Security

Rely on one of the most secure digital platforms to build your solution.

Liferay has made security a priority of our platform so that you can conduct your business operations, with a platform you can trust.

For over two decades, Liferay has placed security, compliance, and data protection at the core of our product, offerings, and operations at Liferay. Because of our expertise and emphasis on security, we've been able to provide trusted solutions to industries where security is paramount, like finance, government, and healthcare.

To that end, we've provided full transparency on how we handle security in our platform and organization. This document aims to describe, at a high-level, some of the most critical features.

For more in-depth information, please visit our Trust Center.

Benefits

- **Liferay's partnership with Google Cloud** means that you can take advantage of Google Cloud's world-class secure infrastructure and technology for hosting your DXP site with Liferay SaaS or Liferay PaaS.
- **Easily control what content users see** or the functions they have access to at the account, user, or role level, using detailed permissions settings.
- **Securely manage identity with authentication widgets** or other configurable options, such as multi-factor authentication and SSO.
- **Secure web services with 4 security layers** that cover IP addresses, server access policies, and user authentication and permissions.

Rely on Liferay's secure platform to:

Manage Users with Robust Identity Management

There are several aspects of securing a Liferay installation including, but not limited to, following the best security practices for your hosting environment, database, search provider, application server, and Liferay DXP itself.

- **Authentication & SSO:** Authentication in Liferay is flexible; you can just use the Sign In widget to log in, and guests can use the same widget to create accounts with default permissions. Nearly every element of the default authentication experience can be changed by an administrator, including:

  - Multi-factor authentication
  - Single Sign-On (SSO)
  - Lightweight Directory Access Protocol (LDAP) for user validation
  - Account Restrictions

  Other methods of authenticating users and/or applications can be configured:

  - OpenID Connect
  - SAML
  - Kerberos
  - Token-Based solutions
  - CAPTCHA solutions
  - Password policies
  - OAuth 2.0 (for API)
  - Audit logs

- **Roles and Permissions:** It's just as critical to manage what users have access to after they log in. Use roles and permission to further tailor access to services, data, and content.

  Here's the different types of roles Liferay provides natively. You can also create your own roles according to your organizational needs.

  - Administrators have full access to the entire installation, including global settings and individual Sites, Organizations, and Users.
  - Guests are unauthenticated visitors and have the lowest-level permissions, which allow them to view public pages and sites, but cannot create or add content unless permitted.
  - Users that are authenticated to the portal have the same rights as guests but also have some additional basic rights for managing content. When enabled, users can build their personal sites.

You can define any number of Roles, each of which has a set of permissions that are scoped differently (e.g., the whole portal, a specific site, or some other scope where the permission is allowed). Users are then “assigned” the Role, and its permissions are enabled when the user enters the scope for which the Role is defined.

For permissions, Liferay provides a robust Role-Based Access Control (RBAC) system, where users assigned to roles are scoped to apply only in a specific context such as a site, organization, or globally.

To help you organize and administer your users, you can use Liferay’s Organizations entity. This allows users in a group to be in a distributed hierarchy and enables large organizations to empower and delegate users to administer their organizations.

Protect Your Users and Data

Emphasis on Data Protection

Liferay designs its products and offerings with robust security measures to safeguard information, including enforcing strict data access policies, carrying out comprehensive vendor evaluations, aligning our practices with evolving privacy regulations, and regularly educating and equipping our employees, commitments enshrined in our agreements.

GDPR Compliance

Though no software product can offer a checklist of features to make your company completely GDPR compliant, Liferay DXP provides tools to greatly accelerate a company’s journey towards compliance. With out-of-the-box features such as data export, data erasure, and user permissions combined with Liferay DXP’s flexible architecture, businesses can adapt the platform to the evolving needs of their data protection strategy.

For example, Liferay’s User Associated Data (UAD) framework helps your organization meet two of the General Data Protection Regulation’s (GDPR) technically challenging requirements:

- **The right to data portability.** Users have the right to receive their personal data in a machine-readable format.

