bluecanvas

Security at Blue Canvas

Blue Canvas is a SOC-2 certified, cloud hosted Git repository that allows you to back-up, track and manage your Salesforce metadata. We safeguard your metadata and help you meet the compliance challenges of managing distributed teams.

Blue Canvas is a SOC-2 Certified Vendor

Security was built into our design. Blue Canvas has completed a full third-party SOC 2 audit—an independent auditor has evaluated our product, infrastructure, and policies, and certifies that Blue Canvas complies with their rigorous standards. Contact us for a copy of the audit report.

Secure Culture

We prioritize security at Blue Canvas. We believe that security is a process – it's more than just firewalls, password rotation, and certifications. Security is also about culture and policies. At Blue Canvas, we have set out to build a security-literate and conscious culture from day one. This ranges from the way we think about hiring and training, to the vendors that we select (like AWS and Auth0), to how we implement our systems. Everyone on the team is trained in security best practices, including two-factor authentication, proper password management, and encryption.

Many young companies treat security as an afterthought. We understand the pressure many feel to do this, but we believe that making a conscious strategic investment in security best practices at an early stage is crucial for us and our customers.

Secure Infrastructure

Secure infrastructure provides the basis for a trustworthy application. We elected to leverage Amazon Web Services (AWS) for their industry leading security focus and best practices. AWS physical facilities, networks, hardware, and operational software is designed and managed according to security best practices and a variety of security

compliance standards, including: ISO 27001, PCI DSS Level 1, HIPAA, and SOC 1, 2, and 3.

AWS Physical Security

AWS offers strictly controlled physical access monitored by professional security staff using video surveillance and intrusion detection systems. Authorized staff are required to pass two-factor authentication a minimum of two times to access data center floors.

Physical security also includes automatic fire detection and suppression systems as well as fully redundant power systems. When hardware reaches end of life, AWS has a strict decommissioning process designed to keep customer data safe. They use practices described in DoD 5220.22-M or NIST 800-88 to destroy data when hardware is decommissioned.

AWS Network Security

AWS provides secure network architecture using firewalls and other boundary devices to monitor communications at external boundaries of the network and key internal boundaries. Boundary devices employ access control lists (ACL). AWS infrastructure is designed specifically to protect against traditional network security issues including: DDoS, Man-in-the-Middle Attacks, IP Spoofing, and Port Scanning. Packet sniffing by other AWS tenants is not possible and even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic.

Salesforce API Security

We leverage security mechanisms provided by Salesforce to protect access to privileged APIs and authentication tokens. We process all authentication and delegation through Auth0 (https://auth0.com/), a purpose built, certified authentication platform. Auth0 acts as the IdP and delegation endpoint for our own user authentication, as well as the connections established between Blue Canvas and the Salesforce APIs. Auth0 is compliant and certified under SOC 2 Type II and HIPAA BAA.

OAuth 2.0 Credential Exchange

The authentication with Salesforce is based on an OAuth 2.0 flow. This ensures that the username/password credentials (and 2-factor if enabled) are handled only by

Salesforce.com and never exposed to us directly. After signing in, the user approves our Connected App.

To access the Salesforce API for synchronization, our backend servers request a short-lived access token from a restricted delegation endpoint. Access tokens are not stored at rest. Each delegation attempt is audit-logged and can be reviewed by us in our Auth0 backend, and by the customer in their Salesforce Org.

The delegation endpoint forwards a request to Salesforce. The forwarded request is authenticated using certificate based (RS256) client assertions, instead of the usual refresh tokens.

Users can independently monitor access from Blue Canvas to their Salesforce Orgs through the Connect Apps OAuth Usage (https://help.salesforce.com/s/articleView?id=remoteaccess_request_manage.htm&language=en_US&type=0) feature provided by Salesforce. If necessary, users can also utilize this feature to completely revoke API access.

Logs

Salesforce independently keeps logs of all security events that happen on their systems, so you can independently audit every request that Blue Canvas makes.

Server and Software Stack Security

Blue Canvas has controls in place to protect the security of application services, customer data and system configuration. Access to production servers is controlled by network isolation and firewalls. Changes to application software and system infrastructure are tracked in version controlled code repositories.

Secured APIs and Authenticated Access

Blue Canvas APIs and applications are only accessible over encrypted TLS/SSL channels, and every request requires authentication with a time-limited access token, issued by the authentication subsystem described above. We utilize 2048-bit RSA keys with a modern cipher suite to strengthen encryption. Server certificates are securely stored using AWS Certificate Manager and cannot be accessed directly.

Logging

All infrastructure API requests, such as administrative management access, storage access, or changes to infrastructure configuration, are logged permanently using AWS CloudTrail. Authentication activity, such as end-user sign-ins, password changes, administrative access, and API token delegation is logged independently for us by Auth0.

Rate Limiting

Blue Canvas applications have built-in rate limiting and block excessive requests to ensure service quality and availability. Excessive attempts to sign into a user account using brute-force attempts are detected and blocked automatically.

Change Management

Changes made to Blue Canvas application software are executed through automated build verification and deployment processes. Code modifications are visible in our version control system. Similarly, infrastructure is managed and changed through declarative configuration files that are stored and versioned in our code repository. Changes are rolled out to minimize impact on our customers and on service availability.

Network Protection

By default, all traffic from external networks is blocked and no traffic is allowed to directly access Blue Canvas servers and services. Firewalls regulate traffic into our private non-routable IP networks. API and application requests are processed by a proxy services and load balancers before they are handed off to our internal servers.

Further Information

If you have any questions about our security culture or practices, we are happy to schedule a call with you. Please reach out to your account representative or email team@bluecanvas.io to set this up.