Securing Your Financial Data with Kyriba

KYRIBA FACT SHEET

With fraud and cyberattacks increasing in both frequency and sophistication, it is important to partner with Kyriba to secure your most important data.

287
Average number of days to identify and contain a breach
– Ponemon Institute

40%
of global respondents reveal they dealt with a cloud breach in the last year
– 2021 Thales Data Threat Report

$4.24M
Average cost of a data breach in 2021
– Ponemon Institute

$1.2B
In GDPR non compliance fines issued in 2021
– DLA Piper Jan 2021

How We Support Your Organization

With a proven track record over more than 20 years in Treasury and Finance SaaS solutions, our extensive, advanced protection for your data, security, controls, and your operational processes will keep your firm protected.

Kyriba's Cyber Defense Center

Kyriba's Cyber Defense Center, staffed with experienced professionals provides 24/7, global, follow the sun support.

The goal of the Cyber Defense Center and Security Incident Response Team (CSIRT) is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the impact and likelihood of the incident from reoccurring. At the heart of the CDC, Kyriba runs Splunk as our Security Information and Event Management (SIEM) system.

Threat Intelligence

- Dark Web scanning for compromised credentials, which includes email addresses, usernames and passwords
- Bolsters our ability to defend against ransomware, credential theft, brand abuse, and other malicious activities both cyber and physical
- Leveraging industry sources which deliver relevant cyber threat insights in real time

Data Loss Prevention (DLP)

DLP focuses on detecting and preventing the leakage, loss or misuse of data whether it's through breaches, exfiltration, or unauthorized use. Kyriba's approach to DLP covers our endpoints and is an effective tool for us to protect our customers' data.

kyriba

DDoS Protections

Amazon Web Services (AWS) Shield defends against the most common and frequently occurring network and transport layer DDoS attacks that target your website or applications.

Encryption

Kyriba uses AWS encryption for all data at rest. This automatically encrypts all block and file data using 256-bit encryption before storing it onto virtual disks. All data is encrypted in transit as well.

Security Features and Capabilities

Kyriba's security is feature-rich and can be used to strengthen your financial controls framework and make audits and tracking of security and workflow easier than ever.

Single Sign On (SSO)

SSO allows a user to login using their company assigned username and password. SSO uses SAML 2.0 for LDAP authentication and Rest APIs to manage authorizations. All password controls are managed internally by their Corporate IT team and policies.

Multi Factor Authentication (MFA)

MFA is an effective fraud prevention tool when used on its own or ideally in combination with other security features like SSO or IP Filtering. MFA creates a randomly generated one-time password using the user's smartphone, a token, or a SWIFT 3SKey digital certificate.

IP Filtering

IP Filtering is a security feature that allows clients to restrict login to a predefined set of IP addresses – or ranges of addresses – which are set up and maintained by the system security administrator. If used on its own, IP filtering is an effective fraud prevention tool.

Kyriba Control Center

Maintaining control of treasury workflows is important for monitoring errors, disruptions and suspicious activity. Kyriba Control Center is used for monitoring workflows and treasury activity within Kyriba. Also used for early detection of unauthorized usage and potential fraud.

Virtual Private Network

Kyriba can set up and maintain a virtual private network (VPN) for each client so that users only access Kyriba through a dedicated network maintained by Kyriba. It is commonly used in combination with IP filtering and MFA to customize the level of protection for both centralized and decentralized users.

3SKey Support

Kyriba incorporates digital signatures as part of the core security features. Personal identity tools are provided that allow the user to digitally sign messages and electronic documents, as well as approve transactions within the system. Kyriba supports the SWIFT 3SKey digital signature format. Kyriba Digital Signatures can be used to approve and/or authenticate payments sent to your banks from Kyriba, authenticate payments sent via non-bank channels and to login to Kyriba as one option for multi-factor authentication.

Assurances, Certifications and Compliance

From third-party penetration testing and ethical hacking, to industry standard auditing and reporting, Kyriba is always focused on compliance and security as well as maintaining security and other data related certifications as part of our commitment to our customers. Kyriba's Risk and Compliance team conducts the following assurance engagements at least annually:

- ISO27001 Certification of Kyriba's Information Security Management System (ISMS)
- SOC 1 / SOC 2 Compliance
- SWIFT L2BA certified (AL2 Provider) / CSP AL2 and Service Bureau Compliant
- Penetration Testing / Ethical Hacking
- Frequent Red Team exercises with industry-leading Cyber Defense Firm
- Dedicated

Privacy Focus

Our Privacy Team is knowledgeable on privacy laws and emerging trends worldwide to keep your corporate entities and your subsidiaries compliant.