BLACKLINE PLATFORM INTEGRITY

Security, Availability, and Disaster Recovery

BLACKLINE

Trust is in the Balance™

Your Trusted Partner for Financial Corporate Performance Management

BlackLine is a leading provider of cloud software that automates and controls the entire financial close process. Recognized by Gartner as a Leader in Financial Corporate Performance Management (FCPM), we partner with over 1,600 organizations globally, including the world's best known brands and fastest growing companies, to elevate their finance and accounting performance.

Beyond delivering transformative visibility, efficiency, and control to the financial close for our customers, we're committed to leading with security and disaster recovery and measure our performance against the highest standards for compliance in the industry today. And as a cloud provider to global enterprises, we continually monitor availability, the threat environment, and improve our information security policies and procedures day in, day out – all as an integral part of our service.

Building client relationships that engender trust is our priority and starts with delivering transparency into BlackLine's operations and policies and procedures that safeguard your data. This document provides you with insight into BlackLine's regulatory compliance, certifications, and processes that are designed to protect and secure your financials.

Regulatory Compliance and Certifications

As part of our commitment to maintaining a world-class security infrastructure, we validate the effectiveness of our security controls by auditing our environment using internationally recognized auditing standards – SSAE 16 SOC 1/2/3 Type II and ISAE 3402. We also hold the ISO/IEC 27001:2013 compliance certification.

Further, BlackLine partners with top tier data center providers to ensure the availability and security of our service. Ultimately, our controls and safeguards translate to unsurpassed security and privacy for our customers' information, no matter where they are in the world.

SSAE 16 (SOC 1) & SOC 2 Auditing

BlackLine publishes annual SOC 1 and SOC 2 Type II reports. These Service Organization Controls (SOC) reports conform to SSAE 16 (Statement on Standards for Attestation Engagements No. 16) and ISAE 3402 (International Standard on Assurance Engagements No. 3402) auditing standards which provide guidance for auditors assessing controls at a service organization, such as BlackLine, that are relevant to customers' internal control over financial reporting.

The SOC 1 Type II report addresses the design and operating effectiveness of BlackLine controls as they relate to customers' internal control over financial reporting. SOC 2 Type II addresses the design and operating effectiveness of BlackLine controls as they pertain to specific Trust Services Principles, such as system security and system availability.

Both SOC 1 and 2 audits are conducted annually by an independent third-party auditor. Together, these reports affirm BlackLine's ability to safeguard our customers' critical business data. Both reports are available to customers and prospects upon request.

ISO/IEC 27001:2013 Compliant

BlackLine is proud to have achieved ISO/IEC 27001 certification in 2013, becoming the first account reconciliation and financial close software provider to attain this certification.

Jointly published by the International Standardization Organization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 is a globally recognized information security standard that provides organizations with requirements for an information security management system (ISMS).

