Crucible

Simplifying Platforms, Amplifying Innovation

What is Crucible?

Simplify software development, deployment, and management for government programs by rapidly building security compliant applications in any cloud.

Supports Multiple Clouds

Works with any cloud provider, offering ultimate flexibility and compatibility

Rapid Infrastructure Automation

Save time and resources while enhancing environment versatility by rapidly deploying or redeploying mission infrastructure.

Security Compliance

Expedites a program's security compliance and ATO with 95% DISA STIG

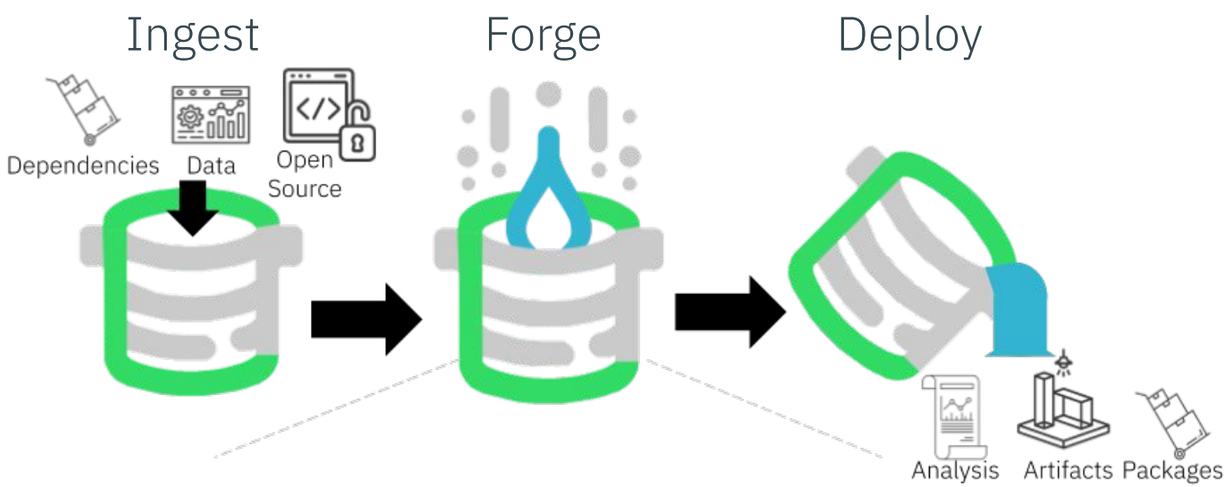
Mission Use Cases

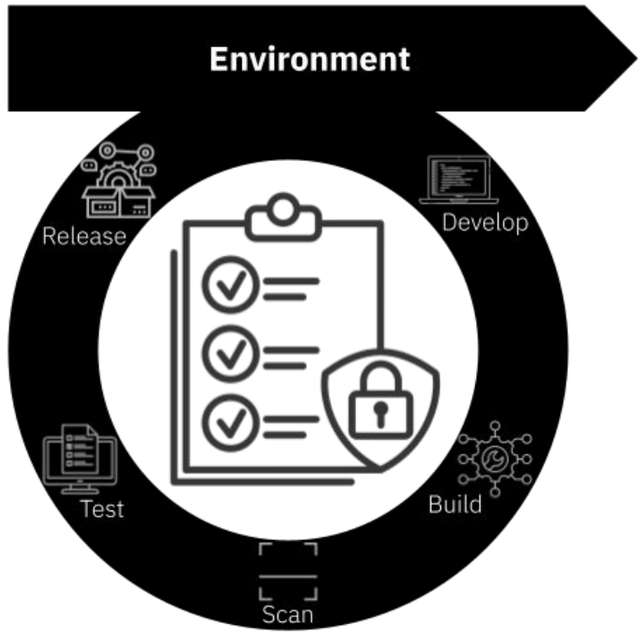
Leverage any cloud for efficient and secure software management. Our solution delivers a comprehensive suite of DevSecOps capabilities, customized to meet specific mission requirements:

1. Develop secure applications within protected environments
2. Maintain secure operational baselines
3. Implement CI/CD pipelines for streamlined production across all classification levels

Customer Environments

Crucible integrates seamlessly into any environment—unclassified, classified, or hybrid—supporting Develop, Build, Scan, Test, and Release processes while enabling centralized management without infrastructure changes, streamlining operations, and boosting productivity.

