Solution Brief

Bring Data Protection to DevOps

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

DevOps teams leverage cloud computing to scale solutions within development, testing, and production environments. Securing the DevOps environment is critical to the success of digital transformation projects. In an atmosphere of continuous improvement and delivery, there is a high need to integrate security flexibly into digital products and services to support an ongoing stream of new features, fixes and technologies. DevOps face challenges to both security and DevOps velocity as they work within existing constraints to handle unknown threats. 58% of DTR respondents[1] in APAC prioritized DevOps and cloud as their greatest emerging security concerns.

[1] 2024 DTR Report – APAC Edition

Challenges to protect sensitive data in the DevOps lifecycle

DevOps want data security to be simple and to fit within their environment—solutions that deploy easily in the cloud and are highly monitorable so DevOps can adapt to changing conditions.

CI/CD pipelines include the automated Continuous Integration (CI) practice performed as Developers are writing code, and the automated Continuous Delivery (CD) practice performed after the code is completed.

- **Scalability and Operational complexity**
  In a dynamic infrastructure, scaling security policies effectively while maintaining compliance with regulations, such as GDPR or PCI DSS, becomes a critical concern.
  DevOps workflows rely heavily on automation, visibility and monitoring tools to inform their choices as they manage CI/CD pipelines—incorporating data security can complicate processes, requiring careful handling to avoid disruptions in CI/CD pipelines. Testing environments also need to be secured with data security tactics to pseudonymize data to ensure the use of realistic but protected data.
- **Latency**
  Adding data security introduces latency – impacting application performance across the network, which can be a concern in real-time, high-throughput environments.
- **Impact to Development Schedules**
  Learning cryptography, and keeping track of updates in cryptography standards, modifying source code and testing the revised code increases the risk of introducing errors and adds to the development schedule.

How Thales Can Help

To overcome DevOps lifecycle challenges, it is critical to have developer-friendly security solutions that integrate easily into DevOps environments. The right data security solutions, designed for modern DevOps environments, enable developers to proactively define and implement controls to maximize security, manage throughput rates and easily push solutions to production.

Solutions that are easy to deploy, monitor, and offer visibility and observability increase infrastructure efficiency and decrease costs. When you see that traffic has increased significantly and you want to shield throughput rates, you can easily spin up another instance. If things are getting quiet, you can terminate the instances that are no longer needed.

Thales has data security built for every role in the DevSecOps pipeline and for each layer of the technology stack to match your security requirements and infrastructure. Where you embed security is your choice.

Three CipherTrust solutions that protect application data and participate with your DevOps pipeline are:

- CipherTrust Application Data Protection (CADP)
- CipherTrust RESTful Data Protection (CRDP)
- Data Protection Gateway (DPG)
- CADP is on the CI side because it is an SDK. CRDP and DPG are on the CD side because they are more traditional orchestration and deployment pieces. Developer involvement is limited to initial coding and integration, Data Security Admins pick up responsibility for making security updates, and Operations involvement is decreased significantly.
- CADP is a performant SDK that is embedded in the application server. CADP is compiled into an application — if the application is in the cloud, then CADP is in the cloud. CADP is available in variants for Java, .NET Core and C. Wrappers can be added to connect the SDK to higher level languages such as Python or GoLang to protect data on behalf of any application or service. CADP is used when performance is the top priority. CADP will be faster than a REST call because the SDK does not have to go across the network to get the data.
- CRDP is a solution for REST behind the API service. CRDP works with any development language and any type of application, and protects data on behalf of any application or service. CRDP is used when sensitive data is received by an application and the data needs to be protected inside the application, and you choose to use a REST API.

- DPG protects data for REST API-based applications transparently without making any changes to the application. DPG works with any development language in a REST environment and protects data in line with RESTful web services and microservices. Intercepts REST calls, protects data and sends the data forward. DPG doesn't need to be aware of the application code or the database schema, it protects the data in the JSON payload shared on the REST API. DPG is used when sensitive data is received by a RESTful web service or microservice and the data is inline. No code change. One CipherTrust solution that protects application data but does not participate in the DevOps pipeline is:

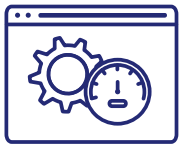
- **CipherTrust Batch Data Transformation (BDT)** BDT performs secure data migration and scheduled transformations between data in the clear and Tokenization or Encryption. BDT can be attached directly to a database or to a server. Unlike CADP, CRDP and DPG, BDT does not participate in the DevOps pipeline because BDT transforms data independent of your application. BDT is used for initial transformation, scheduled data transfers, and key rotations for applications that do not natively support key rotation.

Decrease Dev Involvement

Enhance digital sovereignty with full control over the location of your data and who can access it

Increase Security

Give control to Security with Separation of Duties



Cloud-native Deployment

Enable observability -containerized, orchestratable, monitorable and visible

Align with the dynamic needs of DevOps teams

CRDP and DPG are cloud-native, enabling rapid changes, frequent deployments, and flexible scaling. Crypto agility for data protection makes it painless to update ciphers, parameters and keys.

1. **API-Driven:** Using CipherTrust Manager (CM) APIs, you can create and manage policies and keys to integrate security directly into CI/CD workflows, enabling seamless automation and integration with tools like Jenkins, Kubernetes, and Terraform.

2. **Cloud Native Support:** CRDP and DPG are optimized for cloud architectures. They are containerized solutions purpose-built to work in the cloud and can be deployed and scaled easily across cloud or hybrid infrastructure.

3. **CI/CD Automation & Orchestration:** CRDP and DPG support a "shift-left" approach for security: cloud native, and they participate in orchestration and all liveness and readiness probes. DevOps teams can fully automate encryption, tokenization, key management, and policy enforcement. This approach enables continuous integration and delivery with robust security, without compromising CI/CD speed.

4. **Crypto agility for Data Protection:** Data Security Admins make a selection from a dropdown menu on CipherTrust Manager to update ciphers, parameters and keys. CRDP and DPG pull the updates from CipherTrust Manager and no changes are required to the customer applications, so no Dev involvement is required beyond the initial coding and integration. Vulnerability gaps are reduced from months to less than a minute.

DevOps teams and organizations can benefit from implementing a consistent and centralized data security approach with CipherTrust RESTful Data Protection and/or Data Protection Gateway.

See CipherTrust RESTful Data Protection in action; check out our GitHub repository:

- Get the code: End-to-end demo with Google Big Query
- Get the code: Test the CRDP API via a client

ESG Statement

The CipherTrust Platform supports ESG initiatives by securing sensitive data, reducing cyber risk, ensuring regulatory compliance, and enabling sustainable digital transformation through efficient, scalable, and environmentally responsible data protection solutions for modern enterprises.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us