Sumerian Security

sumerian®
Forward Thinking

Sumerian Security

Sumerian has been delivering analytics services to leading global enterprises for over 10 years, including to some of the world's largest financial services providers. We have a proven track record when it comes to keeping customer data safe and secure.

Sumerian implements a systematic approach to data security:

- Sumerian is ISO27001 accredited. We are externally audited every six months to verify we do what we say we do with respect to our Information Security processes and procedures. These include annual external penetration tests, and quarterly internal audits.
- Sumerian's Software as a Service (SaaS) is hosted on our own private hardware, co-located in a secure Tier II datacenter, managed by Verizon. Physically this is a state-of-the-art, security-manned datacenter, with all the best practice security controls you would expect from a company that provides co-location services for thousands of large enterprises.
- Sumerian has followed good industry practice when it comes to designing, implementing, and running our SaaS environment.

Our approach is outlined in more detail below.

Security details

Network

Our SaaS is deployed on our own private hardware. Only our web servers can be accessed from the Internet and then only via a secure username and password. The application and database servers are separated from the web servers via clustered Firewalls. These servers can only be accessed from within our Local Area Network.

Access to our Production application servers and database servers is strictly controlled. Access may only be granted through an approval process and all access is logged and audited.

Browser security

When you access Sumerian capacity planner your browser will display a secure padlock indicating that you are on a secure site. This means that all data transmitted between your browser and our servers is encrypted. This is also true when you are using Sumerian capacity planner to manually upload your data files; your data files are encrypted in transit.

We apply modern cryptography techniques to encrypt data in transit by using 128 bit TLS1.2 Comodo High Assurance Secure Server Certificate Authority including RSA as the key exchange mechanism.

User authentication

We ask you to use a password that is likely to be longer and more complex than your corporate standard.

Your password is only ever stored in one place on our system and it is hashed and salted. We do not know it nor will we ever ask you to tell us it.

Application security

Your data is only ever stored in our Production environment and, for a limited time, in the backup files we take of those systems.

Should you upload your data using our Data Collector utility, the data files will be compressed prior to transit and encrypted during transit (again using a 128 bit SSL certificate).
Your uploaded data files are then stored in our private storage.

We have processes in place to restrict our access to your data including strict audit trails.

Managing threats and vulnerabilities

Following good practice, we:

- employ multiple different types of firewalls across our infrastructure to protect against unauthorized network connections;
- run continuously-updating, anti-malware software on each of our servers;
- only open necessary network ports;
- regularly patch our servers against vulnerabilities;
- test the patches on our test and development environments before they go live on production;
- monitor our servers around the clock and our monitoring systems alert our team of critical failures;
- backup data every day to an off-site location;
- automate our server build process to make recovery faster.

Information we store about you

The only data about you that we can access and store is your registration data (such as your name, company, user name and email address).
This is necessary so that we can support you if you contact us for help when using our service.

We also store, and can access, any correspondence between you and us. This includes support tickets raised.

What is not secure?

For any browser based application, once data is in your local browser it is not encrypted (data is only encrypted during transportation). We also cannot protect information (i.e. reports) that you may store locally on your systems. This is your responsibility.

Data sensitivity

In forming a judgment as to whether you regard our security as sufficient for your business, you should consider how sensitive the data is that you intend to send us or upload.

The data we process for you is related to your infrastructure and infrastructure performance. It is unlikely that this data will contain commercial or personal data and as such will, in most businesses, be regarded as non-sensitive.

However, as a policy we treat your data as confidential and we have put in place security measures to protect it.

We believe we have done everything we should to protect your data and to give you the information you need to make an informed decision about Sumerian security.

More information

If you require further detail to satisfy your security concerns, please contact us at **support@sumerian.com**

We have a number of security papers available which will allow you to make a fully informed assessment of our security measures.

sumerian®
Forward Thinking