

# Imperva Application Security for Healthcare

---

## Protection that keeps EHR/EMR applications running securely

EHR Applications have become mission-critical for healthcare organizations looking to drive positive patient outcomes. They help facilitate patient reach and can act as the primary interface for all aspects of patient care. These applications require protection from security threats, just like any other web application. Regulations like HITECH make for a tough balancing act between being open to sharing PHI and mitigating the risk of a data breach.

To meet this need, Imperva Application Security empowers healthcare organizations to easily protect their applications while providing an optimal and secure user experience. Imperva also makes security vendor consolidation and management simplicity a reality, with application security components offered as part of an integrated solution set.

---

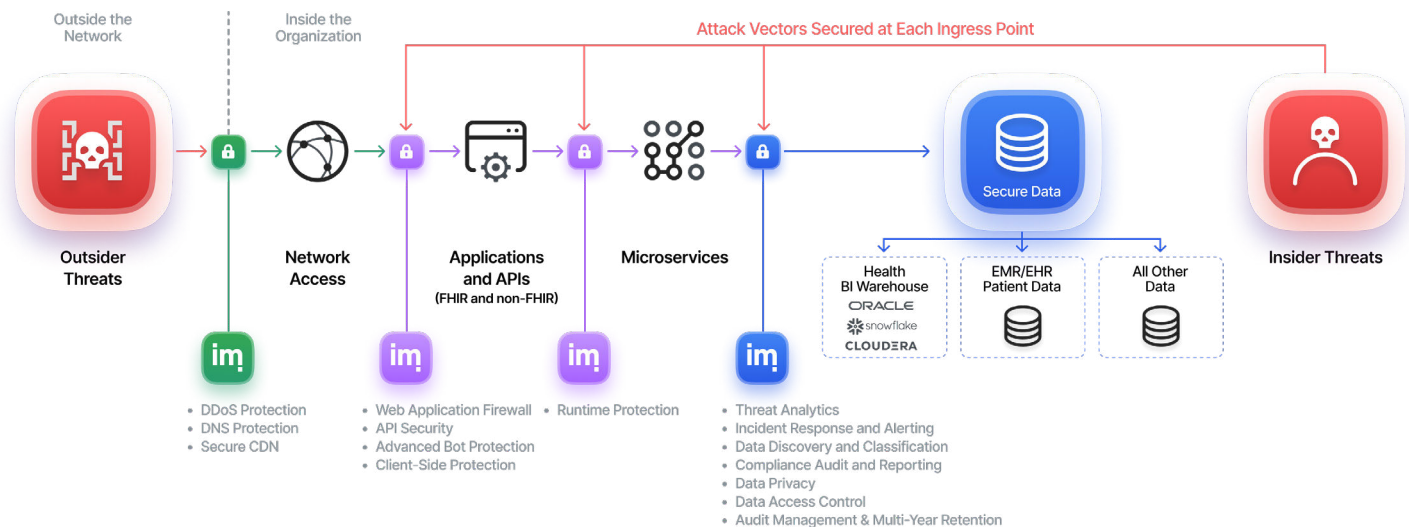
## Secure your critical healthcare applications

Imperva deploys an integrated single-stack platform which provides an optimal, layered approach to enforcing security from the application to the end user. As an industry leader for Web Application Firewalls and API Protection (WAAP), Imperva provides WAF solutions (cloud-based Cloud WAF and on-premises or virtual appliance WAF Gateway) to defend against all OWASP Top 10 threats including SQL injection, cross-site scripting, illegal resource access, and remote file inclusion.

### KEY CAPABILITIES

- AI and machine learning uncover and act on key critical security incidents
- Secure against OWASP Top 10 threats across cloud and on-premises WAF deployments
- Mitigate potentially devastating DDoS attacks before they reach your applications
- Accelerate web content delivery ensuring users have a consistent, optimal experience
- Support faster application release cycles while ensuring application protection during runtime
- Ensure high availability even when under attack from malicious bots and DDoS attacks

Policies and rules are kept up-to-date for your WAF and API Security based on live intelligence from security experts at our Imperva Research Labs. In addition to your localized security settings, inspection and enforcement of all user traffic occurs across our global network of PoPs and each of our PoPs has its own DDoS scrubbing center, which further helps to reduce malicious traffic.



## Act on critical insights

With today's complex and evolving threat landscape, it's more important than ever to gain visibility across your PHI data and applications. An onslaught of security alerts can prevent organizations from discovering critical attacks that pose an imminent threat. Attack Analytics, a key part of Imperva Application Security, addresses alert fatigue by distilling millions of security alerts into a prioritized set of insights. These insights include recommended actions for identifying cyber risk, improving your security posture, and for mitigating threats before they impact patient care.

## Avoid disruption to patient care

Motivated cybercriminals wage disruption campaigns against healthcare organizations every day and utilize vast bot networks to wage devastating attacks. Organizations without proper protection from malicious bots and Distributed Denial of Service (DDoS) attacks are exposed to a wide range of risks, including users experiencing slowed or denied access to healthcare applications. This has implications for providers, patients, and anyone involved in patient care including 3rd parties.

Imperva Application Security provides powerful DDoS Protection and Advanced Bot Protection to eliminate attacks long before malicious traffic has a chance to reach a customer's website. Multiple DDoS protection services are available, with always-on protection for websites, DNS servers, and individual IPs, and always-on or on-demand protection for networks. With near-zero latency and backed by a 3-second Service Level Agreement (SLA), malicious traffic is mitigated without disruption to legitimate traffic.

With Imperva Advanced Bot Protection, fingerprinting and client classification categorizes whether traffic is coming from a human, a good bot, or a bad bot. Classification is performed quickly and with an extremely low false positive rate, protecting against business-logic attacks on websites, APIs, and mobile apps and preventing Account Takeover (ATO) attacks.

Imperva API Security uses deep discovery and classification of sensitive data to provide continuous protection of all APIs. It does so by detecting all public, private and shadow APIs, including APIs in use by EHR applications, 3rd party services and applications used by healthcare providers and patients.

In addition to providing clarity on where sensitive PHI is traveling and being accessed, Imperva API Security actively guards against attempts to steal patient data from any vulnerable FHIR APIs.

## Ensure a secure and responsive user experience

Healthcare organizations depend upon EHR systems to provide premium care and deliver positive patient outcomes. Meeting user demands of these systems requires that web applications and infrastructure deliver web content quickly and securely. With a global network of PoPs, Imperva is able to optimize website content delivery by serving content from a PoP located nearest the end user.

Imperva's application-aware CDN dynamically profiles your website, identifying all cacheable content (dynamic and static) to enable accelerated content delivery. Profiling and frequency analysis ensures the most often accessed resources are detected and served directly from memory, enabling website optimization, delivering improved performance, and lowering bandwidth costs.

## KEY BENEFITS

Imperva safeguards cloud and on-premise applications by:

- Providing a complete WAAP solution
- Delivering actionable security insights
- Protecting against DDoS attacks
- Mitigating malicious botnet attacks
- Blocking cyberattacks that target APIs
- Enabling RASP protection
- Ensuring optimal Content delivery

Learn more about Imperva Application Security and our Healthcare solutions at [www.imperva.com](http://www.imperva.com)

Or call +1.866.926.4678 to speak with a customer support representative.