

securityMETRICS®

POWERED BY

rackspace



- Thousands of customers, worldwide
- Guaranteed 99.95% uptime
- The industry's best value
- Fully deploys in days
- 24/7 support
- Proven installs across vertical markets

### Contact Bold Software

1938 N. Woodlawn  
Suite 410  
Wichita, KS 67208

[www.boldsoft.com](http://www.boldsoft.com)

[info@boldsoft.com](mailto:info@boldsoft.com)

866.753.9933  
316.630.9933



### Overview

Bold Software, LLC, the makers of BoldChat, BoldCall, and BoldCCM, consider its customers' data an asset of the customer entrusted to Bold Software that requires Bold Software to treat each element of data with a high level of security.

Bold Software considers every element of customer data equally private and crucial and has designed its security envelope with that in mind.

### Computer-Related Security

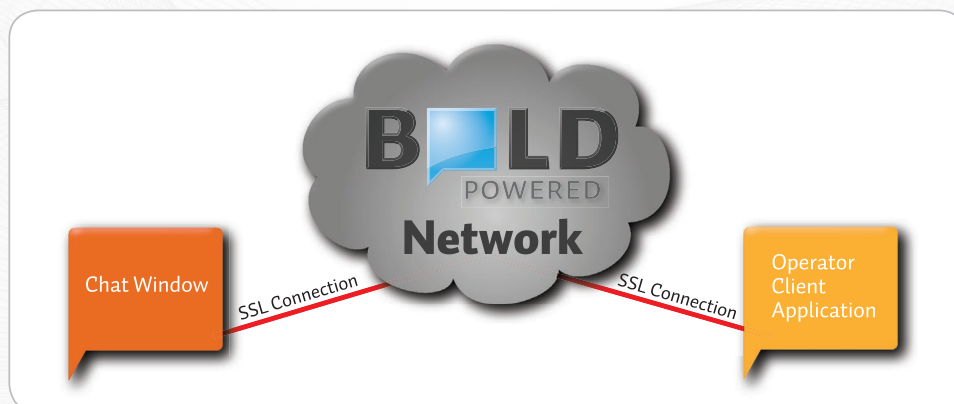
Bold Software has computer-related security and compliance monitoring with security standards and procedures for the Bold Software product line as follows:

- Defined and documented organizational security standards and procedures.
- All employees and contractors required to sign a confidentiality agreement.
- Background checks for all employees that have access to customer data.
- Restricted access to only those employees that have a need to manage customer data or manage servers hosting customer data.
- Process for the timely revocation of access to any customer data from any employee or contractor that leaves the company or who no longer has a need to access customer data. Access is revoked within 24 hours of employee or contractor departure or reassignment.
- Provide training on all internal security policies.
- Conduct ongoing security awareness training programs.

### Physical Security

Physical security for data centers hosting the servers containing customer data meets the following requirements:

- Rooms are secured by at least two access mechanisms (e.g., building key-card, man traps, security guard, and computer room badge-in).
- Only authorized employees are allowed physical access to the servers hosting customer data.
- The vendor maintains 24/7 security at the location.
- All backups of customer data are either stored on-site with controlled access or at a secure vendor-controlled or commercial off-site location.
- The site supports additional levels of protection such as uninterruptible power and fire suppression.



- Failed storage components in the datacenter undergo a DoD-approved “erase” or “wipe” procedure (if functionally possible) prior to destruction.

### Technical Controls

Bold Software has implemented technical controls that provide protection to its network, systems, and applications.

- Bold Software utilizes a top tier hosting provider that provides a professional hosting environment that protects systems hosting customer data from external threats.
- Bold Software maintains individual accountability for employees and contractors that access systems that host customer data. Bold Software has documented user account/password management system for these employees and contractors.
- Bold Software ensures that individual access to customer data is controlled (i.e., a separate user name and password is required for each individual administrator). Customer data is compartmentalized to prevent unauthorized access and separated from the data of other customers.
- Access to customer data is protected by hardened passwords rotated on a 90 day basis.
- Wireless connectivity to networks or servers hosting customer data is protected using security mechanisms such as EAP, TTLS, TLS, or PEAP.
- Bold Software has formal security policies and procedures in place that deal with viruses, other malware, and related threats. Anti-virus software programs are required, installed, and active on all Windows-based machines. These systems have automated periodic full scans and use updated virus signature files.

### Usage Criteria

In order to protect the confidentiality, integrity, and availability of customer data, the Bold Software applications meet the following usage criteria:

- Each user is assigned a unique ID. User IDs and passwords meet the following requirements:
  - Users may change their password at any time.
  - Passwords must be at least 5 characters long.
- The application and resulting access to data in the database has permissionbased controls restricting access to authorized customer users as determined by the customer data owner.
- Each change of user login status is logged within each application. All logs are treated as confidential information and access to reports can be restricted using the permission system. Reporting of this information is available within the application.
- If confidential data, personal data (e.g., names, addresses, phone numbers), or authentication information (e.g., passwords) is transmitted, our products support and Bold Software recommends the implementation of the optional 128-bit SSL encryption between each component of the communications path.
- By implementing the our products, users agree to be bound by the Bold Software Acceptable Usage Policy.
- Bold Software’s security policy assumes customer data retention is permanent and is designed to that standard. Customers retain the ability to implement their own data retention policy.