Overview

Imperva Data Security Fabric

Overview

thalestct.com

THALES
Building a future we can all trust

THALES

Establish unified data-centric security controls enterprise-wide, to protect against data breaches, automate compliance, and accelerate audits

Today's competitive economy requires organizations to fully leverage their data to gain efficiencies and improve customer experiences. To protect your data, and your agency, you need a data-centric security and compliance solution that uses explicit data risk controls.

A better way to protect data assets

Traditional end-point and perimeter-based security are not enough to protect valuable data. The proof is in the news every day, with yet another high-profile data breach incident.

Organizations need more than built-in logging of traditional data platforms - you can't be compliant without separating duties of data management from data auditing - and encryption and data access controls are useless if the attacker has circumvented or stolen account credentials.

Imperva Data Security Fabric (DSF) protects your organization from data breaches and compliance incidents by augmenting traditional enterprise security approaches with controls for the data itself, to drive policy-compliant data handling behavior, and help security staff pinpoint and mitigate data threats before they become damaging events.

The Imperva Data Security Fabric Difference

Broadest coverage

Provides broadest coverage across multicloud, hybrid, and on-premises environments

Protect any data source

Protects any data sources and types, across structured, semi-structured, and unstructured data stores

Ecosystem integration

Integrates with ecosystem technologies for incident context and additional data capabilities

Unifies visibility

Unifies visibility, control, automation, and insights via a single data service or dashboard

Key Value Drivers

SECURITY & IT PROFESSIONALS

Data Security, anywhere

Pursue business innovation, while protecting all data across the data estate. Imperva DSF significantly reduces data risk inherent in an ever-increasing attack surface.

CLOUD ARCHITECTS

Evolve data security for multicloud expansion

Unify visibility, control, automation, and insights across clouds. Know where data from public, private and third-party cloud services is and how it is being used.

EXECUTIVES AND COMPLIANCE OFFICERS

Data security compliance at scale

Ensure compliance in highly-regulated industries across hybrid and multicloud environments at any scale.

TECHNICAL END USERS

Data discovery and classification

Know where sensitive data is stored, who is accessing it and if there are any unusual behaviors or unauthorized activity

Unify Data Security Visibility and Control

Rapid technology change, overloaded staff, and always urgent timelines make it almost impossible to solve enterprise-wide data security and compliance challenges on your own. Many security and compliance teams lack the resources, and sometimes knowledge, to protect every aspect of a modern hybrid data environment spanning on-premises and cloud data platforms. However, if you use the right tools, you can fill those gaps.

