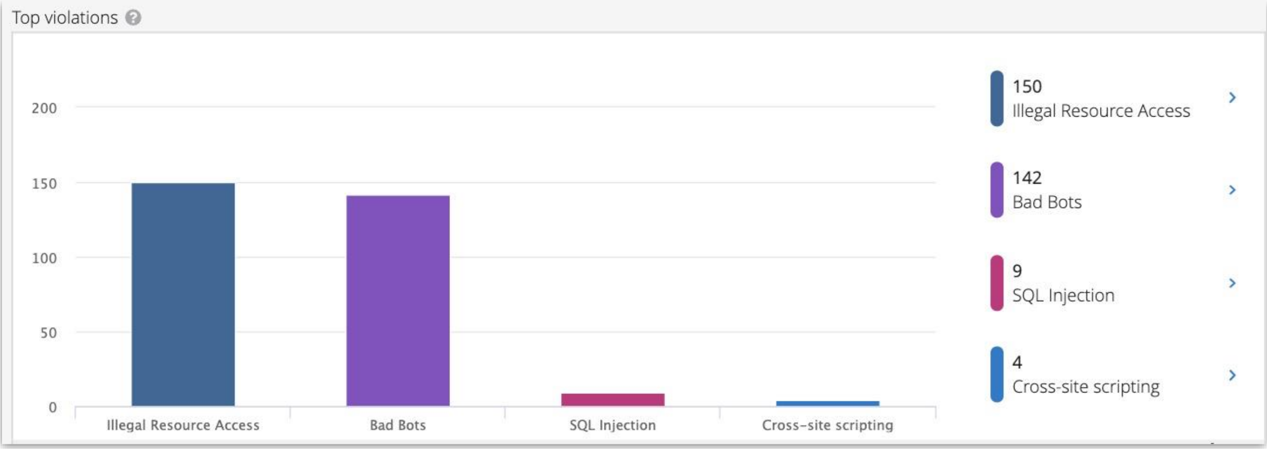
Events 458.6K ↑ 175.08% from previous 7 days

Incidents 309 ↑ 11.15% from previous 7 days

Critical 5

Major 34

Minor 270



150 Illegal Resource Access

142 Bad Bots

9 SQL Injection

4 Cross-site scripting

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales **© 2025 THALES. All rights reserved.**

THALES GROUP LIMITED DISTRIBUTION - SCOPE

Cloud WAF Security

Crowdsourcing

Big Data analysis on

3.5 million bad requests blocked every minute

Clear visibility on web attack landscape

Layered Security

Most up to date

IP Reputation lists

Client Classification

WAF Signatures

<.01% false positive rate

Covers all OWASP Top 10 threats

Cloud Based

Unified Security

No hardware or software

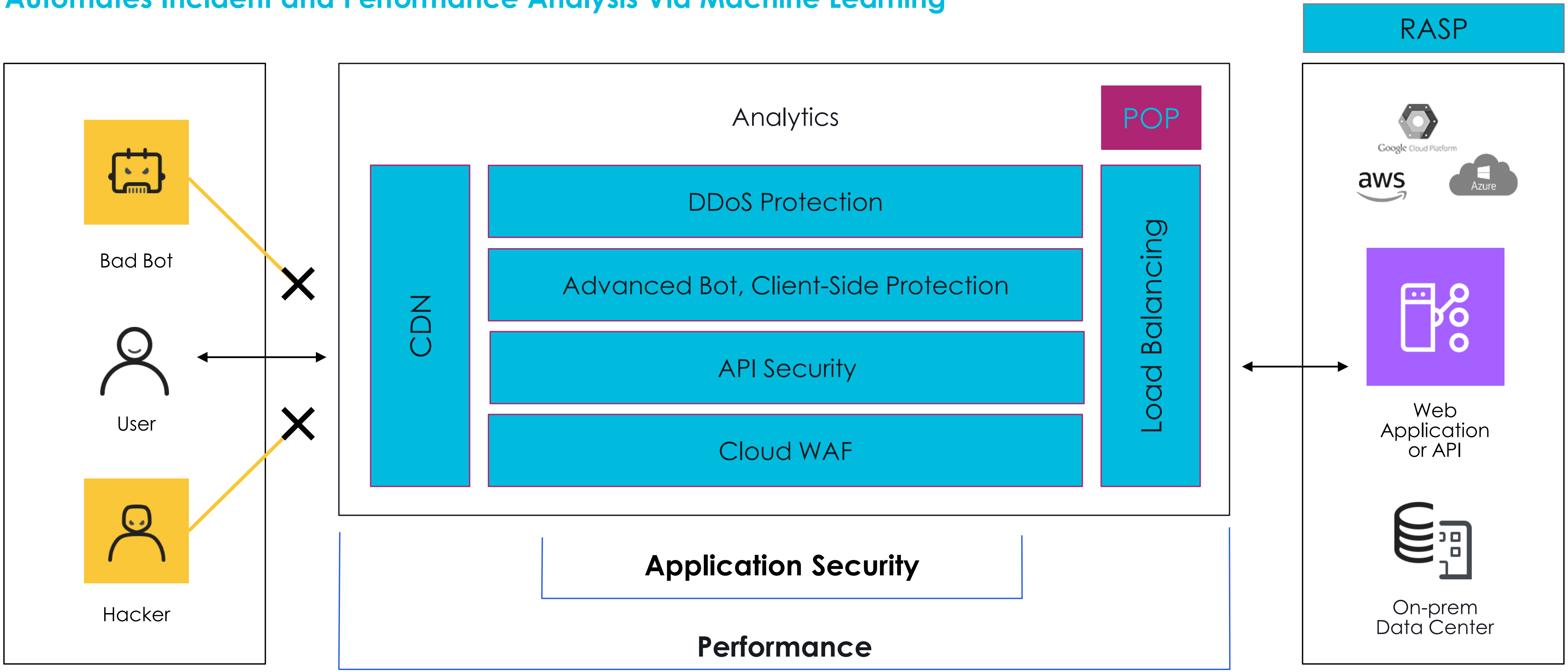
Deployed in minutes

No expertise needed - rely on Imperva Research Labs

Rules propagate automatically

Single Stack Security + Delivery

Automates Incident and Performance Analysis Via Machine Learning


RASP
Bad Bot
User
Hacker
Analytics
POP
CDN
DDoS Protection
Advanced Bot, Client-Side Protection
API Security
Cloud WAF
Load Balancing
Application Security
Performance
Google Cloud Platform
aws
Azure
Web Application or API
On-prem Data Center