

# Secure *By Design*

---

***Security Measures, Processes and Policies at JourneyApps***



# Secure By Design

---

## Security Measures, Processes and Policies at JourneyApps



Top global industrial companies rely on JourneyApps for innovative solutions to run their businesses. JourneyApps has comprehensive operational security controls and measures in place, keeping our customers' data and intellectual property safe. In addition, JourneyApps has been designed with security at its core, ensuring that every app built on the platform automatically maintains the same high security standards. All our Fortune 500 customers agree — JourneyApps has passed each of their stringent security reviews, allowing them to deploy safe and robust applications that work with sensitive information.

## Protection of **Personal Information, Proprietary Information and Intellectual Property**

The apps built on JourneyApps often contain valuable and sensitive information. We are serious about protecting such sensitive information, whether it is personal information, proprietary information, or intellectual property that is used by, or contained within an app. We continuously work to ensure that our platform is safe, each app on the platform is safe, and that our processes and internal controls are best-in-class. The most important security measures are described in more detail below.

# Available Third-Party Security Reports

While this white paper provides a high-level overview of the security measures and controls used by JourneyApps, the following third-party reports on our security are also available:

	<p><b>Cloud Security Alliance (CSA) Security, Trust &amp; Assurance Registry (STAR)</b></p> <p>Through the CSA STAR program, JourneyApps provides a completed version of the CSA Consensus Assessments Initiative Questionnaire (CAIQ), a comprehensive security assessment framework commonly used by enterprises.</p> <p>The JourneyApps CAIQ is publicly available for download on CSA STAR at the following web address:  <a href="https://cloudsecurityalliance.org/star/registry/journeyapps/">https://cloudsecurityalliance.org/star/registry/journeyapps/</a></p>
	<p><b>Service Organization Controls (SOC) 2 Type 2 Report</b></p> <p>JourneyApps performs annual AICPA Service Organization Control (SOC) 2 audits of our platform, and our latest SOC 2 Type 2 report is available to prospective customers and existing customers on request, subject to the execution of a Non-Disclosure Agreement (NDA).</p> <p>The audit affirms that JourneyApps’ information security practices, policies and procedures meet the Trust Services Principles and Criteria for Security set forth in the SOC 2 standards.</p>
	<p><b>Penetration Test and Vulnerability Assessment Report</b></p> <p>The <b>NCC Group</b> (leading global experts in cyber security and risk mitigation) conduct regular security assessments on JourneyApps. At a minimum, assessments are done annually, as well as when any significant changes to the platform are made.</p> <p>The NCC Group report on the penetration test and vulnerability assessment results regarding JourneyApps is available to prospective customers and existing customers on request, subject to the execution of a Non-Disclosure Agreement (NDA).</p>