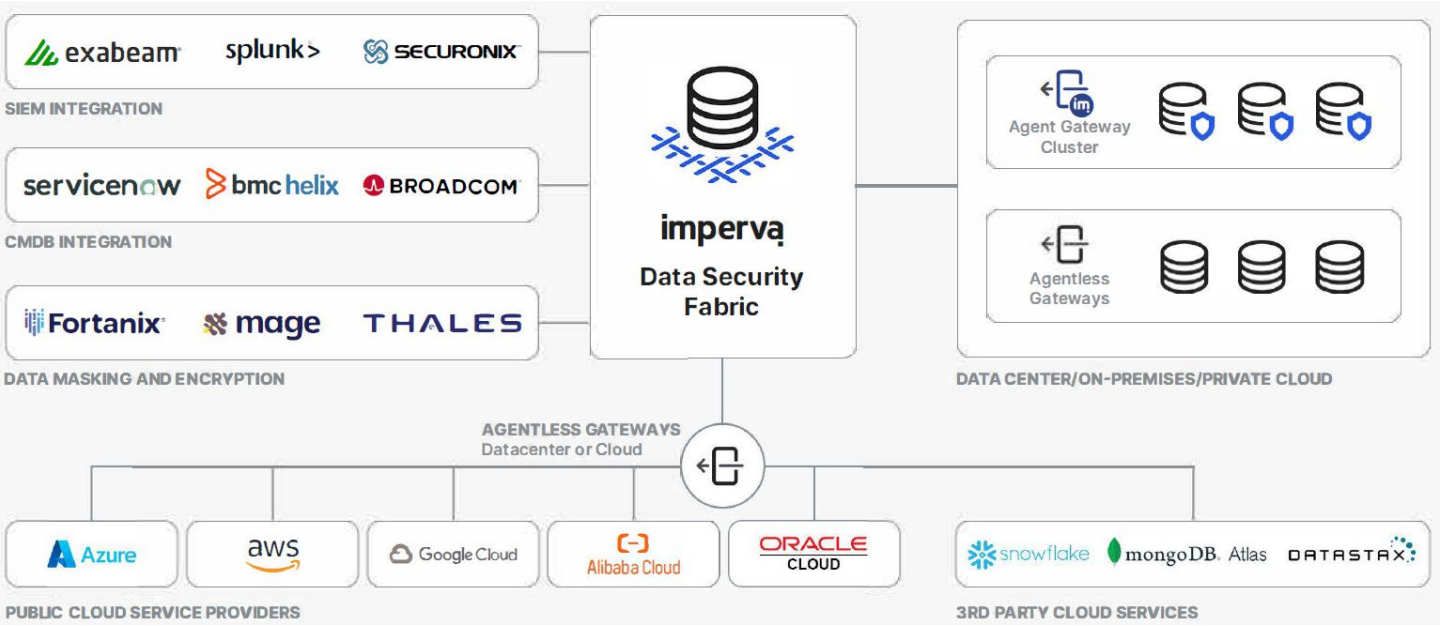
Organizations need Imperva DSF so that they can implement consistent security and compliance best practice procedures that can scale enterprise-wide. Imperva DSF enables your team to get more done without adding headcount, in less time, with better outcomes.

Imperva DSF combines automated security and compliance capabilities into a single technology solution, which eliminates tedious manual labor and removes the complexity of trying to manage a disjointed set of data security tools for data oversight. Through a single dashboard, you can manage data discovery and classification, data activity monitoring, data risk analytics, and threat detection, additional options for data loss prevention, data access control and data masking, plus provide instant audit and compliance reporting.

Cover and scale hybrid cloud environments

Through Imperva DSF you can standardize data security controls across large and complex enterprise data environments so you have full visibility and centralized command of what is happening across all of your file stores and data assets, on-premises, in the hybrid cloud and across multiple clouds.

Imperva's flexible architecture supports a broad range of data repositories, from legacy mainframe systems to modern big data systems and cloud-managed database services, and everything in between. Imperva DSF enables you to migrate your data to the cloud without creating compliance and security gaps - ensuring a safe digital transformation.



Data Security, Anywhere

Imperva DSF provides a comprehensive and unified view of enterprise data risks across both structured and unstructured data management systems - meaning your security policies are applied consistently everywhere.

Structured data support includes traditional databases, mainframes, data warehouses, and databases hosted in Microsoft Azure, Amazon Web Services (AWS), Google Cloud, and more -including Managed Database Services such as Azure SQL and Amazon Relational Database Services (RDS).

Imperva DSF will also discover and classify semi-structured and unstructured data formats for Microsoft Office Documents, PDFs and other commonly used data types on-premises in network file shares, in big data systems, cloud data lakes, or cloud data repositories. such as AWS S3 buckets, OneDrive, Azure blobs, or Google Drive for Google Workspace.

Proactive and predictive analytics

Imperva DSF helps organizations reduce breach risk from internal threats such as careless mistakes or malicious insiders, as well as outsider cyber attacks. Imperva assessment capabilities help mitigate risks of data attacks by scanning data repositories with over 1,500 pre-defined vulnerability tests based on CVEs, and CIS and DISA STIG benchmarks to keep your data protected from the latest known threats.

