litmus

675 Massachusetts Avenue, 10th Floor
Cambridge, MA 02139-3309

(866) 787 7030

hello@litmus.com

Frequently Asked Security Questions

Updated 15 March 2018 | security@litmus.com

Public

About Information Security at Litmus

Our Information Security Program secures the entirety of our business—our people, our processes, and our technology—to provide the security, control, and transparency expected by our partners and customers.

Our Information Security Program includes:

- **Administrative security controls**, including security policies, asset management, security audits, disaster recovery, security awareness training, security response, and vulnerability management
- **Technical security controls**, including application security, access controls, endpoint protection, network security, password management and multi-factor authentication, and security logging and monitoring
- **Physical security controls**, including physical and environmental security for facilities, badge readers, and equipment protection

For more on information security at Litmus, please see the article Security at Litmus: How We Keep Your Data + Assets Safe

About Litmus

The Litmus email creation, testing, and analytics platform empowers marketers, designers, and agencies to confidently deliver customer experiences that ensure brand alignment and quality, as well as maximize performance and deliverability. Major global brands across every industry and vertical trust Litmus to make email better, including 9 of the top 10 ecommerce brands, 7 of the top 10 technology companies, and 23 of the top 25 US ad agencies.

Security FAQs

1. How is my data protected?

Litmus maintains strict confidentiality and integrity of our customers' data. We leverage Amazon's AWS infrastructure and built-in security controls, which incorporates several modern security standards and best practices. Additionally, AWS maintains several security certifications and accreditations (e.g. HIPAA, FedRAMP, ISO 27001, and PCI compliance among several others). You can learn more about AWS security at http://aws.amazon.com/security/ and their compliance program at http://aws.amazon.com/compliance/

Data classified as "Confidential" or "Secret", such as usernames, passwords, analytics data, and email addresses are encrypted at rest and in transport using a cryptographically strong cipher (AES-128 bit or higher). Data classified as "Internal Use Only" is encrypted and password-protected and is only accessible to Litmus employees, contractors, and business partners. Data classified as "Public" is not password-protected or encrypted.

We recommend that customers with strict data sensitivity concerns omit any Personally Identifiable Information (PII) from our Email Analytics platform. Litmus should never have any of your sensitive, confidential, or proprietary data. For more information, visit https://litmus.com/help/analytics/exclude-pii/

2. Who has access to my data?

Litmus enforces several internal security policies and access controls to ensure that our customers' data is accessible only to those with proper authorization and need-to-know. Litmus only allows trained and authorized operations personnel to access data. The data is accessed only through secure VPN access which uses Two-Factor Authentication and elevated privileges to view campaign engagement data. This data is also encrypted at rest.

Litmus is willing to work with any customer to ensure a comprehensive understanding of the nature of our data access control policies.

3. Is my data shared with any third parties?

We share Your Personal Information in personally identifiable form with affiliated businesses and agents as part of our normal business operations. We use this information to personalize and improve our products and services. To read our full Privacy Policy, please go to https://litmus.com/privacy

4. What happens to my data when I close my Litmus account?

The account holder/owner retains copyright/ownership of any content uploaded to Litmus. In terms of your customer data, we only collect what you give us. For more detail, please see https://litmus.com/help/analytics/exclude-pii/

Clients are in charge of provisioning and deprovisioning accounts. This responsibility is owned by the admin of the account as appointed by the client.

If you decide to stop using Litmus, Litmus will delete all data associated to you at your request. Litmus can also send you all of your data in a downloadable format upon account closure. Please contact your Business Account Representative or email hello@litmus.com. Note that there is typically a 7-10 business day turnaround for these types of requests.

5. Does Litmus comply with Safe Harbor, Privacy Shield, and GDPR?

Since all our data is stored with Amazon, we automatically adhere to Safe Harbor laws. Amazon's Safe Harbor policy found here https://aws.amazon.com/privacy/ and here: https://aws.amazon.com/compliance/eu-data-protection/

Litmus is currently in the process of certifying with the Privacy Shield Program as well as the General Data Protection Regulation (GDPR). Note that we currently do not have the ability to limit the processing and storage of data to the EU. Litmus stores its data in AWS (US-EAST region) and cannot segment its data by region. We are diligently working to be GDPR compliant by the May 25, 2018 deadline. If you have any questions, please don't hesitate to reach out at privacy@litmus.com.

