Solution Brief

Imperva Solutions for MHS Genesis

thalestct.com

THALES
Building a future we can all trust

THALES

The Military Health System's MHS Genesis electronic health record system manages and stores personal health information (PHI) for service members, veterans, and their families. MHS Genesis is a complex system composed of front-end web-based applications supported by backend services and databases. Such a system requires robust application and database security.

Electronic Health Record (EHR) systems provide a unique challenge for cyber security practitioners. The most sensitive personal data is maintained on systems that are accessed from all over the globe while executing workloads in multiple on premises data centers and multiple cloud vendor environments. To secure such system effectively requires solutions that enable flexible deployment options in complex environments.

Thales Trusted Cyber Technologies (TCT) and Imperva enable healthcare customers to secure their most sensitive applications and data with Imperva's Application and Database security solutions.

Protecting all paths to healthcare data

Imperva Data Security Fabric

Imperva Data Security Fabric from Thales TCT enables agencies to secure databases from those running bare metal in on premises data centers to intricate virtualized and/or containerized environments in complex multi-cloud deployments. Data is secured where it resides.

Imperva Data Security Fabric allows organizations to meet compliance and authorization requirements by providing security controls, separation of duties, long term retention of audit records, reporting of details of data access while providing actionable insights to react to improper/malicious access of the most sensitive of data.

Imperva Application Security

Applications, services and their respective APIs are effectively clients for accessing data. Therefore, to protect data it is necessary to protect the applications accessing such data. Since applications are continually updated and improved, their attack surface continually changes, thus the application protection needs to adapt accordingly. From front-end web application firewall to API security to the last line of defense—runtime protection, Imperva Application Security from Thales TCT ensures that applications are accessing sensitive data in a manner that has not been maliciously tampered with. Protecting complex and ever changing front-end systems of EHR solutions requires the tried and tested capabilities of Imperva Web Application Firewall (WAF) dynamic profiling, API discovery and zero day protection of Imperva Runtime Application Security Protection (RASP).

End-to-End Security for MHS Genesis Imperva Solutions with Application and Data Security

By combining Imperva's Application Security solutions with Imperva's Data Security Fabric, MHS can ensure that its patient's data is secured end-to-end.

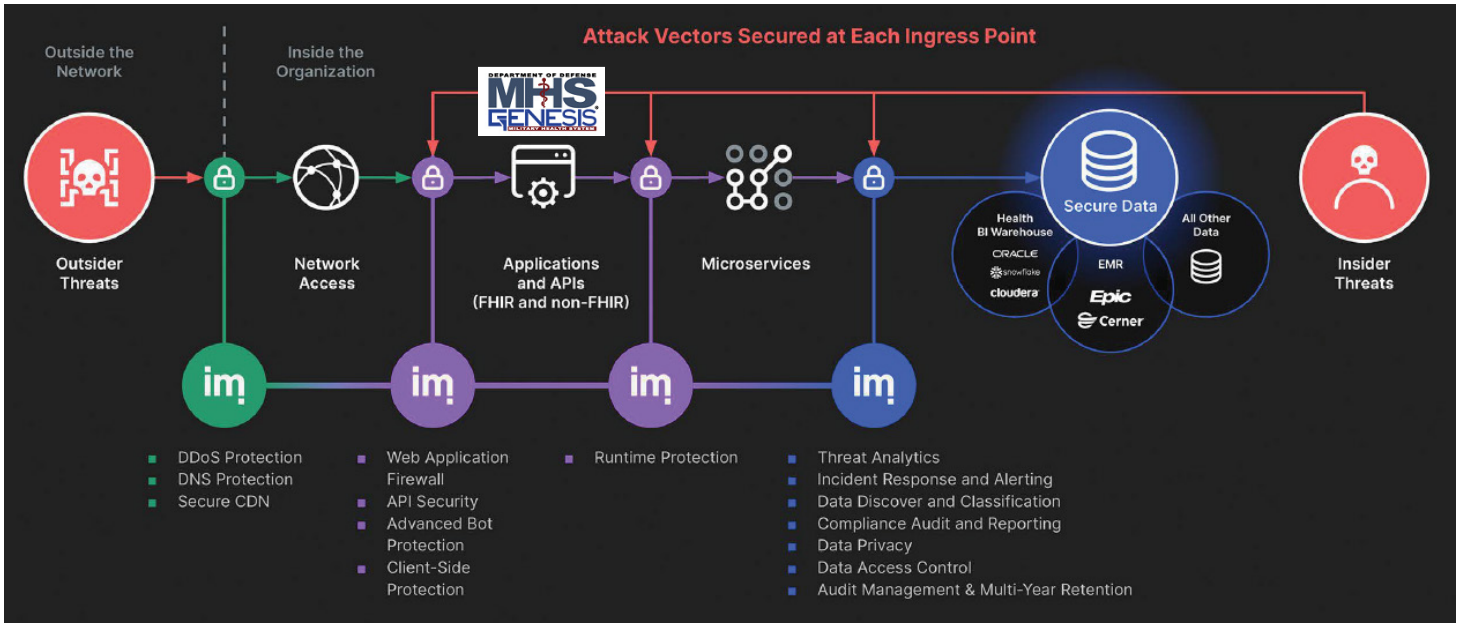
Imperva Solution Summary:

