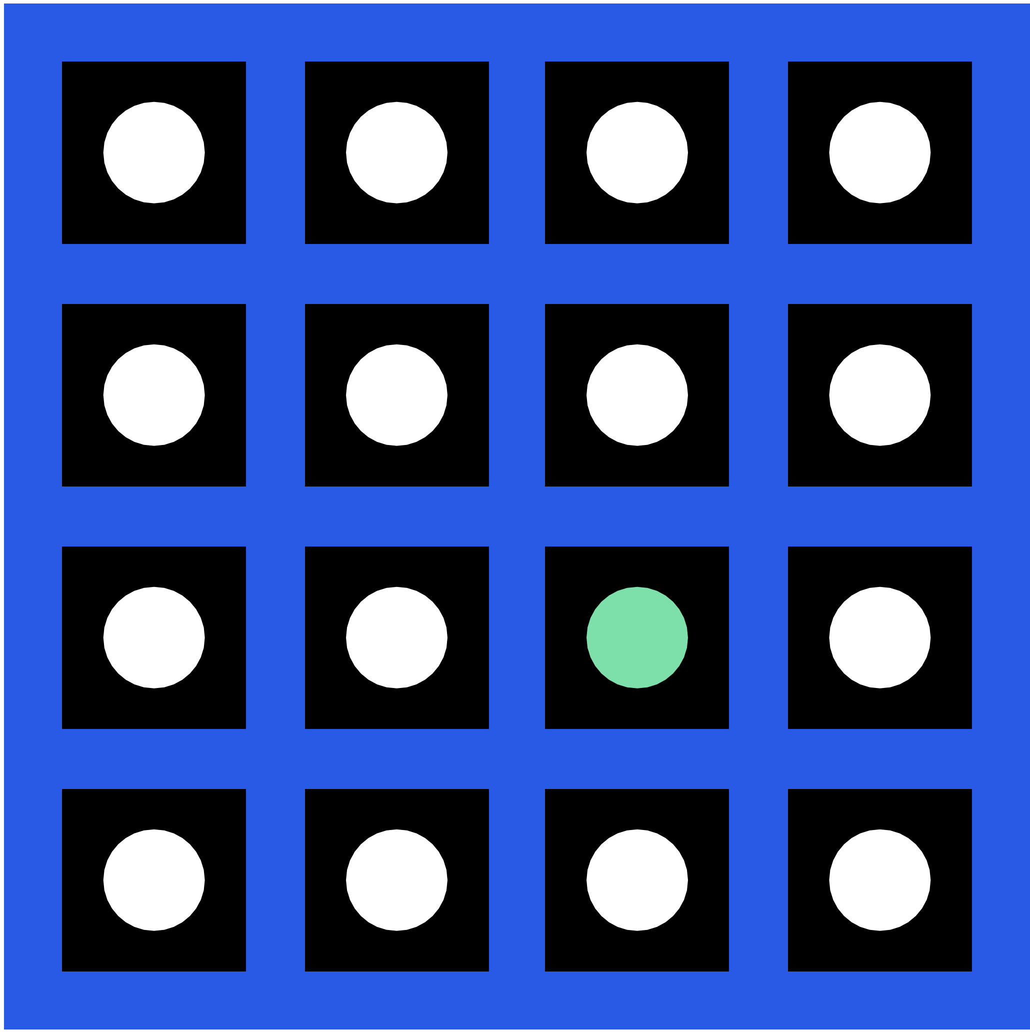
imperva

SALES GUIDE

Imperva Application Security

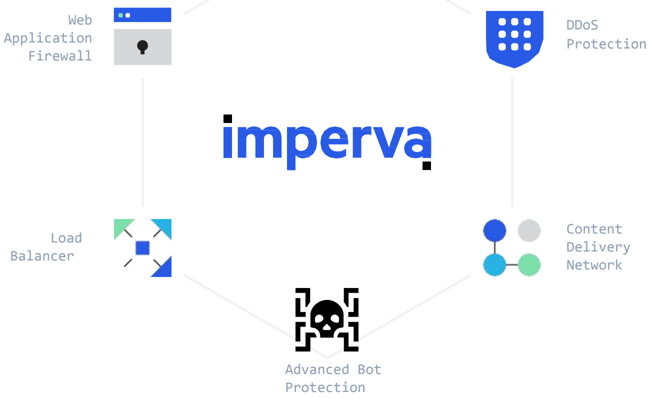
Trusted by over 3 million websites and the world’s most recognized brands, the Imperva application security solution is designed to deliver end-to-end visibility, protection, and edge services at scale.



Elevator pitch

Imperva's core competency is application security—as a consistent leader in Gartner's WAF Magic Quadrant, we know how to help customers secure web applications from threats dominating the IT landscape today.

