Kyriba Extended Security

KYRIBA FACT SHEET

With fraud and cyberattacks increasing in both frequency and sophistication, it is important to partner with Kyriba. 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 Extended Security package offers additional layers of application security to better protect treasury information, workflows and information. Kyriba's standard configuration offers strong password controls such as timeouts, mandatory resets, alphanumeric requirements and Kyriba's Virtual Keyboard – all of which can be set up to meet treasury and corporate IT policies.

> "Average cost of a data breach in 2020 was $3.8M."
>
> **– Ponemon Institute**

How We Support Your Organization

Our Team

Kyriba's Cyber Defense Center, staffed with experienced professionals provides 24/7, global, follow the sun support. The Center is responsible for responding to information security incidents that happen and provides quick turn-around times for contacting and resolving security and privacy issues.

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. Kyriba's Information Security organization is well versed and certified in the areas of Information Security ranging from CISSP, CRISC, GIAC and PMP. The Information Security team has a deep understanding of various security frameworks such as ISO, PCI, FedRAMP, DOD and NIST. At the heart of the CDC, Kyriba runs Splunk as our Security Information and Event Management (SIEM) system.

AWS Hosting

- Our Global SaaS infrastructure is hosted on Amazon Web Services (AWS) across multiple availability zones and regions in several countries (Europe, North America, Canada and China). AWS allows Kyriba to scale efficiently when it comes to performance, enhanced security, modern application practices, and availability.
- No maintenance fees (describe in more detail the benefits of SaaS).
- Comprehensive Disaster Recovery Program
- Uptime SLA and RTO/RPO (recovery time objective and / recovery point objective)

DDOS Protections

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

Encryption

Kyriba uses AWS default encryption for all storage. 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.

Threat intelligence

- Dark Web scanning for compromised credentials, which includes email addresses, usernames and password (we have real world examples where we've discovered stolen credentials of a customer and were able to alert them).
- Bolsters our ability to defend against ransomware, credential theft, etc...
- Leveraging industry sources which deliver relevant cyber threat insights in real time

Data Loss Prevention

An important part of any company's overall security strategy includes a comprehensive approach to Data Loss Prevention (DLP). DLP focuses on detecting and preventing the leakage, loss or misuse of data whether it's through breaches, ex-filtration transmissions or unauthorized use. Kyriba's approach to DLP covers all of our endpoints and is an effective tool for us to protect all our customers data.

Features and Capabilities

Kyriba's Extended Security offers features to take application security and protection to levels not offered by other SaaS firms to protect our customers and prevent outages, prevent unauthorized access, data theft or mitigate the risk of fraudulent attacks and crimes.

Multi Factor Authentication

Multi-factor authentication creates a randomly generated one-time password using the user's smartphone, a token, or a SWIFT 3SKey digital certificate. When multil-factor authentication is activated, the user is prompted to enter the one-time password after submitting their normal UserID and password. This makes multi-factor authentication an effective fraud prevention tool when used on its own or ideally in combination with other Kyriba Extended Security modules.

IP Filtering

Kyriba IP Filtering is a security feature that allows clients to restrict login to a pre-defined 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 IP Filtering can also be used in combination with other Kyriba Extended Security modules – for example any user logging in outside of the pre-defined set of IP addresses is required to use multi-factor authentication.

Single Sign On (SSO)

Single Sign On allows single sign-on with a client's internal security environment. SSO uses SAML 2.0 for LDAP authentication and Rest API's to manage authorizations. With SSO, no additional UserID and password is required and all password controls are managed internally by the corporate IT team and policies.

Kyriba Control Center

Maintaining control of treasury workflows is important for monitoring of errors, disruptions and suspicious activity. Kyriba Control Center is often used for monitoring workflows and treasury activity within Kyriba. Also used for early detection of unauthorized usage and potential fraud, Kyriba Control Center offers the opportunity to monitor and analyze:

- Bank connectivity failures, including files expected but not received
- Payment files where final acknowledgement was not received
- Escalation and summary of pending workflow approvals
- Real-time status alerts of additions, deletions or modifications of data
- Red/Yellow/Green status for workflow, data, and task monitoring

Reporting

- Hundreds of configurable reports
- Out-of-the-box dashboards
- Automated scheduling
- PDF, Excel and HTML formats
- Distribute reports via email

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. The VPN is ideal for centralized or regionalized treasury teams.

It is commonly used in combination with IP filtering and dual-factor authentication 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 approving transactions within the system. Kyriba supports the SWIFT 3SKey digital signature format. Kyriba Digital Signatures can be used in the following scenarios:

- Approve payments – those payments originated within Kyriba or imported from external systems such as ERP
- Authenticate payments sent to bank from Kyriba – payments managed within Kyriba or batches blind routed from ERP to the bank via Kyriba's Payment Hub
- Authenticate payments sent via non-bank channels from Kyriba – for both payments managed within Kyriba and batches blind routed from ERP
- Login to Kyriba as one option for multi-factor authentication

Assurances and Compliance

From outside firms conducting ethical hacking tests and other penetration testing, Kyriba is always focused on compliance and security testing as well as maintaining security and other data-related certifications as part of our commitment to our customers.

- ISO27001 Certification
- SOC 1 / SOC 2
- SWIFT Compliance Audit
- Penetration Testing / Ethical Hacking
- Frequent Red Team exercises with industry leading Cyber Defense Firm
- Full Risk and Compliance Team

ISO 27001 CERTIFIED by schellman

Privacy

Kyriba is privacy focused. Our dedicated Security Team stays current on all privacy laws and emerging trends and technology, worldwide to keep your corporate entities and your subsidiaries protected.

SUPPORT FOR:
GDPR (Global privacy laws for UK/EU)
CCPA (California Consumer Privacy Act)

To learn more and find out how Kyriba's Security capabilities can help protect your organization, visit **www.kyriba.com**.