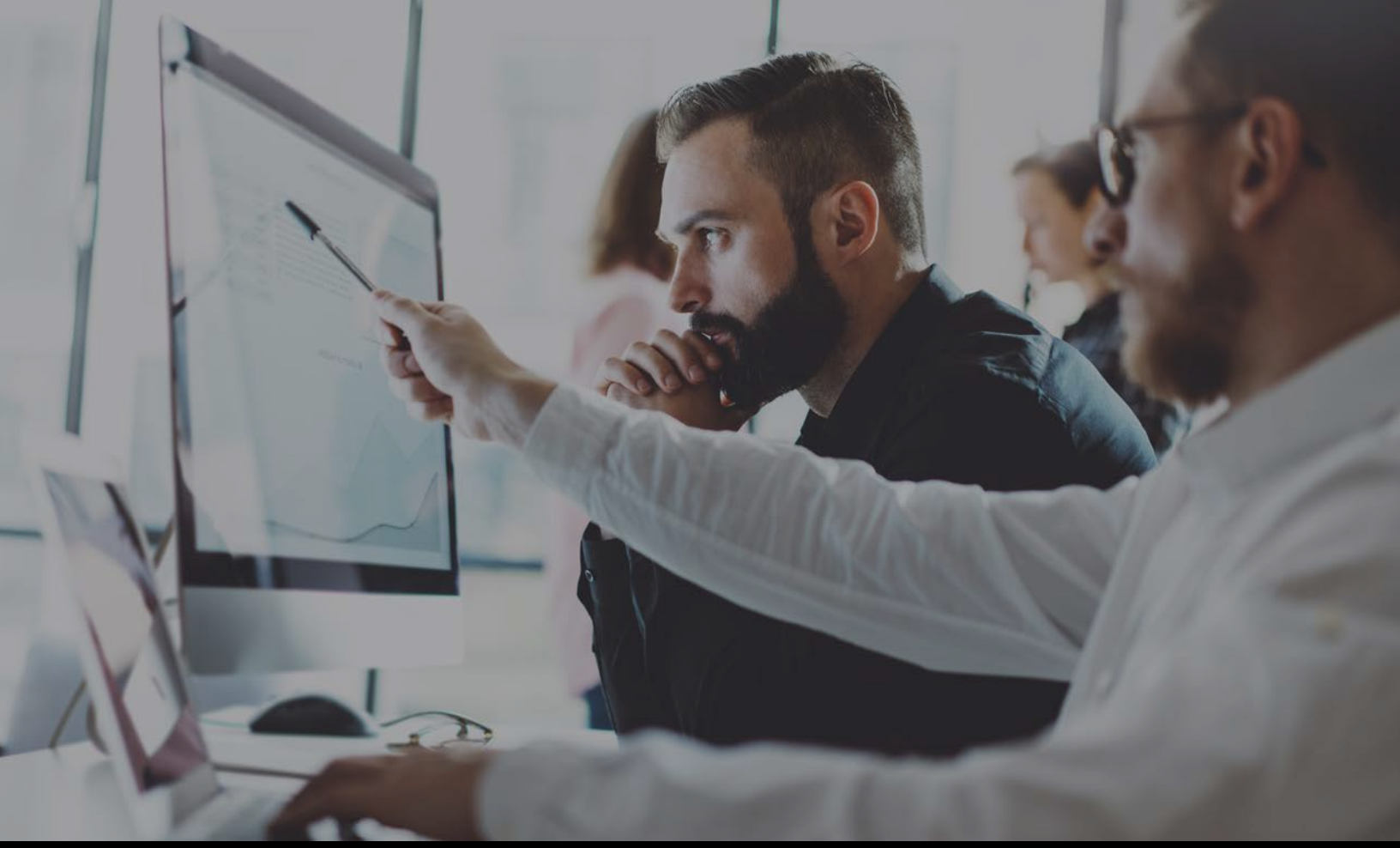
To maintain ISO/IEC 27001:2013 certification, BlackLine undergoes a two-stage certification audit by an independent certification body. Annual audits are conducted to validate compliance with the standard, and a full recertification occurs every three years.

BlackLine's ISO27001:2013 certificate is available for customer and prospect review upon request.

Cross-Border Data Transfers

BlackLine maintains separate data centers in the EU, and no EU customer data is transferred outside of the EU. BlackLine is committed to maintain compliance with EU security and privacy regulations, including the EU-US Privacy Shield.

Additionally, BlackLine provides production and disaster recovery data centers in both the United States (Culpeper, Virginia and Las Vegas, Nevada) and Europe (Amsterdam, Netherland and London, England). This ensures that customers data is proximal to their geographic locations.



Security

As a standard part of our service delivery, we maintain physical security at our data centers, as well as data, network, and application security. Our team of technology and security experts operates world-class layered infrastructure that protects our production and corporate environments. Our security infrastructure includes: firewalls, load balancers, intrusion detection systems, log management systems, encryption for data at rest and in transit, anti-malware technologies, behavioral and pattern analysis tools, and other security solutions, including proprietary tools developed by our team.

Physical Security

BlackLine servers and operations for production and disaster recovery are located in top tier, enterprise-grade data centers certified for security and availability. Designed to meet the stringent requirements of the world's largest enterprises, they provide the best practices around secure physical access control; environmental monitoring and management and redundancy; power protection and backup; fire detection and suppression; and network performance management and redundancy. The result is a level of physical security and failover that often exceeds what enterprises can achieve in-house.