Application Security

- Web Application Firewall (WAF). Font-end protection for MHS Genesis.
- API Security. Protection for backend services that use APIs.
- Runtime Protection. Application protection against zero-day attacks and third-party library vulnerabilities.

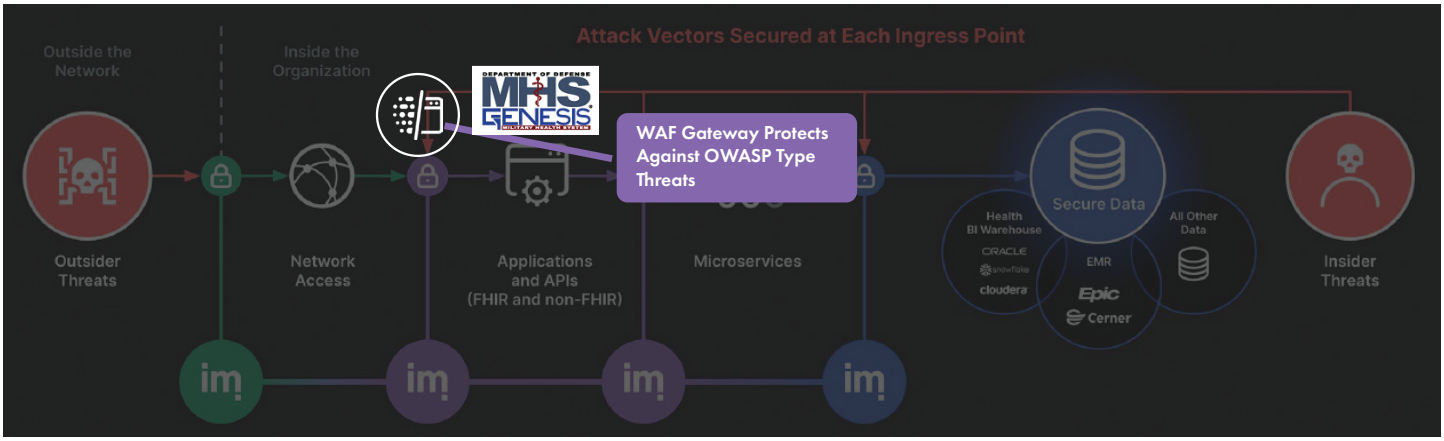
Data Security Fabric (DSF)

- Database Activity Monitoring (auditing and alerts). Determine who is accessing what data.
- Data Risk Analytics. Analyze what data access is questionable, anomalous, or dangerous
- Discover and Classify. Enumerate specifically where sensitive data resides (database, table, column, etc.).
- Database Vulnerability Assessment. Assess databases in accordance with DISA STIGs, CIS Benchmarks and dozens of Imperva Benchmarks.
- User Rights Management. Determining if user privileges are appropriate.
- Compliance Reporting/Retention. Automate and simplify regulatory compliance activities with superior long-term retention of live audit data.
- Incident Mitigation. Integrate with SOAR systems to mitigate incidents.



