# Crucible

## ZERO TRUST INFRASTRUCTURE-AS-CODE

## SUMMARY

Crucible automates environment provisioning and application deployment as infrastructure-as-code, embedding Zero Trust principles—never trust, always verify—across on-premises and multi-cloud environments. Policy enforcement, versioned playbooks, and audit trails drastically reduce attack surfaces and configuration drift.

## ZERO TRUST FOUNDATIONS & KEY CHALLENGES

Zero Trust requires continuous verification, least-privilege access, and segmentation of infrastructure into minimal trust zones. Operations need telemetry, Just-In-Time (JIT) and Just-Enough-Access (JEA) controls, and immutable baselines to prevent drift and misconfigurations.


### Infrastructure as Code

- Versioned Playbooks
- Immutable Images

### Fine-Grained Access Controls

- Just-In-Time Provisioning
- Least-Privilege Enforcement

### Microsegmentation

- Automated Network Policies
- Dynamic Port Management

### Continuous Verification

- Vulnerability Scanning
- Audit Trails

### Automated Updates

- Policy-Driven Patching
- Configuration as Code

## BUSINESS BENEFITS

- Shrinks attack surfaces with immutable deployments and microsegmentation.
- Cuts downtime with automated rollback and JIT access.
- Makes audits easy with built-in compliance reporting.
- Speeds up delivery by embedding security into every pipeline.

## CONCLUSION

Crucible operationalizes Zero Trust at scale—codifying provisioning, enforcing least privilege, segmenting workloads, and continuously verifying changes—to simplify security, accelerate compliance, and strengthen resilience.

## Get In Touch

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