Blueprint Cloud delivers a highly secure world-class offering with 24/7 monitoring that helps customers save time and money on costly internal IT security infrastructure and maintenance. Zero-effort scalability also allows you to focus on your business, while we take care of your service infrastructure.

Blueprint Cloud is hosted in highly secure, scalable, Tier III-aligned data centers using one of our hosting partners. Hosting infrastructure is load-balanced, highly available, and housed at geographically optimized locations across at least two data centers. Daily database backups are replicated to secondary sites for disaster recovery.

### Services

<table>
<thead>
<tr>
<th>Primary Regions</th>
<th>Secondary Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blueprint</strong></td>
<td><strong>North America - USA - Chicago</strong></td>
</tr>
<tr>
<td>North America - USA - Dallas</td>
<td><strong>Europe - UK - London</strong></td>
</tr>
<tr>
<td>Europe - Ireland - Dublin</td>
<td><strong>North America - USA - Oregon</strong></td>
</tr>
<tr>
<td><strong>Integrations</strong></td>
<td><strong>Europe - Ireland - Dublin</strong></td>
</tr>
<tr>
<td>North America - USA - Northern Virginia</td>
<td><strong>Europe - Ireland - Dublin</strong></td>
</tr>
</tbody>
</table>

### Hosted Integrations

Blueprint integrates with more than 40 ALM tools including JIRA, VersionOne, CA Agile Central, and TFS. Customers can seamlessly push artifacts, such as user stories and tests, from Blueprint to their ALM tools.

Bespoke integration capabilities are available using webhooks and our REST API.
Customer Website Security
Each customer is provisioned with dedicated HTTPS-only sites. Data transmitted between their users and Blueprint Cloud is always encrypted in transit using the TLS 1.2 protocol.

Customer Data Security
Each customer is provisioned with dedicated SQL databases to store their solution data and ensure data segregation. AES-256 encryption is used to encrypt data at rest on disk.

Infrastructure Security
Blueprint Cloud’s servers have security updates applied monthly and are regularly scanned for vulnerabilities. Host-based IDS and IPS technologies are also used to monitor and defend against malicious intrusion attempts. Security events are logged to a centralized event management service for alerting and analysis.

Blueprint Application Authentication
User access and authentication are managed through the built-in secure authentication system. Using granular role-based access controls, customers can customize exactly what actions their users and administrators can perform.

Customers may also use their own authentication systems by leveraging SAML 2.0. The Blueprint application supports both SP and IdP initiation and has been verified to work with ADFS 2.0.

Penetration Testing
Blueprint completes comprehensive, regularly scheduled, and independent full-stack penetration testing.

Data Center Compliance
Blueprint Cloud operates in SOC II Type 2 and ISO 27001 compliant data centers. Compliance documentation can be provided upon request and more information can be found below.

Service Level Agreement (SLA)
Incidents or service requests can be logged by licensees 24x7x365 via the Blueprint Community. Initial response and incident assignment will take place within two hours for Severity 1 incidents related to service availability and normal service operation. Blueprint Cloud provides a monthly 99.5% uptime SLA.

For more details, please see our Cloud Support Terms.