What we do and how we do it

How do we extract your data?

The Sumerian Data Collector extracts data using the most effective means available based on the management system in question. For example, with vCentre, the tool makes use of the vSphere eb Services API. The data collector then uses a secure R ST API to send this data to your Capacity Planner instance.

Communications using the Sumerian API are protected through a secure AAA authentication, authorization and accountability process that is performed over a mandatory SS connection. Authentication is requested by the Data Collector using your Capacity Planner login credentials, and a secure time restricted access token is issued from our login controller. The token is then hashed must be used for every subsequent API request. e then verify authentication on each request and perform an authorization process to make sure the request is valid and that you have access to the appropriate data.

e provide example code pro ects in common programming languages to demonstrate how to access our API. API documentation can be found at https://api.sumerian.com/v . / elp

As an additional security measure, we can revoke tokens if necessary.

What data do we take?

The data used by Capacity Planner is often considered as 'exhaust' of operations management. Resource utilization data at a fine granularity, normally used for near real time monitoring and reactive troubleshooting. This data is normally discarded or aggressively aggregated to the point where statistical analysis becomes meaningless. Capacity Planner retains this data at the original granularity to develop a rich statistical model of resource utilization and available capacity across the IT estate.

Capacity Planner uses a 'core' set of metrics as the starting point for capacity modelling. These core metrics are:

Server Compute

- CPU capacity and utilization
- Memory capacity and utilization
- IO rate

Storage

- Datastore capacity, utilization and allocation or equivalent
- VMDK/VM Files configuration and utilization or equivalent
- VM drive capacity and utilization

All data that is extracted from your environment is configured via a JSON configuration file and placed in a transfer folder prior as a package containing CSV data. It can be inspected and shared to ensure that the data that has been sent is what is expected and adhere to your internal security policies.

How do we use it?

our data is only ever stored in our Production environment and, for a limited time, in the backup files we take of those systems. our uploaded data files are then stored in our private storage. e have processes in place to restrict our access to your data including strict audit trails.

The data we process for you is operational data related to your IT Infrastructure and Capacity Planning. It is unlikely that this data will contain commercial or personal data and as such will, in most businesses, be regarded as non sensitive. As a policy we treat your data as confidential and we have put in place stringent security measures to protect it.

ach of our customers has their own dedicated and isolated Sumerian Capacity Planner stack meaning there is no risk of cross pollination of data.

Keeping your data secure

By upholding the highest information security standards and best practices, Sumerian have a proven consistent track record when it comes to keeping customer data safe secure.

- Sumerian employs the highest standards of internal security and privacy for customer data and as a testament to our commitment, we have been ISO27001 compliant since 2008 and accredited since February 2011.

- Sumerian is 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 we run quarterly internal audits.

- Sumerian's Capacity Planning as a Service (CPaaS) is hosted on our own private hardware co-located in a secure Tier II datacenter, managed by Verizon. This highly secure and state of the art datacenter, has 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.

Network Security

Our service environment 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.

Managing threats and vulnerabilities

To ensure that Sumerian provide the utmost best 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.