BlackLine

Security Datasheet

World-Class Security

BlackLine delivers state-of-the-art security that ensures our customer data is protected and held as a top priority. BlackLine has committed significant ongoing resources to building and maintaining a world-class security infrastructure. We validate the effectiveness of our security controls by achieving internationally recognized auditing standards - SSAE 16 SOC 1/2/3 Type II, ISAE 3402 and the ISO/IEC 27001 certification.

BlackLine partners with top tier, ISO 27001 certified datacenters to ensure the availability and security of our service and to protect client's data from theft, corruption or mishandling. Ultimately, our world-class controls and safeguards translate to unsurpassed security and privacy for our customers' information.

Information Security Ensured By:

- Certified engineering and security teams that are thoroughly experienced in managing and monitoring enterprise-grade technologies
- Effective use of modern risk assessment techniques and security management tools
- Ongoing evaluation of emerging information security trends and threat landscape
- Total commitment to a secure, private, scalable, and always available platform

Security Details

BlackLine's team of technology and security experts operates world-class layered security infrastructure that protects our production and corporate environments. Our security arsenal includes firewalls, load balancers, intrusion detection systems, log management systems, encryption for data at rest and in transit, anti-DDoS, anti-malware technologies and other security solutions, including proprietary products developed by our team.

Data Center Security

Our production equipment is located in tier-3 and tier-4 datacenter facilities that provide 24-hour physical security, keycard and biometric authentication, continuous interior and exterior surveillance, N+1 redundant HVAC (Heating Ventilation Air Conditioning) systems, advanced fire suppression systems, N+1 redundant UPS (Uninterruptible Power Supply) power with instantaneous failover if primary UPS fails, routinely tested on-site diesel generators that can run indefinitely, fully redundant enterprise-class network backbone, multiple internet uplinks, and rigorously tested backup and recovery processes designed to keep our service available during regional disasters and major outages.

Network Perimeter Defense

The network perimeter is protected by firewalls and monitored by intrusion detection systems which are sourced from leading information security vendors. BlackLine monitors and analyzes firewall and IDS logs around the clock to proactively identify and respond to security incidents. BlackLine's network achieves zero downtime through the use of redundant network providers, disparate access points, proactive network management and fault-tolerant network architecture.

Operating System Security

BlackLine enforces strict operating system-level security by running only required services on all production servers. Physical access to production servers is restricted; we also centrally enforce and manage authentication and authorization and maintain strong access and password policies. Our change management processes ensure that all operating systems are maintained at current patch levels for security; we monitor compliance with our minimum security baselines and adhere to information security standards and best practices.

Server Management Security

BlackLine operations team utilized a wide portfolio of tools to monitor health and performance of BlackLine servers. BlackLine employees do not have direct access to the production servers, except when it is necessary for system maintenance, management or troubleshooting.

Database Security

Databases containing clients' data reside within a protected network segment that is not directly accessible from the Internet. Only authorized production DBAs have privileges to access the databases; this access is strictly controlled. Our databases are configured in compliance with information security best practices. BlackLine applications access databases through a standardized data access layer that minimizes a possibility of any unauthorized access. Your information is logically segregated from other customers' data and it cannot be accessed by other BlackLine customers.

Application Security

Our application security model implements compartmentalization and role management to enforce segregation of duties and logical isolation of clients' data. This prevents one BlackLine customer from accessing another customer's data and low-privileged application users from accessing data outside of their domains. BlackLine production and development applications are continually tested for security defects by third party application testing services. Any identified issues get reviewed by Information Security and prioritized for prompt remediation.

Internal Systems Security

BlackLine web servers that do not house any clients' data are the only ones directly accessible from the Internet. BlackLine application servers and other systems are protected by firewalls and have no internet connectivity. BlackLine maintains a set of security configuration standards and monitors compliance with these standards to ensure adequate protection of internal systems. BlackLine conducts weekly vulnerability scans and annual penetration tests of our infrastructure.

User Authentication

Users access BlackLine's application with a valid username and password combination, which is encrypted via TLS while in transmission. Users are required to choose strong passwords and to change them at regular intervals. Single-Sign-On may be utilized to integrate with clients' identity management and authentication systems. An encrypted session ID is used to uniquely identify each user and for added security, is automatically renewed at regular intervals. BlackLine does not store user passwords in clear text; they are irreversibly encrypted to prevent brute force attacks.

Data Encryption

BlackLine utilizes strong encryption to protect customers' data and communications. Online communications are protected using SSL certificates. BlackLine servers require the use of at least 128-bit ciphers and disallow insecure protocols, such as SSLv2. Data imports are protected using industry-standard secure communication mechanisms, such as FTPS and SFTP. We also encrypt data transfers with 1024-bit or longer RSA public keys. Additionally, BlackLine goes beyond industry standards providing encryption for data at rest. All clients' data within BlackLine environments (in the database or via attached items or reports) is encrypted using 256-bit AES.

Reliability and Backup

All customer data are stored on databases that reside on redundant enterprise-class NAS storage where data availability is ensured by using RAID volumes and multiple data paths. All customer data, up to the last committed transaction, is automatically replicated to a secondary database and also securely backed up daily. Backup integrity is verified and AES-256-encrypted backup media are moved to a secure, fire-resistant, off-site storage facility on a weekly basis. BlackLine has strategically implemented high availability throughout its environment to prevent single points of failure and to maximize uptime. To achieve this, BlackLine has deployed redundant (N+1) devices for all network switches, firewalls, load balancers, storage arrays, physical servers and database servers. Additionally, web servers, application servers, and backend services are deployed in a highly available manner.

Disaster Recovery

BlackLine offers a Hot Disaster Recovery service which is included with the OnDemand offering. This service continuously synchronizes data between our production and geographically remote disaster recovery data centers. The DR site and our recovery procedures are designed to guarantee one hour recovery point objective (RPO) and two hour recovery time objective (RTO) during any outages. BlackLine regularly tests and reviews our disaster recovery procedures.

Security Governance & Training

BlackLine maintains a comprehensive information security program that follows ISO27002. We maintain, test, and continuously update our information security policies, risk management, and incident response processes to ensure that our customers' data stays protected at all times. Our information security program is communicated to all employees. BlackLine conducts annual company-wide information security awareness trainings and hosts secure coding practices classes and other specialized security trainings for our development and technical teams.

Use of the BlackLine services is subject to the terms and conditions of the customer's subscription agreement with BlackLine. BlackLine may modify its security infrastructure and/or this security datasheet from time to time.