

Tools and DevOps Support to Move Faster

Access senior DevOps support whenever you need it — [get your quote](#)

Component	Challenges addressed	How it works
Current architecture audit	Outdated architecture, bottlenecks, technical debt	- Analyze existing architecture, identify gaps, and suggest improvements. - Ensure adherence to industry standards and best practices
Containerization	Inconsistent application environments, difficulty in scaling applications, long deployment times.	- Containerize applications using Docker to standardize environments across development, testing, and production. - Set up container orchestration platforms for scalability and reliability (e.g., Kubernetes). - Provide best practices for container security and resource optimization.
CI/CD	Slow release of versions, manual deployment errors, inconsistent environments.	- Design and implement CI/CD pipelines for automated builds, testing, and deployments. - Configure pipeline triggers for code changes and integrate with testing frameworks.
Advanced CI/CD Pipelines	Complex workflows, lack of integrated testing, and manual intervention in releases.	- Build advanced CI/CD pipelines with integrated testing, canary releases, and blue/green deployments. - Automate deployment rollback in case of failures.
Observability and Advanced Monitoring	Lack of deep visibility into application and infrastructure health.	- Implement distributed tracing, log aggregation, and advanced alerting mechanisms. - Set up visualization dashboards for real-time insights.
Performance Optimization	Slow application performance, unoptimized infrastructure leading to resource contention.	- Identify performance bottlenecks in applications and infrastructure. - Optimize infrastructure and implement caching mechanisms where necessary.
Incident Management and SRE Practices	Long recovery times during incidents, lack of structured incident response.	- Implement incident management practices, such as runbooks and on-call rotations. - Set up Service Level Objectives (SLOs) and Service Level Agreements (SLAs).
Disaster Recovery	Lack of failover mechanisms, high recovery time in case of system failures.	- Set up backup and disaster recovery (DR) solutions to ensure data and system resilience. - Perform regular DR drills to validate readiness.
Security Audit	Vulnerabilities, lack of security controls, unauthorized access risks.	- Conduct security audits and implement basic security policies.
Cost Optimization	High operational expenses due to overprovisioned resources and unused assets.	- Analyze resource usage and costs, identify inefficiencies, and rightsize resources. - Implement automated scaling and cost management policies.
Support and Maintenance	Operational downtime, outdated infrastructure, insufficient expertise.	- Provide ongoing technical support, system monitoring, and troubleshooting. - Conduct routine updates and patches to keep systems secure and efficient.
VPNs	Unsecured remote access, data interception risks, lack of encrypted communication channels	- Set up secure Virtual Private Networks (VPNs) to enable encrypted remote access. - Configure access control, authentication mechanisms, and traffic routing. - Integrate VPN with identity and access management tools for role-based access.