- **The right to be forgotten.** Organizations can remove the ability (even for administrators) to glean information that could lead to knowing the identity of the user whose personal data was erased or anonymized. This mainly consists of deleting the identity information from the system and erasing or anonymizing content the user has interacted with, so it cannot be tracked to a real person.

Additionally, you can ensure GDPR compliance for your cookies by selecting Explicit Cookie Consent Mode within Liferay's configuration interface. You can also customize the text that will appear to display your company's cookie and privacy policies.

For a more detailed dive into how Liferay ensures it complies with the requirements under GDPR, read more here.

AntiSamy Module to Protect Web Editor Code

Liferay DXP includes an AntiSamy module that protects against malicious user-entered code. If your site allows users to post content in message boards, blogs, or other applications, these posts could include malicious code. The AntiSamy module filters HTML/CSS fragments and removes suspect JavaScript code from them. Liferay DXP uses the AntiSamy sanitizer and any existing configured sanitizers to scrub user input to blog entries, calendar events, Message Boards posts, Wiki pages, and Web Content articles.

Antivirus Module to Protect File Uploads

The product features ClamAV integration to scan and quarantine files uploaded to Document Library. The files are checked during upload or as a parallel job to ensure no malicious content is hosted by the site.

System for Cross-Domain Identity Management (SCIM)

System for Cross-domain Identity Management or SCIM, is an open standard that automates user provisioning. In other words, it's a standard way to create, update, and deactivate user identities. SCIM provides a unified, RFC-compliant way to keep user/group data in sync between different applications.

Secure Web Services

Liferay DXP relies on several layers of security measures to protect Liferay's web services, including customer deployed web services and/or REST or GraphQL applications.

- **IP Permission Layer:** The IP address from which a web service invocation request originates must be white-listed in the Liferay DXP server's portal configuration. Any attempted web service invocation coming from a non-whitelisted IP address will automatically fail. Controls access to the portal from previously white-listed addresses.

- **Authentication Verification Layer:** The authentication verification layer serves to validate provided credentials and to create portal authorization contexts for Service Access Policies, OAuth 2.0 Resource Server access checks and user permissions layer.

- Service Access Policy Layer: Service access policies allow the portal administrator to whitelist web service endpoints available to remote clients. They allow public services to require no authentication as well as restrict endpoints available to clients relying on user password, OAuth 2.0 and other supported credentials.
- User Permission Layer: Properly implemented web services have data permission checks. The user invoking a web service must have the appropriate Liferay DXP permissions to manipulate with the respective entities and data.
- OAuth 2.0 Resource Server Authorization Layer: This layer, similar to Service Access Policies, restricts access to JSON WS and REST resources for clients relying on OAuth 2.0 authorization credentials. The access is restricted based on OAuth 2.0 scopes that were granted during authorization phase by user and must match the scopes required by the respective JSONWS or REST and GraphQL application endpoints.
- CORS Support: Cross-origin resource sharing (CORS) is a standard allowing users to request resources stored on another origin, or web server at a different domain. Users can leverage CORS on Liferay in order to enable JavaScript clients or Single Page Applications to use Liferay Portal web services as a headless server.

For a complete list of Liferay DXP Application Security Features, download this whitepaper.

Test and Secure Platform Code

The platform source code is developed according to secure SDLC. The development team hiring process includes background checks and developers are educated annually on securite coding concepts and paradigms.

The code itself is tested regularly using SAST, DAST and SCA tools and annually using penetration tests. Please contact our Support team to obtain respective reports.

There is a vulnerability management process in place to fix any found vulnerability in a timely manner and notify customers with CVE records and CVSS scoring. As an open source company, Liferay believes in information sharing and posts all known vulnerabilities here: https://liferay.dev/portal/security/known-vulnerabilities.

