Cloud Security

Exari strives to keep the valuable data in your contracts secure at all times, which is why we utilize the most advanced and secure platforms for hosting. The Exari hosted delivery model provides a full service solution requiring only a web browser for user access, eliminating the need for internal IT support and expensive hardware.

Hosting Solution

Exari leverges Amazon Web Services (AWS) world-class platform for its hosting. AWS utilizes world-class data center facilities that offer cutting edge physical, security and technical solutions with the following certifications:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

Exari is SOC 2 certified

In addition the AWS platform meets several industry-specific standards, including:

- Criminal Justice Information Services(CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act(HIPAA)
- Motion Picture Association of America (MPAA)

Exari uses the AWS hosting infrastructure across four geographies – East Coast USA, West Coast USA, EU and APAC. Each region has multiple data centers that can be used for disaster recovery, redundancy and business continuity purposes. Exari provides dedicated virtual servers to its clients in a single tenant environment which increases security and allows our customers to control when maintenance is performed. Each server has its own unique address and can be restricted to only allow access from designated client IP addresses.

The Exari hosting solution provides our clients secure access to their mission critical contract data 24x7x365. The all-inclusive annual hosting fees includes your license, maintenance and technical support.

Data Center Facilities - Physical Security

The data centers Exari utilizes via AWS are state of the art, utilizing innovative architectural and engineering approaches. Every data centers are housed in nondescript facilities.

Physical Access

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. Access is only provided to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked. All physical access to data centers by all employees are logged and audited routinely.

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without any impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature

Climate control systems maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

Electrical, mechanical, and life support systems and equipment are all monitored so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning

When a storage device has reached the end of its useful life a decommissioning process begins that is designed to prevent customer data from being exposed to any unauthorized individuals. Techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) are used to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices

Network Security

Exari has implemented a world-class network infrastructure that is carefully monitored and managed.

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. Exari utilizes global AWS firewalls and ACLs along with local software based firewalls.

Protection and Monitoring

Exari along with AWS utilize a wide variety of automated monitoring systems to provide a high level of service performance and availability. These monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity. Systems are extensively instrumented to monitor key operational metrics.

Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics.

Every hosted server has at least the following metrics monitored with alarms:

- CPU
- Memory
- Network
- Data Storage
- OS Storage
- Application Server Status
- Web Server Status

Additionally, application and operating system logs are monitored via alerting mechanisms based on identified entries and patterns.

Security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. Man in the Middle (MITM) attacks are mitigated via SSL-protected endpoints which provide server authentication that automatically generate new SSH host certificates on first boot and log them to the instance's console.
Intrusion detection and prevention systems exist at various layers of the stack, including at the server level via configuration file monitoring.

Security scans against known exploits are conducted regularly by Exari and by independent external third parties.

Secure Transmission of Data

All data is transmitted to and from the application using SSL using a minimum of 128 bit encryption, the same technology that is used by secure banking applications.

Backup

Every Exari hosted server disk is snapshot nightly on at least a 14 day cycle. This allows full recovery to the same data center, another data center in the same region or if applicable, to another data center in a different region. Additionally, manual backups are taken of both the application and its data. These are all encrypted and stored using the same cycle as the snapshotting.

ABOUT EXARI

Exari delivers the most complete Enterprise Contract Lifecycle Management platform, used every day by market-leading companies to understand all aspects of their contract ecosystem worldwide. With Exari, customers can reduce contract risk and improve operating efficiency with 100% Contract Certainty™.

exari