# Technological Security Measures in JourneyApps

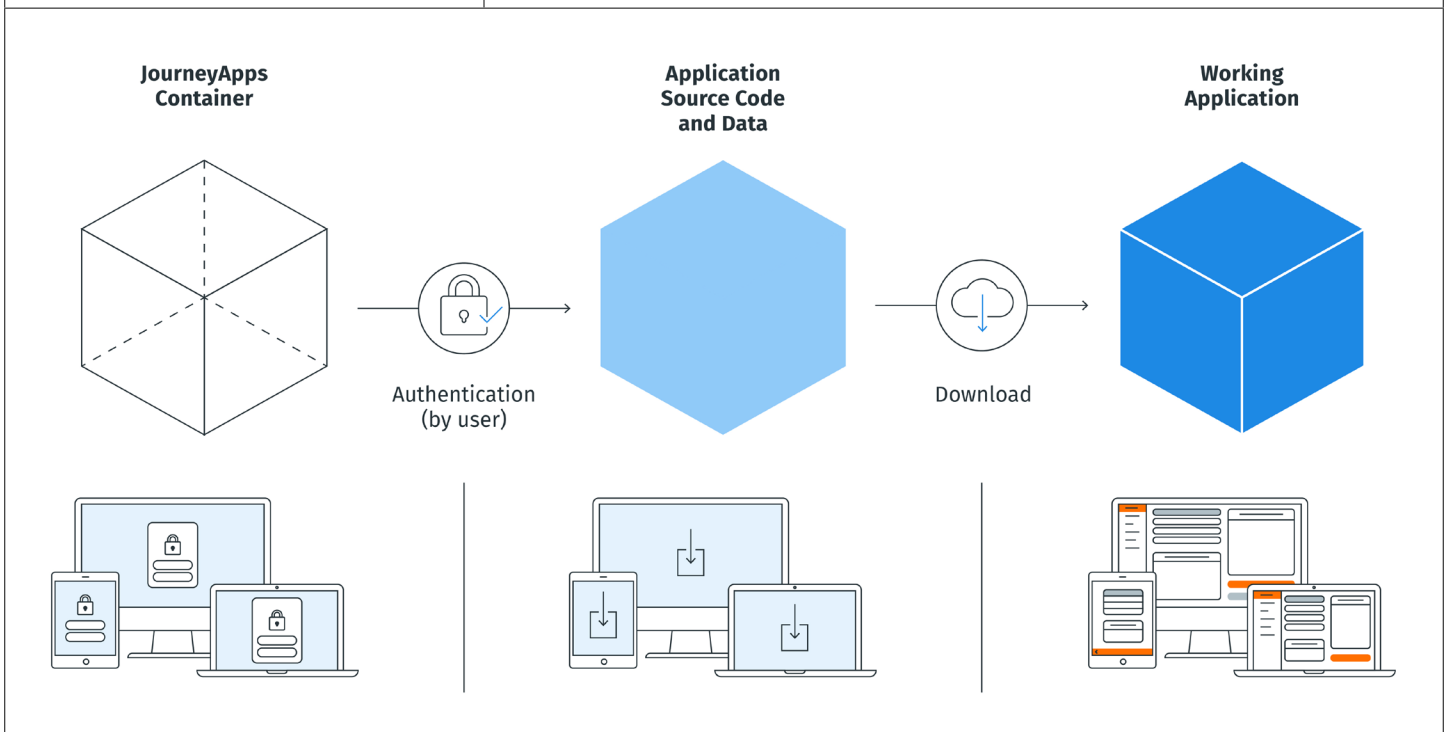
## Platform Architecture

### Applications:

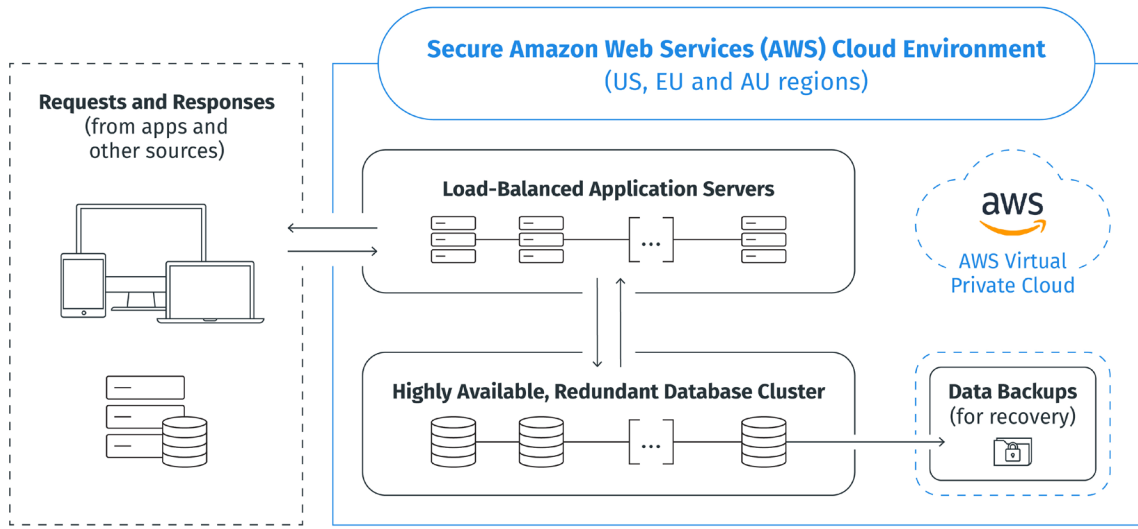
Users install generic “containers” that contain no customer proprietary information. Containers can be distributed via Mobile Device Management (MDM) software or other means. Once users **securely authenticate** in the container, their proprietary custom application and data are downloaded.