Access Control

- 24-hour manned security, including foot patrols and perimeter inspections
- Computing equipment in access controlled steel cages
- Video surveillance throughout facility and perimeter
- Building engineered for local seismic, storm, and flood risks
- Secure, network operations center to monitor building management system

Environmental Monitoring and Controls

- Entire HVAC plant – chillers, compressors, heat exchangers, and distribution systems – monitored for all environmental operating parameters by a Building Management System
- Redundant N+2 HVAC cooling system with 100% Service Level Agreement

Power Management and Failover

- Underground utility power feed
- Redundant N+2 CPS/UPS systems
- Redundant power distribution units (PDUs)
- Diesel generators with on-site diesel fuel storage

Fire Detection and Suppression

- State-of-the-art fire detection and suppression systems using the latest advances in pre-action water

Power Management and Failover

- Redundant internal networks
- Network neutral; connects to all major carriers and located near major internet hubs
- High bandwidth capacity
- Redundant network providers, disparate access points, proactive network management, and fault-tolerant network architecture

Network Security

BlackLine is dedicated to continually improving upon our monitoring procedures in response to changing risks and threats. We adhere to industry standard processes, procedures, and best practices regarding information security. We continuously scan our networks and applications for vulnerabilities, and regularly conduct third party penetration testing exercises. The network perimeter is protected by firewalls and both external and internal networks are monitored by intrusion detection systems which are sourced from leading information security vendors. BlackLine collects, monitors, and analyzes systems, infrastructure, and application logs in an effort to identify and respond to security incidents as quickly as possible.

Secure Transmission and Sessions

Connection to the BlackLine environment is via TLS cryptographic protocols, ensuring that our users have a secure, encrypted connection.

Network Protection

- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers
- Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts, and reports
- External networks are scanned for vulnerabilities daily

Data Security

Data Management

Client databases reside within a protected network segment that is not directly accessible from the internet.

Only authorized production DBAs have privileges to access the databases; and this access is controlled and user access lists are audited on a periodic basis.

Data Encryption

BlackLine adheres to the highest security standards to protect our customers' data and communications. Client data is encrypted in transit using TLS/SSL technologies, and our service enforces, at a minimum, 128-bit TLS ciphers (higher-strength ciphers are preferred if supported on the client side) and 2048-bit encryption keys for all web communications and data transfers.

Data transfers via SFTP (SSH File Transfer Protocol) and FTPS (File Transfer Protocol over SSL) are encrypted using public key authentication with a minimum 2048-bit RSA key.

All data at rest is secured using 256-bit AES (Advanced Encryption Standard) encryption.

Application Security

Authentication Methods

BlackLine supports a full range of authentication methods to meet the specific needs of your organization.

Native Login

With BlackLine's native login, a unique username and password combination is used to authenticate users. System administrators can configure a variety of password settings to enforce password requirements and security policies. All session IDs are unique and encrypted.

Single Sign-On Authentication

Single Sign-On (SSO) allows application administrators to provision access by enabling users to easily access BlackLine using an integrated logon. BlackLine supports Security Assertion Markup Language (SAML 2.0) and works with a variety of SAML providers such as One Login, SSO Easy, VMWare Identity Manager, Extend CA Single Sign-On, and more.

BlackLine supports user authentication via a federated identity, reducing the need for provisioning user accounts, by using federated authentication using Security Assertion Markup Language (SAML) with Microsoft Active Directory Federation Services (ADFS). Additionally, if the client's authentication system supports an integrated logon through a browser, the user won't be prompted for credentials; they'll be authenticated silently and the federation service will translate the local knowledge of the user's identity into BlackLine.

Passwords

With BlackLine's native login, a unique username and password combination is used to authenticate users. System administrators can configure a variety of password settings to enforce password requirements and security policies. All session IDs are unique and encrypted.

Password Complexity

Minimum password complexity requirements (i.e., minimum length, must contain special characters, numbers, mixed case letters, etc.) are configurable within the system.

Password Expiration

BlackLine passwords expire after a defined interval which can be configured by system administrators. Users will be alerted to change their password when the password expiration date is approaching.

Enforce Password History

To prevent users from reusing the same passwords, administrators can set the number of unique passwords that must be used before a user can reuse an old password.

Failed Login Attempts

The number of times a user can unsuccessfully enter a password before they are locked out of the system is a configurable property. If this limit is reached, the user will not be able to login for a period of time that is also definable by the administrator.

Session Security

BlackLine administrators can configure their system inactivity timeout interval. The default session timeout value is 60 minutes.

