Product Brief

Imperva

Data Security Fabric

thalestct.com

THALES
Building a future we can all trust

THALES

Avoid data breaches, simplify compliance and accelerate audits with a unified platform for data-centric security

Imperva Data Security Fabric (DSF) protects your data 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.

A unifying approach to data protection

Whether consolidating multiple data security tools, or upgrading from an outdated legacy solution, federal agencies can now take advantage of capabilities available in one modern, unified data-centric security solution.

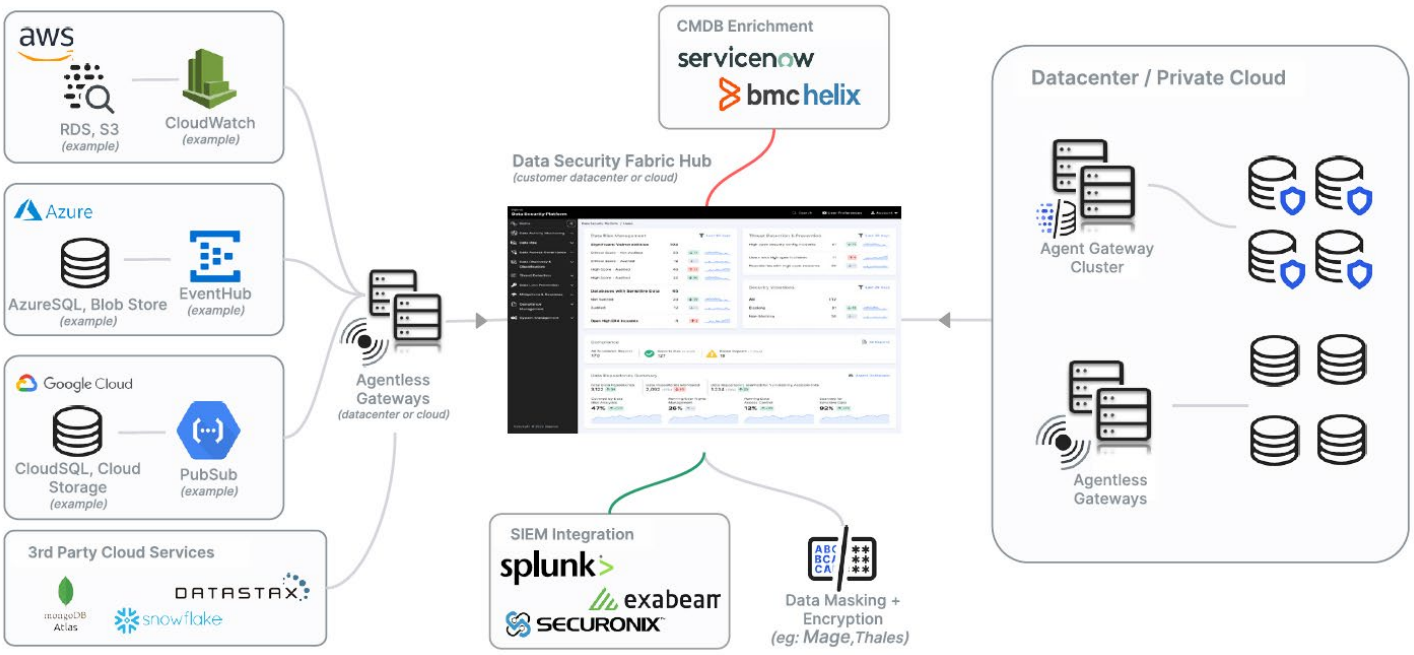
Imperva DSF provides proactive controls and predictive analytics so that security analysts and governance staff can leverage capabilities for activity monitoring, security assessments, risk modeling and attack detection to avoid damaging data breaches or compliance failure.

For example, Imperva DSF identifies behavior that violates data use policy, and its advanced risk analytics detect indicators of malicious insider activity or compromised user accounts that can evade data repository access controls and circumvent data encryption.

In unifying data security, Imperva Data Security Fabric simplifies the operational complexity of deploying disparate security tools to mitigate data security threats. Automated workflows, and integrations with other enterprise security management infrastructure tools ensure that staff can resolve incidents quicker.

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

Imperva Data Security Fabric Architecture



Imperva Data Security Fabric protects data across hybrid enterprise environments and integrates with your existing enterprise security infrastructure

Key Benefits

Imperva Data Security Fabric eliminates blind spots for security and governance teams by providing visibility to how sensitive data is stored, shared, and used - even in the cloud. It also unifies security controls enterprise wide, and protects both structured and unstructured data, including privacy related personal data.

Imperva Data Security Fabric boosts overloaded security and compliance staff efficiency by automating data security and compliance tasks that had previously been done manually, such as reporting and incident management. Imperva customers gain immediate value by getting more done, without adding headcount, in less time, with better outcomes.

Imperva Data Security Fabric improves how security teams and governance stakeholders work together across departments, by integrating with other enterprise ecosystem tools such as Splunk and ServiceNow, to accelerate audits, incident investigation and remediation.

This combination of visibility, control, automation, and integration significantly reduces compliance costs, improves security staff effectiveness, and helps to future-proof and enhance the overall ROI of security programs.

Imperva Data Security Fabric Integrations

Imperva Data Security Fabric provides over 260 built-in integrations with widely used enterprise data repositories and security ecosystem solutions such as SIEM tools, and CMDB tools. Imperva Data Security Fabric also works seamlessly with cloud infrastructure from AWS, Azure, Google and others, plus traditional on-premises infrastructure from network and storage vendors

Technology Integrations		
Databases and NoSQL platforms	Oracle, Microsoft SQL, IBM DB2, SAP HANA, Teradata, Hadoop, MongoDB, Cassandra, Aerospike, Couchbase and dozens of others.	
Cloud managed services and warehouses	IaaS platforms such as AWS EC2, Microsoft Azure, Google Cloud Platform, Oracle Cloud as well as managed database services such as AWS RDS, DynamoDB and Redshift, Microsoft Azure SQL, Synapse and CosmosDB, Teradata Ventage, Snowflake and more	
Unstructured data repositories	Shared Network Files Sharepoint Email (through archives) Windows Network Drives (SMB) File Folders (mounted drives) Linux Network Drives (SMB/SSH) MacOS Network Drives (SMB/SSH)	Cloud Files AWS S3 OneDrive Office 365 Mail Azure Blob and Azure file shares Google Drive for Google Workspace Gmail for Google Workspace
Identity Management, Access Management, and Authentication	Microsoft AD, Azure AD, Ping Identity, Oracle, Cyberark, AWS, Hashicorp, plus federated credentials using LDAP. ODBC w/Kerberos, and SSH w/Kerberos	
Data Masking and CMDB	Mage, ServiceNOW, BMC Helix	
SIEM formats	Syslog, Rsyslog, Splunk, Exabeam and others	

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