Web Application Firewall (WAF) Gateway

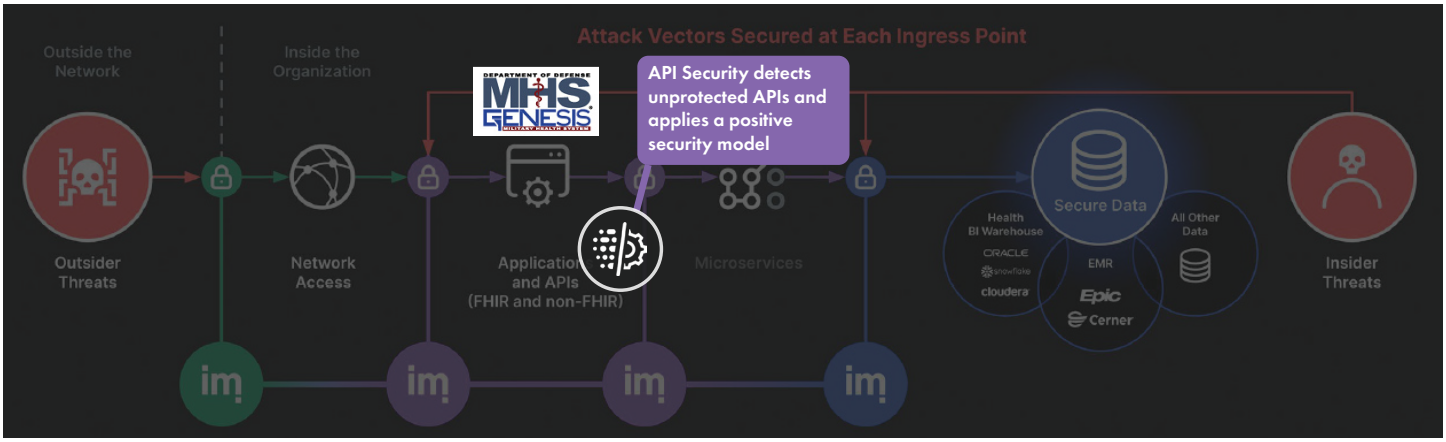
Imperva's WAF provides out-of-the-box security for web applications. It detects and prevents cyber threats, including OWASP Top Ten, ensuring seamless operations and peace of mind.



Imperva API Security

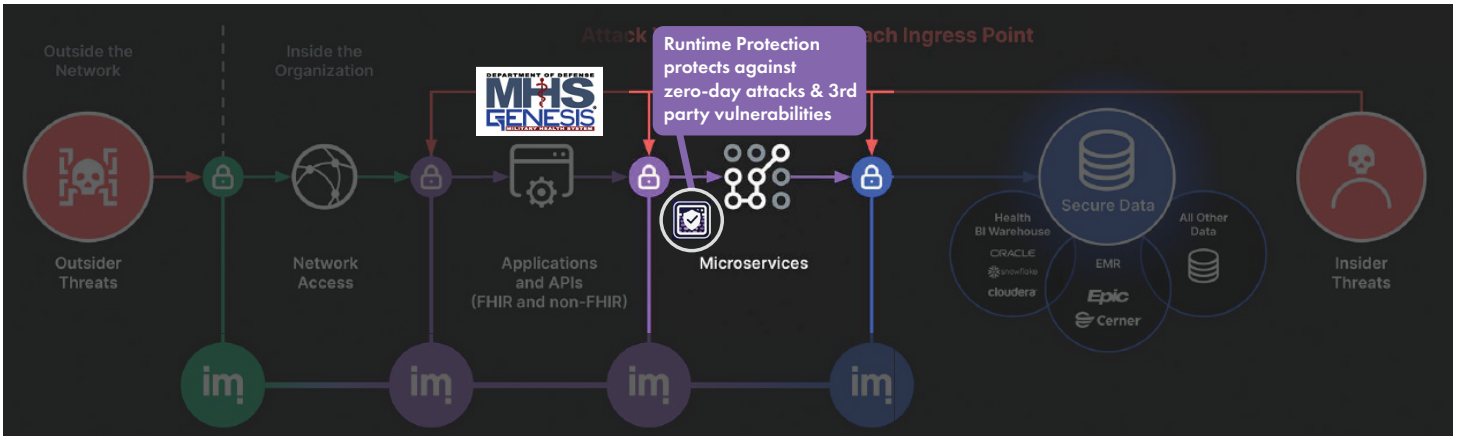
Imperva API Security provides continuous protection of all APIs using deep discovery and classification to detect all public, private and shadow APIs—helping security organizations devlope a complete inventory of the APIs they are charged with protecting. It also protects against business logic attacks and many more of the OWASP API Top Ten threats.