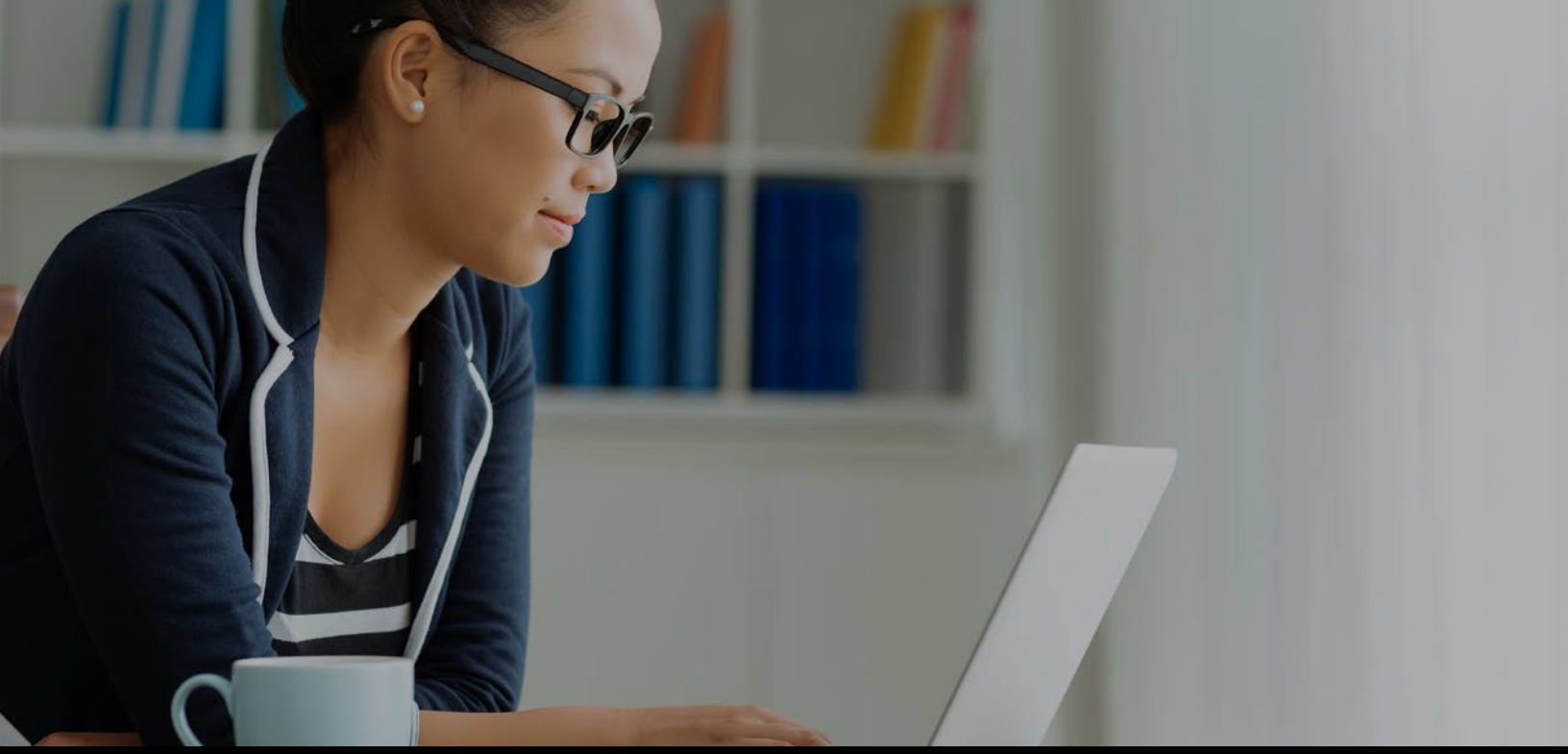
IP Whitelisting

To apply an additional layer of security and prevent unauthorized access to your BlackLine instance, administrators can define a range of IP addresses that are permitted to access the application. Once IP whitelisting has been enabled, users attempting to login from an IP address outside the defined range will be denied access.

Authorization

BlackLine's application utilizes role-based security for authorization. User access is enforced using a set of flexibly defined user roles. The application prevents customer end users from directly accessing the production database. BlackLine's security groups, combined with BlackLine's predefined security policies, grant or restrict user access to functionality, business processes, reports, and data.

Customer-configurable security groups can be based on users, roles, jobs, organizations, or business sites and can be combined into new security groups that logically include and exclude other groups. Customers can thereby tailor these groups and policies to meet their needs, providing as finely grained access as required to support complex configurations, including global implementations.



Availability and Performance

We take pride in our track record of availability and are confident that we won't just meet your expectations when it comes to performance and availability – we'll exceed them. Current status, response times, security status, and more, are published on trust.blackline.com to provide transparency into our performance at all times.