With Imperva DSF in place, you gain a clearer understanding of who is accessing what data and what they did with it. Auditor and analyst queries can be answered quickly and with precision.

Simplify Compliance and Reduce Costs

Imperva DSF streamlines data-related compliance processes for assigning policy controls, enforcing separation of duties, retaining audit records, archiving, and reporting by removing the manual labor and providing easy access through interactive tools. Tasks that formerly required days to complete can be executed in minutes, saving time, shortening audit cycles, and significantly reducing compliance overhead costs.

Compliant data made easy

Many compliance regulations such as Payment Card Industry Data Security Standard (PCI DSS), Federal Information Security Management Act (FISMA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX) have specific provisions focused on data protection requirements.

>500,000
critical databases under protection

1,500
file formats, data types, and cloud assets

200
data repositories with 100% coverage

Imperva DSF continuously locates regulated data, tracks who has access, and audits what they are doing so you can easily document that data is appropriately protected and used as required.

Automated, policy-based data retention

Imperva DSF automates audit record storage and archiving by allowing you to define audit data retention policy, deduplicating and compressing the information in ratios up to 10x, at thousands of events per second per core so you can cost-efficiently collect and retain everything in one place to meet any multi-year retention requirement or policy.
This significantly reduces manual labor. Information is consolidated across all audited data assets, fully indexed, and efficiently stored so that you have years worth of information at your fingertips should you need to retrieve it later.

In addition, the platform allows you to utilize any cost-effective underlying storage infrastructure you already own, both on-prem resources such as a Storage Area Network (SAN), or cloud services such as AWS S3 and Glacier or Azure blobs for further cost avoidance.

Long-term, live audit data access

With Impera DSF, years worth of retained records are instantly accessible for detailed search and investigation. Audit data is archived automatically, as time passes, but remains accessible in seconds for queries and reporting. Built-in interactive dashboards and on-demand Kibana visualization tools deliver easy to understand results. Integrations with 3rd-party data analytics tools provide additional options so that any audit data stakeholder in the organization can use their favored search, reporting, or data mining tools such as Tableau.

Streamlined reporting

Templatized reports for data-related audit requirements of major compliance regulations such as SOX, PCI, NYDFS, HIPAA, GDPR and others are available out of the box. An interactive console allows you to build new reports on-demand or to customize reports. The high-performance foundation of Imperva DSF will deliver your report information in minutes instead of the days it often takes to compile large documentation tasks with manual processes.

Avoid Data Breaches

With Imperva DSF providing centralized data-centric data protection, by discovering, classifying, assessing, monitoring, and constantly analyzing security threats, you are equipped and enabled to stay on top of the ever changing threat landscape. Imperva DSF enables your data protection to keep pace with changing data infrastructure that can open the door to data attacks.

Data discovery and classification

In a dynamic environment many organizations don't actually know where all of their sensitive data is and whether it is exposed. Such blind spots establish conditions where something as simple as an employee mistake could lead to data leaks, and create security risks that attackers can exploit. Imperva DSF automatically discovers databases with sensitive data on file shares, data repositories, or in the cloud. In the process it automatically classifies the data using a number of techniques, including dictionary, pattern-matching and cross reference against other data, or you can create your own categories, so you can determine data sensitive levels and the right controls to mitigate risks.

Data activity monitoring and predictive data risk analytics

Many data incidents are the result of mistakes or poor security practices, such as password sharing, and a staggering percentage of successful data breaches come from privileged insider activity and stolen user credentials.

To mitigate these ever-present data threats, organizations need to continuously validate what users are doing with data and be instantly notified if that data access activity is improper, whether deliberate or by mistake.

