BOMGAR™

Security Whitepaper

TC:4/21/2014

Table of Contents

Introduction

The purpose of this document is to help technically-oriented professionals understand the security related value Bomgar can bring to your organization. Bomgar can help move your support organization forward by helping your organization stay secure and compliant, all while improving the efficiency and success of your support organization with a better end-user support experience.

Revised April 2014

Bomgar Overview

Bomgar is a comprehensive remote support solution using an appliance-based architecture. The Bomgar Appliance gives support technicians secure remote control of computers, over the Internet or on local networks. This specialized appliance provides exceptional performance, reliability, ease of use and scalability through a solution that is optimized for remote support. With Bomgar, a support technician can see the supported screen and control the supported system remotely, as if physically present.

Using multiple features designed to ensure the security of remote support sessions, Bomgar integrates with external user directories, such as LDAP, for secure user management; prevents sensitive data from being routed outside the organization; and supports extensive auditing and recording of support sessions. Logging is performed by the Bomgar Appliance, which allows for the review of all customer and support representative interactions, including video playback of all desktop screen interactions. Bomgar also integrates with leading systems management and identity management solutions and includes an API for deeper integration. With Bomgar, support managers can create support teams, customize queues, and report on all support activity.

Bomgar enables remote access to multiple operating systems, including Windows, Mac, various Linux distributions, and mobile operating systems. Bomgar also enables remote control of various kinds of systems, including laptops, desktops, servers, kiosks, point-of-sale systems, smartphones, and network devices.

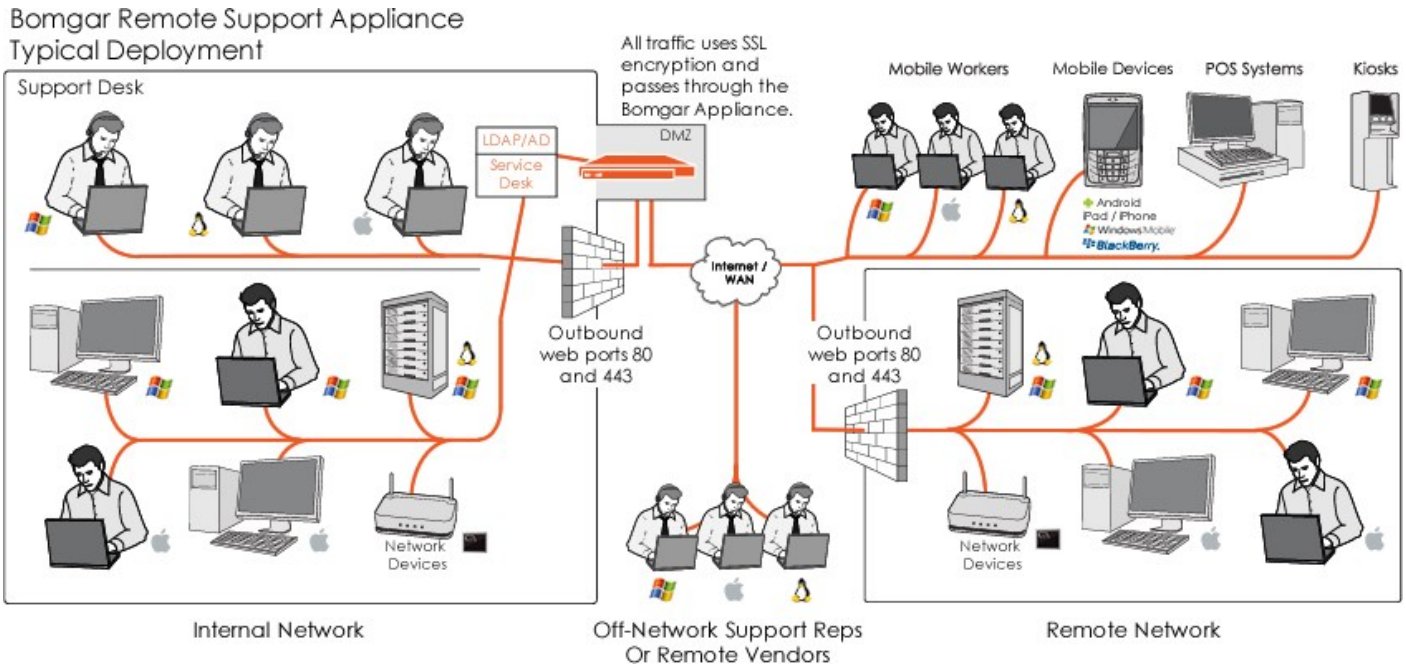
Bomgar can work over internal and extended networks, or it can be Internet accessible. This allows support organizations to avoid less effective means of support by driving requests through custom support portals hosted on a hardened appliance. Bomgar can match support requests with the appropriate technician or team. Bomgar then mediates connections between customers and support representatives, allowing chat sessions, file downloads/uploads, remote control of desktops, screen-sharing in either direction, running of presentations, and access to system information and diagnostics.