Launch Securely in the Cloud

If you leverage either of our cloud offerings, Liferay SaaS or Liferay PaaS, they are both backed by Google Cloud. Your data security will be handled by a vendor that will ensure every part of your infrastructure is compliant and secure, leveraging Google's world-class and secure technology.

Cloud Security Assurance

Due to Liferay's partnership with Google Cloud, this allows Liferay to improve web traffic coming from ISP networks, providing a sophisticated form of DDoS protection, CDN, load balancing, and WAF.

Both Liferay SaaS and Liferay PaaS provide self-healing, high availability, and automated disaster recovery to make your solution as resilient as possible.

Shared Responsibility Model

Hosting applications and data on premises and in the cloud represents various challenges and security is one of them. Data and IT infrastructure ownership changes and it's important to understand the shift of responsibility from Customer to Liferay and the service provider, Google Cloud.

	Liferay DXP (Self-Hosted)	Liferay PaaS	Liferay Saas
Customer Data			
• Sites and hosted content • Personal Data compliance • Users, Accounts and Identities	Customer	Customer	Customer
Liferay Platform			
• Secure Configuration • Liferay Vulnerability Management • Liferay Upgrades, Patches and Hot-Fixes	Customer	Customer	Liferay
Application layer			
• Applications Vulnerability Management • Disaster-Recovery • Clustering, High-availability and Fail-Over • Backups • Performance Monitoring • Deployment and components orchestration • Web server, JVM, ElasticSearch, Tomcat, DB	Customer	Customer + Liferay	Liferay
• OSI Layer 7 DDoS protection and WAF	Customer	Customer	Liferay + Google

	Liferay DXP (Self-Hosted)	Liferay PaaS	Liferay Saas
OS and Virtual Network Layer			
• Access Monitoring • OSI Layer 4 DDoS protection	Customer	Google	Google
• Load Balancing • SSL/TLS termination and Key Management • Vulnerability & Patch Management • Operating System and Containerization • Data-in-transit encryption • Virtual networks and isolation	Customer	Liferay + Google	Liferay + Google
Physical Layer			
• Firewalls and network appliance • Data-at-rest encryption • Hardware maintenance • Environmental safeguards • Physical security	Customer	Google	Google

SaaS Benefits

With Liferay SaaS, you can offload data security and management to the Liferay team. Our SaaS offering provides features only available with SaaS including:

- AI-powered DDoS prevention and WAF to thwart cyber-terrorists.
- Automated data backups to ensure data and documents are protected and ready for restoration if needed.

Data Protection in the Cloud

Liferay utilizes several subprocessors like Google Cloud, AWS, or a SIEM provider to be able to provide the cloud services in a secure way. Personal data transfers to subprocessors undergo thorough review and implement appropriate safeguards where required by regional data protection laws.

Cloud services customers can choose their data residency to align with their GDPR, CCPA, LGPD, or other data privacy regulations.

Liferay employees' access to customer data is strictly isolated based on team location to provide support according to the respective regulations.

For more information, please visit our Trust Center.

Rest Assured with Security Certifications

Liferay platform follows the OWASP Top 10 (2017) and CWE/SANS Top 25 lists to ensure that Liferay DXP meets the security requirements necessary for protecting enterprises against known vulnerabilities and attacks.

Our cloud infrastructure compliance program includes:

- SOC 2 Type 1 & 2 Certification
- ISO/IEC 27001:2013 Certification
- ISO/IEC 27017:2015 Certification
- ISO/IEC 27018:2019 Certification
- HIPAA
- CSA Star Level 2

To learn more about our certifications, please visit our Trust Center.

Next Steps

Security is foundational to Liferay's offerings. On a single platform, you can leverage a secure platform, alongside many other native capabilities, to build current solutions and future ones, as your business needs expand.

Ready to see how you can depend on Liferay's secure platform?
Request a demo at liferay.com/request-a-demo.