PROVEN AVAILABILITY

Over the past 12 months, BlackLine has achieved over 99.98% availability

PROVEN PERFORMANCE

Over the past 12 months, BlackLine has achieved quick response time

Application Availability

To ensure high availability and prevent any single point of failure in the application environment, BlackLine deploys redundant devices for all network switches, firewalls, load balancers, storage arrays, physical servers, and database servers. Web servers, application servers, and backend services are also configured in a highly available manner. Additionally, all data is stored on enterprise-class NAS (network-attached storage) systems using RAID (redundant array of independent disks) storage systems and multiple data paths to ensure redundancy and performance.

Application Performance

We know that user satisfaction is closely tied to application performance. It's why we publish our performance and responsiveness at trust.blackline.com. We continually monitor our performance and identify any infrastructure or application bottlenecks. With our cloud infrastructure, our customers benefit from elastic use of resources as their user and transaction volumes grow. We are continually adding more compute resources to our cloud, enabling our customers to benefit from accelerating performance based on the latest commodity hardware and infrastructure.

Maintenance and Scheduled Downtime

BlackLine's uptime target is 100% (excluding emergency and scheduled maintenance). Application downtime may occur for the following reasons: scheduled maintenance; emergency maintenance; and any unavailability caused by circumstances beyond BlackLine's reasonable control. Downtime is measured from the time a trouble ticket is opened.

Disaster Recovery

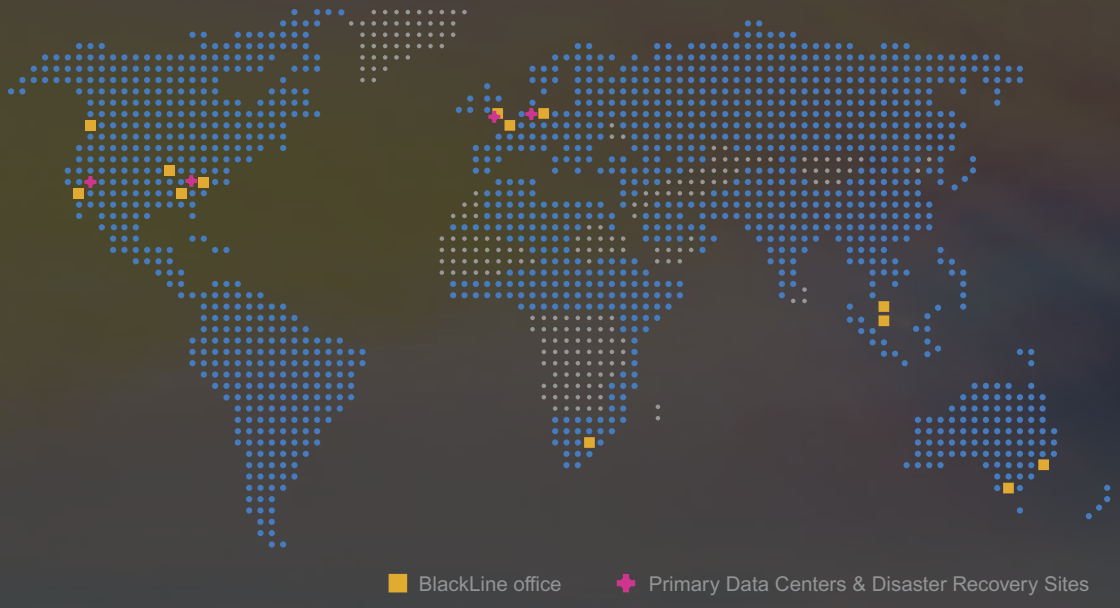
BlackLine has prepared a hot site within our data centers to ensure network operations continue in the event of a disaster. More specifically, all application data is backed up in real time via secure VPN tunnel to alternate mirrored data centers. In the event of an unscheduled outage that is expected to exceed a predefined duration, production processing will be diverted to a disaster recovery site for continued operation.

Data Backups

All BlackLine customer data, up to the last committed transaction, is automatically replicated to a secondary database and backed up daily. Full data backups are stored to a secure, offsite data center on a daily basis and are protected using AES-256 encryption.

Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

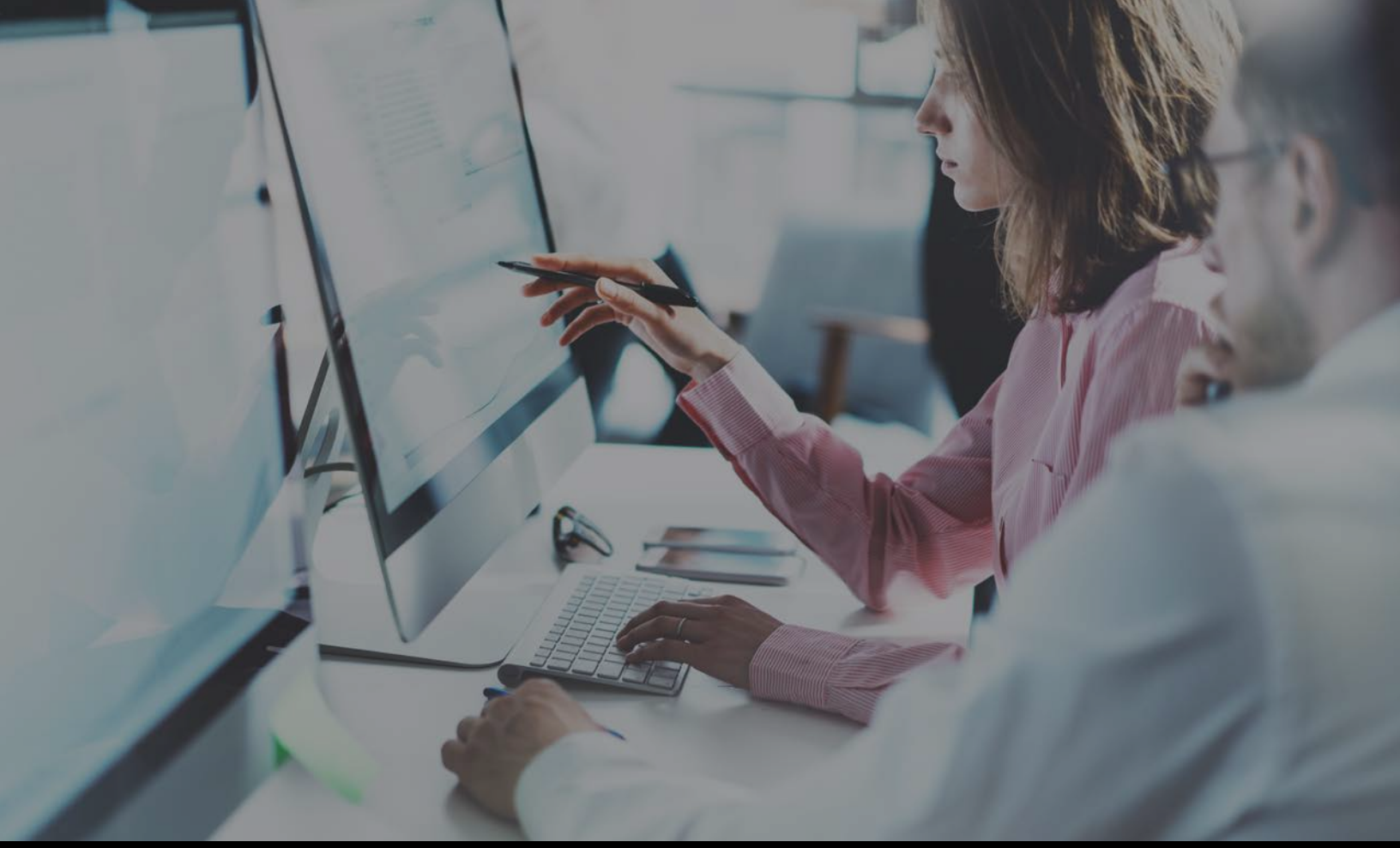
BlackLine assures a 1-hour RPO (the maximum allowable time interval in which data might be lost) and a 2-hour RTO (the maximum amount of time the application will be unavailable). Disaster recovery testing is conducted at least once annually, and the environment is monitored 24 hours a day, 7 days a week.



Production & Disaster Recovery Data Centers

BlackLine employs multiple data centers for both production systems and disaster recovery (DR) across North America and Europe, providing customers with production and disaster recovery data centers proximate to their center of business.

CULPEPER, VIRGINIA LAS VEGAS, NEVADA AMSTERDAM, NETHERLANDS LONDON, ENGLAND



Summary

Trust is at the center of what we do. And we understand that inspiring trust in the financial close means more than transforming process alone – it's delivering on our promise to protect your business critical information and adhering to the most rigorous standards for data confidentiality, integrity, and availability. It's why we're focused on continually leading the industry, with not only the most stringent certifications and procedures when it comes to protecting your data, but also providing transparency into how we're meeting our commitments to you.

We're ready to answer further questions to ensure you have the utmost confidence in our demonstrated commitment to information security and privacy.