With a complete solution for both on-prem and cloud-based WAF, plus DDoS protection, advanced bot protection, CDN, and load balancing, we make it simple for customers to keep applications available and secure. For customers who are migrating towards DevOps, our products support the ability to programmatically configure and manage policies through APIs, ensuring that security does not become a bottleneck and can keep up with the speed of app development. Our products support some of the most popular cloud platforms today such as AWS, Azure, and Google Cloud Platform (GCP). When it comes to packaging, we offer licensing for customers to mix and match products within a single contract, allowing customers to bundle on-prem and cloud security assets and eliminate the need to track multiple contracts.



Imperva Application Security covers the full range of web attacks.

- Secures websites against attack—on-prem and in the cloud
- Eliminates downtime due to DDoS attacks
- Maintains always on-availability
- Delivers a speedy web experience
- Protects against account takeover and advanced bot attacks, API threats

Why Imperva Application Security wins.

- API support for core features, easy to deploy
- Security-focused approach
- Advanced Bot Protection with proven accuracy
- RASP, Attack Analytics
- Virtually no false positives to degrade performance
- Integrated with AWS, Azure, and Google Cloud
- Leadership in both multiple Forrester Waves across application security solutions and Gartner Magic Quadrant for WAF

What is Imperva Application Security

Today, attackers can come from anywhere and attack anything: mobile apps, websites, open APIs, microservices and more. Imperva Application Security makes cloud workloads, including applications and websites, always performant, always secure and always available, even while under attack. Imperva App Sec solutions work together to provide easy-to-implement, cost-effective protection that enables digital transformation by accelerating and protecting your move to the cloud.

Web Application Firewall A leader in Gartner's MQ for six years in a row, Imperva's WAF secures websites against known and emerging threats including SQL injections, remote file injections, cross site scripting and more. It's pre-tuned to immediately block, with zero false positives

Advanced Bot Protection Imperva combats automated attacks from scrapers, spammers, and other malicious bots, without ever interfering with legitimate human users, and also detects attempts to perform account takeover via credential stuffing.

DDoS Protection Imperva sets the standard for DDoS Protection: a portfolio of services to protect against the largest targeted attacks on networks, applications and DNS servers. Available for an entire Class C network as well as for individual IPs in public cloud instances. Our solution mitigates DDoS attacks instantly, offers a better end user experience, and is simple to activate and use.

Load Balancer Imperva offers a cloud-based load balancer which supports local and global server load balancing across on-premises and public cloud data centers. It supports automatic failover to standby servers to enable high-availability and disaster recovery without any TTL-related (Time to Live) delays.

API Security Imperva automatically generates a positive security model from OpenAPI specification file, immediately enforcing the relevant policy with regard to what traffic is allowed to pass through.

RASP Imperva Runtime Application Self-Protection sits inside the app to protect against both known and zero-day vulnerabilities. It's security by default.

Attack Analytics Imperva correlates and distills thousands of security events into a few readable security narratives, AI and machine learning simplifies app security event investigations, enabling IT organizations to mitigate and respond to real threats quickly and decisively.

Global CDN Imperva offers a global CDN that uses advanced caching and optimization techniques to improve connection and response speeds. We're the only ones to integrate security and delivery rules. Dynamic Profiling means faster load time: performance with built-in security.

Identifying Prospects

CRITICAL WEBSITE	Is your customer's website critical to their business?	Imperva Application Security is best suited for customers with business-critical websites, especially if they can quantify how much business is lost per minute of downtime or how much of their web traffic is bots. If the business is also complaining about problems to the website, including increased fraud inside online accounts or worsening conversion rates, they are a good candidate especially for advanced bot protection.
CLOUD MIGRATION	Is your customer planning a migration to the cloud?	When customers are planning a cloud migration, the opportunity to take a fresh look at their environment often reveals WAF requirements that were not previously apparent (i.e. quick migration of security policies to the cloud, rule tuning by in-house experts and automatic propagation of new security rules in blocking mode).
DDOS ATTACK	Is your customer prepared for a DDoS attack?	Vulnerability to DDoS attacks can go unnoticed because the responsibility for web access and content is held by the NOC or operations team rather than the security team.

Who To Engage

Application security is typically owned by the *website operations* or network operations team. However, for DevOps-oriented audiences, much of the influence in the buying process can also come from *app developer teams* as well. Because Imperva Application Security can integrate security processes through API automation within the DevOps toolchain, while at the same time improve app performance by eliminating security problems and accelerating content delivery, the security team is a key champion for pushing Imperva Application Security. A typical approach is to pursue initial discovery with the web ops or NOC team, then to bring potential security gaps to the attention of the *security team*.

Most security teams are not aware of whether or not DDoS protection is in place for the network.

- Pursue initial discovery with the web ops, security or NOC team
- Use discovery questions to identify security concerns
- Identify the key members of the security team
- Bring potential security gaps to light
- Bring the teams together to evaluate Imperva application security

Discovery Questions

Is your website critical to your business?

A multi-million dollar company with a website that is merely a 'brochure' is not a good candidate for Imperva app security because—despite their size—they don't transact business on their website. Imperva Application Security is ideal for businesses that depend on their websites to generate revenue.