*Authentication methods supported: SAML, WS-Federation, JourneyApps Standard, and custom REST authentication.*

*Authentication products supported: Active Directory, Okta, Ping Identity, Auth0, and more.*



<b>Platform Architecture</b> <i>(continued)</i>	<b>Cloud Environment:</b> <ul style="list-style-type: none"> <li>• Application servers and database servers for JourneyApps run in a virtual private network on Amazon Web Services (AWS).</li> <li>• JourneyApps runs on a redundant load balanced cluster which is horizontally scalable and resilient against single points of failure. If any single server fails, there are redundant servers which can take over the load seamlessly. The cluster’s redundancy is further supported by hosting in multiple isolated failure zones.</li> </ul>
--	---



<b>User Management and Permissions</b>	<ul style="list-style-type: none"> <li>• Only authorized users can obtain access to applications or data.</li> <li>• Any user’s access can be revoked, and sensitive application data can be remotely deleted by administrators.</li> <li>• Roles and customized permissions can be assigned to each user.</li> </ul>
<b>Data Encryption</b>	<p>Data is encrypted end-to-end on JourneyApps:</p> <ul style="list-style-type: none"> <li>• <b>At Rest:</b> Data stored in the platform uses block-level encryption (AES-256).</li> <li>• <b>In Transit:</b> Data in transit is encrypted using TLS V1.3.</li> <li>• <b>In Use:</b> Data stored and used in applications are encrypted on the device. On Windows and Android devices, configuration of an application PIN is required for full protection.</li> </ul>
<b>Data Synchronization Rules</b>	<p>JourneyApps supports a powerful set of synchronization rules to allow fine-grained control of data that gets synchronized and stored offline on user devices. Synchronization rules can be customized to meet the exact business requirements of each application.</p>
<b>Source Code Encryption</b>	<p>When required, application source code is encrypted using AES-CBC (256-bit key length) and securely stored on each authenticated user device.</p>

<b>Intrusion Detection and Prevention</b>	JourneyApps makes use of an Intrusion Detection System (IDS), and firewalls with restricted ports. Intrusion Detection & Prevention is within the scope of the SOC 2 Type 2 report which is available from JourneyApps on request.
<b>Infrastructure-Level Security</b>	<p>JourneyApps is hosted on Amazon Web Services (AWS), and as a result, JourneyApps leverages the robust controls that AWS has in place to maintain security and data protection in the cloud. AWS provides various certifications and attestations including SOC 1, SOC 2 and SOC 3, and auditing reports are available for review by customers. Please consult the <a href="#">AWS Cloud Compliance</a> and <a href="#">AWS Cloud Security</a> portals for further information, or contact JourneyApps.</p> <p>JourneyApps makes use of several AWS products to provide automatic mitigation of infrastructure and application level attacks. These use a combination of traffic signatures, anomaly algorithms and other analysis techniques to detect malicious traffic in real-time and mitigates attacks with deterministic packet filtering, and priority-based traffic shaping.</p>
<b>Data Access Privilege Elevation and Audit Trails</b>	Comprehensive audit trails are automatically captured by JourneyApps. The audit trails contain information about data access, modification, and where data access privileges have been elevated by JourneyApps staff to access data for issue debugging and system maintenance purposes. Data Access Privilege Elevation is within the scope of the SOC 2 Type 2 report available from JourneyApps on request.
<b>Data Logical Separation</b>	JourneyApps is a multitenant environment with logical separation between all application deployments. An example of an application deployment is “Development” and “Production” for a specific application. NCC Group specifically tests the logical separation to ensure that all data is securely sandboxed.
<b>Configuration Management</b>	Configuration management is performed using infrastructure automation tools, and changes to systems follow the <i>Secure Development Process</i> described below.