> "Our organization performed an internal exercise that led to a simulated database breach. Before Imperva, it took over three weeks after this activity completed to product a holistic picture of the impacted application database environment, let alone the remediation steps required to mitigate future scenarios. It was a laborious and time-intensive process. If that was a real-life breach, a three-week turnaround time would be unacceptable. We needed to collapse that into the same day and reduce all the manual work involved stitching the pieces together." Lead Cybersecurity Engineer

Imperva DSF monitors and continuously analyzes all data access activity by both database user accounts and privileged user accounts and can automatically determine if a data access event violates a compliance or security policy. In addition, Imperva data risk analytics utilize machine learning and unique detection techniques developed by Imperva Labs to spot known attack exploits or suspicious activity even if the behavior attempts to be evasive. Imperva DSF goes beyond the anomaly detection techniques of other security products. We use purpose-built algorithms capable of identifying signs of malicious insider behavior such as privilege escalation, data exfiltration, or compromised user account activity that other security tools miss.

Imperva data risk analytics leverage Imperva discovery and classification features to always consider the risk context of data access, filter out false positive noise produced by other anomaly-based behavioral analytics, and only report issues involving sensitive data or when a critical event has happened.

Advanced analytics detect even evasive attack behavior that may indicate insider abuse or compromised accounts

Automated workflow and process orchestration

Built-in Imperva DSF incident workflow processes turn days of incident management work into minutes. These include reporting signs offs, entitlement review, and change request reconciliation which direct incident management actions to stakeholders ensuring nothing is missed.

Integrations with other mission-critical security and management tools enable automated orchestration between systems. For example, a critical incident flagged by Imperva analytics could trigger what is called a playbook, that automatically deactivates the user account in the database, assigning a critical incident ticket to a security analyst in their SOC workflow manager for investigation.

Embed data security into your enterprise security ecosystem

Imperva DSF provides over 260 built-in integrations with other widely used enterprise security infrastructure systems - including traditional SIEM solutions, Splunk, CMDB tools, Enterprise SOAR, Web Application Firewalls, and more.

For Splunk users, Imperva DSF provides a unique integration that allows them to take advantage of high-value audit and security information already stored in place on the Imperva platform, using Splunk dashboards and workflow. Imperva will deliver pre-processed contextual information about data-specific security events to Splunk - saving the organization significant time and avoiding Splunk indexing costs, staff manual labor costs, custom development costs, and potentially licensing fees.

Proactive risk assessments and mitigation

To help manage data access risks, Imperva DSF user rights assessment capabilities that provide you with a comprehensive report of user access entitlements to the sensitive data types you have discovered and classified. Additional risk mitigation, including that from privileged users, comes from a combination of previously mentioned separation of duties along with the continuous monitoring of data access. Built-in data system authentication and access control are powerless against these threats, because in all cases the credentials are valid, they are just being improperly used or the data is mishandled.

Data masking and data encryption

Secure your sensitive data, at scale, without the need for any complex configurations or application code changes, Imperva provides seamless integrations with modern data masking and data encryption tools for heightened security that clients, employees, and suppliers need to maintain confidence in your organization.

These tools can securely de-identify or encrypt your sensitive data in non- production and pre-production environments using advanced data transformation algorithms to mitigate the risk of a data breach, and demonstrate compliance to global data privacy regulations.

Summary

These are just a few of the capabilities Imperva Data Security Fabric brings to customers. Data-centric security is a key component of the Imperva solution - helping you constantly detect emerging threats across all of your enterprise data - through automated procedures that simplify and standardize data protection, auditing, and compliance across your entire enterprise data environment. The combination of data protection, cost reduction, and improved staff effectiveness benefits that Imperva DSF delivers helps to future proof and enhance the ROI of security programs.

Imperva provides a variety of licensing options for securing data enterprise-wide so that you're protected regardless of the number, location, or type of devices or services used, protecting your data wherever it lives - in the cloud, on-premises, or in hybrid configurations. Thousands of customers around the world trust Imperva to protect their data, applications, and websites. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey.

Imperva Research Labs and the global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into its solutions.

Imperva DSF is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

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

Contact us - For office location and contact information, please visit thalestct.com/contact-us