API Security Anywhere works in on-premises, containerized and cloud environments detecting insecure APIs as well as sensitive data that may be exposed within the application architecture. The easy-to-deploy solution empowers security teams to implement a positive API security model.



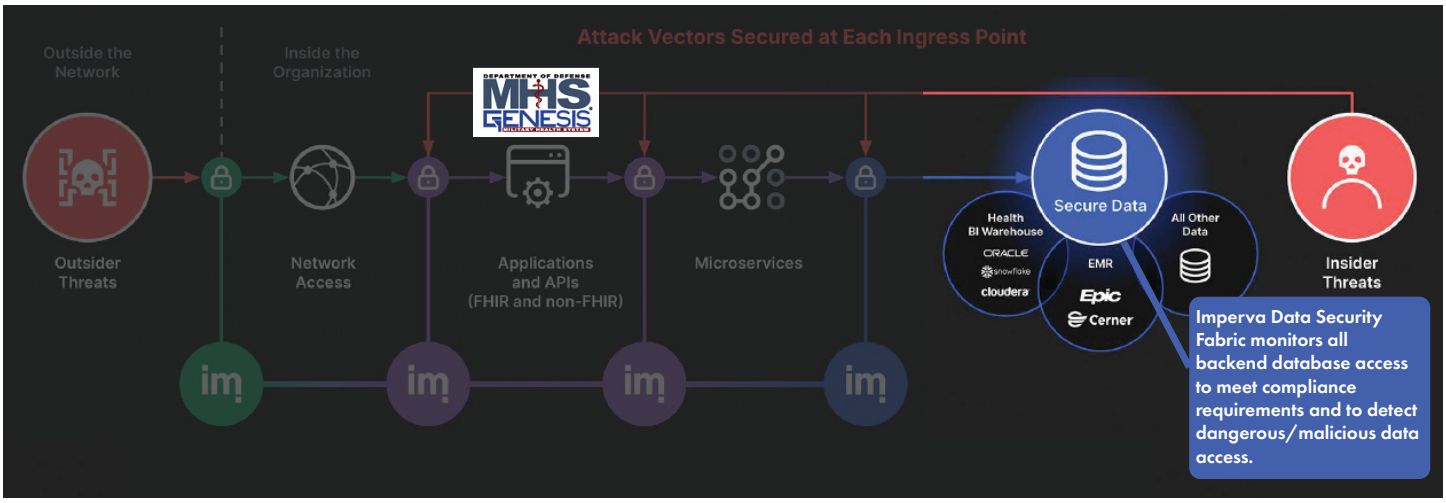
Imperva Runtime Protection (RASP)

Imperva Runtime Protection (also known as RASP) is the last line of application defense. Imperva Runtime Protection uses Language Theoretic Security (LANGSEC) to detect and neutralize known and zero-day attacks, ensuring applications are secure by default. It requires no code changes or external communication and works in Java, .NET/.NET Core, Node.js and Python environments. With Imperva Runtime Protection, agencies can identify vulnerabilities, patch them on their schedule, and maintain optimal performance.



Imperva Data Security Fabric

Imperva Data Security Fabric provides the most complete database security solution available. Working with over 70 database solutions, Data Security Fabric provides detailed visibility and insights into how data is being accessed in an environment. Audits, alerts and behavioral analytics detect and alert on suspicious/dangerous database access and provide a detailed narrative understanding for threat hunters within Security Operations Centers (SOC). Continuous monitoring requirements for Authorizations to Operate (ATO), Data Security Fabric performs automated/scheduled vulnerability scans on databases in on-premises and cloud environments.



About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com