Bomgar Architecture

To make secure remote support possible, Bomgar architecture places the Bomgar Appliance as the focal point of all communications. The appliance provides a platform to build a support portal, a site, through which an organization funnels all remote support requests. The support portal offers a web site interface using Hypertext Transfer Protocol (HTTP) for unauthenticated services, Secure HTTP (HTTPS) for authenticated services, and direct client connections accepted over a proprietary, Bomgar-defined protocol.

Bomgar has two primary binary components that provide the appliance's functionality. The first, called Base, is made up of the firmware that provides system-level configuration of a Bomgar Appliance. Settings such as IP addresses and Secure Socket Layers (SSL) configuration are all configured via the Base interface which is accessed via the /appliance web interface.

The second component is made up of the software that provides site-level configuration and is accessed via the /login web interface. Behind the /login page is where customer support portal configuration takes place, and the Bomgar Representative Console, Bomgar Customer Client, Bomgar Jump Clients, Bomgar Jumpoints, and security provider connection agents can be downloaded. Support sessions will always occur through the appliance, and since the connections are outbound from the clients to the appliance using well known ports, the application can communicate without local firewall changes.

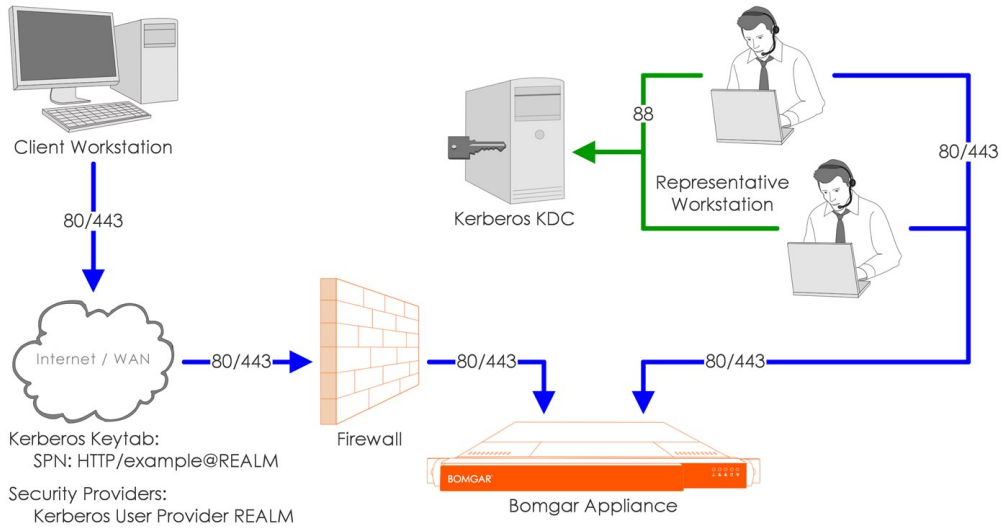


Authentication

Bomgar may be provisioned for locally defined Bomgar user accounts or can be integrated into existing authentication sources. For instance, a commonly integrated authentication source is Microsoft Active Directory. When using a directory such as this, all authentication follows the existing controls and processes in place for safeguarding user accounts.

Additional security providers are available that allow for representative authentication using Kerberos (for single sign-on) or using RADIUS (for multi-factor authentication). Each of these providers can be configured to use LDAP groups to set the permissions for the support representative, allowing you to map existing LDAP groups to support teams in Bomgar.

There are a large number of granular permissions that can be granted to support representatives. These permissions determine what features in Bomgar a representative has access to, and can require end-user prompting so that the user receiving support must approve representative actions. Additionally, a representative can be allowed view-only support access, if the organizational preferred permission is restricted to that level.