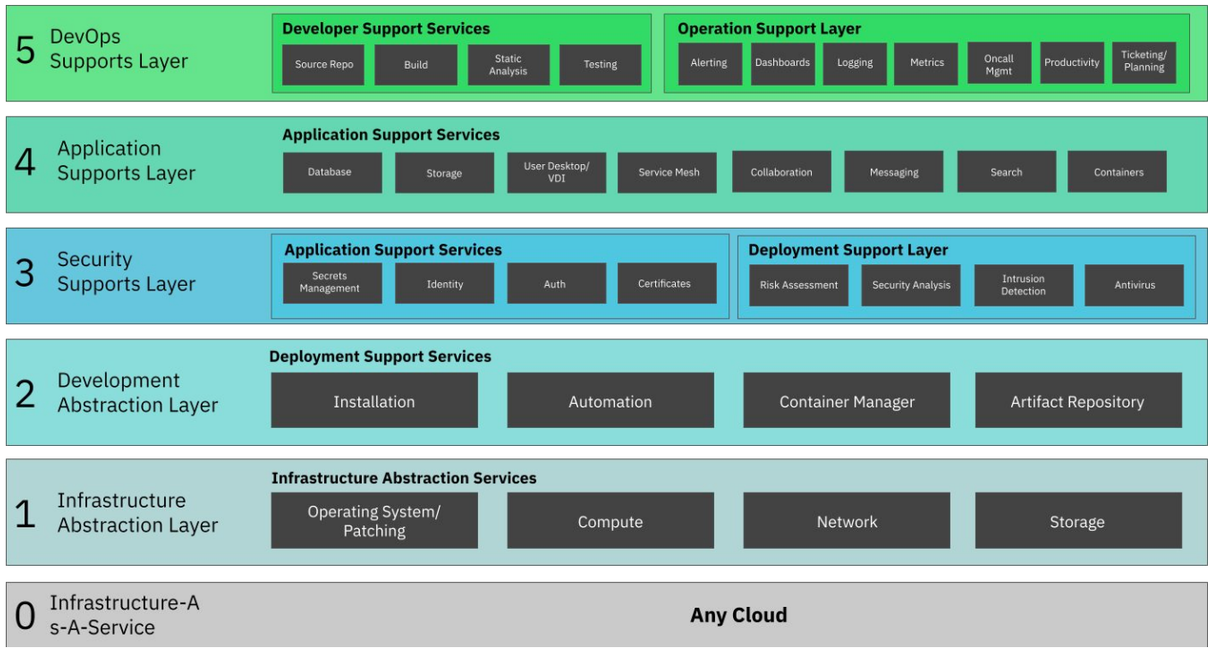




Services + Tools

The Crucible platform is divided into five distinct layers each providing services while remaining cloud agnostic.

Crucible Services



1. **Infrastructure Abstraction Layer:** Interfaces with underlying infrastructure, ensuring consistent service deployment across any cloud.
2. **Deployment Layer:** Manages CI/CD pipelines, artifacts, and containers for scalable and flexible deployments
3. **Security Layer:** Speeds up authorization with application security (IdAM) and deployment monitoring (risk and incident detection)
4. **Application Support Layer:** Provides data storage, secure communication, database, persistent storage, service mesh, messaging bus, search, and container services.
5. **DevOps Support Layer:**
   - Developer Support: Source code repositories, build, test, and cyber scanning services for rapid, secure capability deployment.
   - Operations Support: Includes system monitoring, debugging, and issue tracking.

Support Models

BS | Basic Support Model - Onboarding program accesses baseline Crucible artifact repository maintained by the DIDO Solutions Crucible Team and customer manages own Crucible instances.

CS | Core Support Model - Onboarding program accesses customized Crucible artifact repository maintained by the DIDO Solutions Crucible Team, and customer manages own Crucible instances with remote support from the Crucible Team.

PS | Premier Support Model - The DIDO Solutions Crucible team is integrated with the customer onboarding program to manage customized Crucible artifacts and Crucible instances.

Crucible Onboarding Process

	BS	CS	PS
Crucible Team supplies user technical requirements document to Program	1	1	1
Crucible Team conducts technical exchange meeting with Program	2	2	2
Crucible Team prepares tenant design and cost estimates	3	3	3
Program provisions tenant space	4	4	4
Crucible Team builds Crucible release and delivers required Crucible artifacts	5	5	5
Program* deploys Crucible in program tenant space	6	6	
Program* onboards users	7	7	
Program* conducts post deployment configuration of services (with program System Administrators)	8	8	
Program* assists with deployment of application	9		
Program* supports setup and configuration of CI/CD pipelines	10		
Program* supports Risk Management framework	11		
Program* provides ongoing Operations, Maintenance, and Support	12		

Get in touch

Start your secure DevSecOps journey today: **support@didosolutions.com**