

Make Compliance for Remote Computer Control Easier.

In addition to meeting security measures for remote computer control, many industries must satisfy federal compliance standards like HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and others. Many federal regulations affect how you authenticate users, grant remote access, audit your helpdesk, or ensure security during remote computer control sessions. The chart below explains how features of Bomgar™ remote support solutions endeavor to answer these regulatory requirements.

Security Standard	Bomgar™ Feature	Function
Identification & Authentication	Multiple password layers	Prevents unauthorized users from accessing the software
	Optional complex password requirement	Requires users to create a password with three of the four character classes
	Failed password lockout	Prevents users from logging in after password attempts have failed a set number of times
	Password expiration	Requires reps to change passwords after a set length of time
	Session keys	Randomly generates session keys to prevent unknown customers from connecting to the support rep
	Multi-factor authentication	Authenticate users with multiple security providers, including LDAP and RSA
Limiting Access	Permission-based access	Prevents users from accessing a remote PC without the remote client's permission
	Level of access determined by administrator	Enables an administrator to determine features and level of control allowed to individual reps or support rep groups
	Application sharing	Customers can grant access to their entire computers or limit access to selected programs
	Complete customer client uninstall from the remote computer	Uninstalls the small download on the remote PC to ensure that users cannot access the remote computer after termination of a session unless the customer reinitiates the session
Manual Session Termination	Customer can terminate session at any time	Enables the customer to end the session whenever needed in order to prevent the rep from viewing classified information
	Idle session time-out	Logs idle reps out of the rep console after a set length of time
Audit Controls	Downloadable reports	View reports on all session data, including command prompt recordings, complete chat transcripts, files transferred, and permissions granted
	Session recordings	Keep FLV recordings of support sessions for detailed auditing
	Logging and reporting API/ BMC Remedy Integration	Automatically upload session activity reports, session recordings, and remote command prompts into external applications and databases, such as BMC Remedy, for easy retrieval and auditing
	Syslog server configuration	Configure your PC to receive real-time data on appliance configuration changes
Secure Data Transfer	256-bit AES encryption of all session traffic and login pages	Encrypts datastream end to end to protect all data from outside attack
	No firewall configuration or extra ports opened	Works transparently through corporate firewalls on both rep and customer systems

Why is self-hosting remote computer support better than using a 3rd party service provider?

Control vs. Responsibility

Compliance regulations acknowledge that a company's scope of responsibility often extends beyond its scope of control. Regulated companies must not only ensure that internal processes, data storage and procedures are compliant with federal regulations, but also that any engagement in which a third-party service provider handles one or more business functions complies just as rigorously. In effect, companies are ultimately liable for compliance in each third party service relationship, whether the third party service is regulated or not.

You can outsource business processes and resources, but you cannot outsource liability. Service level agreements or other contractual elements may lessen potential damages, but they cannot lessen liability and may therefore be insufficient protection. One route of self-protection involves regular audits of third-party services by a third-party auditing organization. Thorough audits are preferable to cursory ones to demonstrate for liability purposes that a company has undergone the process of due diligence in ensuring compliance. Nevertheless, such audits are time consuming and costly.

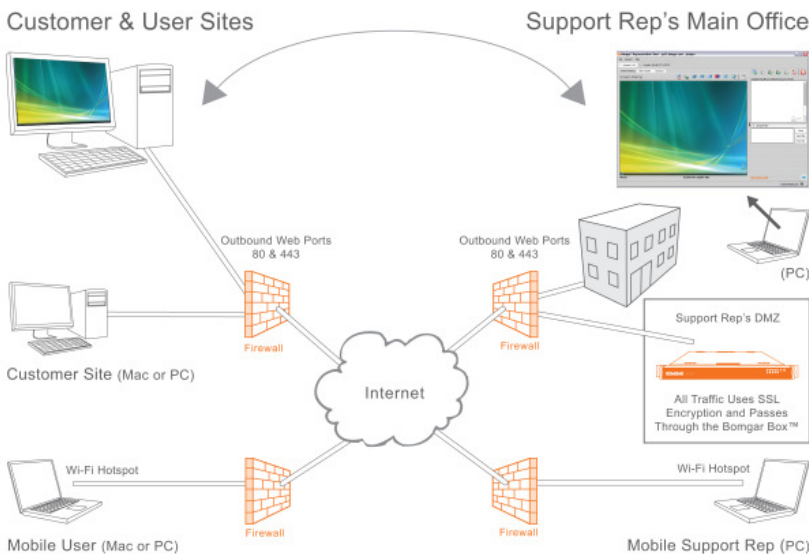
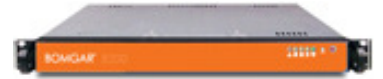
Minimize Risk by Increasing Control

To ensure the most protection from non-compliance liability, companies should keep regulated data inside. It is easier to bring in-house those procedures that involve secure access to regulated information, especially when those procedures involve remote access to clients' computers. Companies should also record and report on actions taken by support reps giving remote assistance. Bringing remote computer support in-house allows companies to maintain their existing infrastructure while minimizing the scope of compliance responsibility.

Bomgar™ is the only remote support software application with its own dedicated appliance. By facilitating the direct administration of support processes, the Bomgar Box™ helps companies remain competitive without exposure to the unnecessary risks entailed with using a remote computer support application as a service. Appliance-based remote support helps regulated companies remain compliant by enabling them to control processes for which they are ultimately responsible.

The Bomgar Box™

- Administer all support reps from a central interface
- Granular control of rep access privileges by client and admin
- Conform security settings and authentication methods to your environment
- Store commonly used support files
- Self-host the Bomgar Box™
- Record & report on support sessions



Secure Support

Bomgar™ uses Symantec-audited security architecture for remote computer control.