How quickly do you need to be able to launch new environments?

For any company that is transitioning to a cloud environment, or already cloud-ready, this is a key operational question to evaluate what they need from their security solution. Imperva licensing is typically a competitive differentiator for us when dealing with hybrid cloud.

Competitors often require customers to purchase separate licensing and contracts to manage cloud-based and on-premises security assets, making the transition difficult.

Are you moving applications to the cloud?

Cloud migration is on everyone's mind. An impending cloud migration project offers an excellent opportunity to review the customer's environment and check for missing pieces, such as a web application firewall.

How much time are you putting into learning how to secure your app?

Imperva's patented profiling technology allows us to dynamically learn the app to make custom rules that accommodate new software versions. This ensures your WAF constantly 'self-tunes' to save time and overhead on security operations and allows staff to keep up with the pace of app development.

What would happen to your business if hit with a sustained DDoS attack? What kind of bot problems are you currently experiencing, with bots constantly scraping prices and content, and engaging in account takeover?

Organizations that are sensitive to downtime are very aware and concerned about DDoS attacks, even if the prospect is not able to calculate the cost of downtime. And, every industry has a bot problem, whether it's competitors scraping web content to get an advantage, or credential stuffing using stolen credentials from data breaches.

Following a DDoS attack, which area of your business would take the largest financial hit?

Driving home the specific business impact of a DDoS attack can uncover sensitivity to downtime, even if the prospect hadn't originally identified this as a concern.

Competitive Landscape

Competitive solutions fall into one of three categories: Basic (cheaper) cloud-based services like Cloudflare, the customer's ISP, and enterprise WAF / bot / DDoS vendors like Akamai and F5/Silverline. When you look at comprehensive solutions that include DDoS Protection, API Security, Advanced Bot Protection, RASP and actionable analytics, the competition pales in comparison.

Akamai

Imperva Application Security beats Akamai **Kona** and **Prolexic** in terms of technology and often beats Akamai in price. It can be difficult to persuade a customer to switch from Akamai once it is entrenched in their infrastructure, however. But if your customer is approaching the end of an Akamai contract, a head-to-head POC is the perfect way to swing the conversation toward Imperva App Security. Attack Analytics is also a differentiator for actionable intelligence and subsequent time savings. And, for bot protection, Imperva is proven to be more effective than Akamai **Bot Manager**, blocking a far greater percentage of bots. Akamai is much more expensive, and requires multiple products to achieve what Imperva can do with one. Also, Akamai cannot protect from request zero.

F5

Imperva Application Security beats F5 Silverline on cloud-first technology. As a hybrid solution, F5 **Silverline** depends on an F5 appliance on-premisesvwhich is expensive to maintain and cumbersome to update. Imperva's cloud approach manages large DDoS attacks, keeping them off your customer's network while increasing web performance. F5's **Advanced WAF** solution is also limited in its internal threat intelligence, whereas Imperva pulls from a combination of multiple sources, including threat research from Imperva Threat Research Labs and crowdsourced intelligence. F5's acquisition of **Shape Security** also means it is still a newer player in the bot market, with less time to perfect its bot identification capabilities. Shape Security is only a Contender in the 2020 Forrester New Wave for Bot Management, while Imperva is a Leader.

Cloudflare

Imperva beats Cloudflare on efficacy, technology and breadth of offering. If your customer is price-conscious, Cloudflare may be an appealing option to them them. If they are security and performance conscious, however, we offer better DDoS protection and infrastructure protection in addition to better uptime. Cloudflare is limited in its ability to mitigate Layer 7 DDoS attacks without business disruption. Cloudflare has also remained only a Challenger in the last two Forrester Waves for Bot Management in 2018 and 2020, not progressing in its capabilities and efficacy.

What's In It For Me

Fast track to recurring revenue

Imperva Application Security is quick to sell, quick to deploy and creates a recurring revenue stream. Fast onboarding makes it quick and easy to demonstrate its value to your customers.

Gartner Magic Quadrant

FORRESTER WAVE LEADER 2020

LEADER IDC ANALYZE THE FUTURE

Provides Complete Investment Protection

FlexProtect is a flexible approach to securing applications. A single license offers you the ability to deploy Imperva Application Security how and when you need it. FlexProtect for Applications allows customers the flexibility to adapt their security without regard to infrastructure. You're protected regardless of the number, location or type of devices or services used. FlexProtect helps you protect apps wherever you deploy them - in the cloud, on-premises or as a hybrid model.

Sell with confidence

Imperva is a leader in the IDC DDoS Marketscape (2019), as well as the Forrester Wave for DDoS Mitigation Solutions (2015, 2016, and the latest report published in 2017), the Forrester Wave for Bot Management (2018), the Forrester New Wave for Runtime Application Self-Protection (2018), and the Gartner Magic Quadrant for Web Application Firewalls (2014, 2015, 2016, 2017, 2018, 2019).

Protecting data and all paths to it.

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

+1 (866) 926-4678
imperva.com

imperva