# Security Processes and Policies at JourneyApps

---

<b>Defense in Depth</b>	JourneyApps follows the <i>Defense in Depth</i> strategy, applying redundancy and multiple layers of technical, administrative and physical controls to prevent security incidents. For further details, please refer to the SOC 2 Type 2 report available from JourneyApps upon request.
<b>Security Patch Management</b>	JourneyApps makes use of automated application and OS-level vulnerability scanning, and further subscribes to security advisories for any vulnerabilities. Security patches are applied as soon as they become available. Security Patch Management is within the scope of the SOC 2 Type 2 report available from JourneyApps on request.
<b>Secure Development Process</b>	The JourneyApps Secure Development Process takes a holistic and integrated approach to security and addresses security concerns during training, planning, architecture design, implementation, and verification. The process includes several practices such as source control, code review and quality assurance to ensure that a good security posture is maintained at all times. The Secure Development Process is within the scope of the SOC 2 Type 2 report available from JourneyApps upon request.
<b>Incident Management Process and Privacy Data Breach Notification Process</b>	<p>The JourneyApps Incident Response Plan consists of six key phases: preparation, identification, containment, eradication, recovery and root cause analysis.</p> <ul style="list-style-type: none"><li>• <i>Breach Notification Time Frame: within 24 hours after an incident has been identified.</i></li></ul> <p>The Incident Management Process is within the scope of the SOC 2 Type 2 report available from JourneyApps upon request.</p>

<p><b>Data Policies and Disaster Recovery / Business Continuity</b></p>	<p>The data on JourneyApps always remains the sole property of the customer. JourneyApps staff only access data when absolutely required in order to support a customer app (in accordance with <i>Data Access Privilege Elevation &amp; Audit Trails</i> described above).</p> <ul style="list-style-type: none"> <li>• Data Backups are held for 2 months.</li> <li>• Data modification audit logs are kept for 3 years.</li> </ul> <p><u>Recovery Objectives:</u>  JourneyApps aims to exceed our cloud uptime Service Level Agreement (SLA) by providing a highly available platform service running on distributed infrastructure, ensuring redundancy and resiliency. By delivering cloud services with an always-on / always-replicating architecture, the terms Recovery Time Objective (RTO) / Recovery Point Objective (RPO) become obsolete. Please refer to “Cloud Uptime Guarantee” for your specific subscription plan <a href="#">here</a>.</p> <p><i>On contract termination, all data is handed over to the customer in an open format determined by the customer and then securely deleted from JourneyApps servers.</i></p> <p><i>Data Policies and Disaster Recovery / Business Continuity is within the scope of the SOC 2 Type 2 report available from JourneyApps upon request.</i></p>
<p><b>Staff Policies</b></p>	<p>JourneyApps:</p> <ul style="list-style-type: none"> <li>• enforces <b>role-based access</b> for users and administrators.</li> <li>• follows the <b>principle of least privilege</b> – employees should only have the minimum security privileges required to do their job.</li> <li>• observes strict rules in terms of <b>confidentiality</b> – sensitive data is only disclosed to authorized staff.</li> <li>• has formal policies and procedures in place for <b>employment screening</b>, commensurate with the employee’s position and level of access, including conducting criminal background checks.</li> <li>• has a <b>permission control system</b> in place to limit access to system resources.</li> <li>• has an <b>account review and audit</b> process in place to review access to system resources by staff.</li> <li>• has a <b>credentials policy</b> in place.</li> <li>• ensures that if an employee is terminated, access to all systems is immediately revoked.</li> </ul> <p>Staff Policies are within the scope of the SOC 2 Type 2 report available from JourneyApps on request.</p>



# *Let's Get* **Started**

---

JourneyApps is a full-stack platform for building custom, integrated apps used by frontline teams on desktop, mobile and wearable devices, even when they're offline.

**See what JourneyApps can do for you. Get in touch!**

✉ [hello@journeyapps.com](mailto:hello@journeyapps.com)

🖱 [journeyapps.com](https://journeyapps.com)



# JOURNEYAPPS

The development platform  
for industrial apps.

Connect with us @journeyapps