For more insight on information security at Litmus, please see the article Security at Litmus: How We Keep Your Data + Assets Safe

6. Does Litmus maintain ISO 27001 certification?

While we currently do not hold the ISO 27001 certification, we align our security principles, procedures, and best practices with ISO 27001. As Litmus has grown, we have recognized the need to provide clear and effective security policies and access controls to ensure that our customer's data is secure and accessible only to those authorized. The Litmus team is willing to work with you to ensure that your company has a comprehensive understanding of the nature of our data access control policies.

7. What type of data is collected for Email Analytics?

With our Email Analytics product, we collect data about the emails that you send. Such data may include the recipients' email, the browser and email client they use, the city that they are located in, and details about how the recipients engage in the email (e.g., whether or not the email was read, forwarded, or printed).

The data that is collected for Email Analytics can be categorized as follows:

- Campaign metadata - Campaign unique id, data regarding the date of the campaign, custom campaign fields
- Activity data - Aggregated counts regarding email opens, forwards, print activities
- Individual hit data - Data regarding email client, email client version and email platform (desktop, webmail, mobile)

8. What security controls does a Litmus account have?

Enterprise customers can control session settings and password settings, two-step verification, SSO, and role-based authorization for each of their account users.

- Session settings: You can set how long a user's session can be idle before they are automatically logged out. This helps prevent unauthorized access to a customer's account.
- Password settings: Admins can create password rules and adjust settings to ensure internal security requirements are met, including minimum password length and password complexity rules. You can set passwords to expire on a regular basis, for instance every 90 days. You can also opt to prevent password reuse and configure how many password changes are required before a password can be reused.
- Two-step verification: To provide your account with an added level of security, we have two-step verification via SMS.
- Multi-factor authentication: SAML-based Single Sign On is available to our Enterprise customers
- Rules-based authorization: Litmus supports the concept of admin, user and read-only role permissions on an account. These roles, except for admin, can be assigned at the sub-account/team level to control access and permissions.

Additionally, account admins have the ability restrict Email Analytics access for users across three levels of access:

1. Full Analytics Access
2. Partial (No PII) Analytics Access

3. No Analytics Access

9. What other security controls does Litmus employ to guarantee the security of customer data?

The following technical and administrative security controls are in place at Litmus to strengthen our security posture and maintain the highest levels of confidentiality, integrity, and availability required by our customers:

Application Security	The technical and administrative controls used to protect our applications from security threats.
Asset Management	The documentation, monitoring, and reporting of Litmus assets (e.g. data, physical machines, intellectual property), their owners, classification level, and lifecycle requirements.
Compliance & Security Audits	Scheduled third-party audits of our infrastructure, code, and processes to ensure we maintain the highest level of confidentiality, integrity, and availability of our systems and data. Compliance with major national and international privacy and data protection regulations.
Disaster Recovery	The processes and procedures followed in order to ensure the overall continuation of Litmus business operations during an outage event. Our confidential disaster recovery plan is available internally and reviewed annually, but is not available for public consumption.
Endpoint Protection	The hardening, patching, and protection of endpoints used by Litmus employees and contractors.
Incident Response	The identification and resolution of information security incidents quickly and effectively, minimizing their impact to the business, and reducing the risk of similar incidents occurring in the future.
Network Security	The configuration and application of security controls as applied to network devices to prevent unauthorized access or incorrect updates to the Litmus network.
Password Management and Multi-factor Authentication	The policies, procedures, and technical guidelines that ensure the secure implementation of the password management lifecycle at Litmus, as well as the guidelines and best practices for enabling multi-factor authentication for services used by Litmus team members.
Physical Security	The policies, procedures, and best practices that ensure the physical protection of Litmus assets against accident, attack, or unauthorized physical access.
Security Awareness Training	Activities undertaken by Litmus employees to ensure that effective, risk-based decisions are made in the best interest of the organization, while protecting critical and sensitive information from being

	compromised.
Security Event Logging and Monitoring	The recording, storage, and monitoring of important security-related events to help in the identification of threats that may lead to an information security incident, and to support forensic investigations.
Vulnerability Management	The standards and procedures for the identification and remediation of Litmus system and software security vulnerabilities.