Kerberos Authentication Flow with LDAP Group Lookup

SSL/TLS and Port Surface Exposure

Bomgar can be configured such that it enforces the use of SSL for every connection made to the appliance. Bomgar requires that this SSL certificate being used to encrypt the transport is valid, and can also be configured to ensure that only FIPS 140-2-compliant algorithms are used.

Bomgar can natively generate CSR requests using 2048 or 4096 bit RSA for the key length choices, but also supports importing certificates generated off of the appliance. Configuration options also are available to disable the use of SSLv3. Bomgar will always have TLSV1 enabled to ensure proper operation of the appliance. Available cipher suites can be enabled or disabled and re-ordered in the preferred preference of use.

The Bomgar software itself is uniquely built for each customer. As part of the build, an encrypted license file is generated that contains the support portal Domain Name System (DNS) name and the SSL certificate, which is used by the respective Bomgar client to validate the connection that is made to the appliance.

The chart below highlights the required ports and the optional ports. Note that there is very minimal port exposure of the Bomgar Appliance. This drastically reduces the potential exposed attack surface of the appliance.

Firewall Rules	
Internet to the DMZ*	
TCP Port 80 (optional)	Used to host the portal page without the user having to type HTTPS. The traffic can be automatically rolled over to port 443.
TCP Port 443 (required)**	Used for all session traffic.
TCP Port 8200 (optional)	Used as a rollover port if traffic is not being routed through port 443.
Internal Network to the DMZ*	
TCP Port 80 (optional)	Used to host the portal page without the user having to type HTTPS. The traffic can be automatically rolled over to port 443.
TCP Port 161/UDP	Used for SNMP queries via IP configuration settings in the /appliance interface.
TCP Port 443 (required)**	Used for all session traffic.
TCP Port 8200 (optional)	Used as a rollover port if traffic is not being routed through port 443.
DMZ to the Internet*	
TCP Port 443 to the specific hosts **update.bomgar.com** and **download.bomgar.com** (optional)	You can optionally enable access from the appliance on port 443 to these hosts for automatic updates, or you can apply updates manually.
TCP Port 5832 (required for Passive)	Used as a listening port by Passive Jump Clients. Operating system firewalls should also be aware of this port. Note that the port number is configurable by an administrator.
DMZ to the Internal Network*	
UDP Port 123 (optional)	Access NTP server and sync the time.
LDAP - TCP/UDP 389 (optional)‡	Access LDAP server and authenticate users.
LDAP - TCP/UDP 636 (optional)‡	Access LDAP server and authenticate users via SSL.
Syslog - UDP 514 (required for logging)	Used to send syslog messages to a syslog server in the internal network. Alternatively, messages can be sent to a syslog server located within the DMZ.
DNS - UDP 53 (required if DNS server is outside the DMZ)	Access DNS server to verify that a DNS A record or CNAME record points to the appliance.

Firewall Rules	
TCP Port 25 (optional)	Allows the appliance to send admin mail alerts.
TCP Port 443 (optional)	Appliance to web services (such as HP Service Manager and BMC Remedy) for outbound events.
TCP Port 5832 (required for Passive)	Used as a listening port by Passive Jump Clients. Operating system firewalls should also be aware of this port. Note that the port number is configurable by an administrator.

*Rules can conform to the specific IP address(es) used by your Bomgar Appliance(s).

**Each of the following Bomgar components can be configured to connect on a port other than 443:

Representative Console *Customer Client* *Presentation Attendee Client*
Jumpoint *Connection Agent*

‡ If the LDAP server is outside of the DMZ, the Bomgar Connection Agent is used to authenticate users via LDAP.

Auditing

Bomgar provides two types of support session logging. All the events of an individual support session are logged as a text-based log. This log includes representatives involved, permissions granted by the customer, chat transcripts, system information, and any other actions taken by the Bomgar representative. This data is available on the appliance in an un-editable format for up to 90 days, but can be moved to an external database using the Bomgar Integration Client. All support sessions are assigned a unique session ID referred to as an LSID. The session LSID is 32 character string that is a unique GUID for each session. The LSID is stored as part of each session log for every session conducted.

Bomgar also allows enabling video session recordings. This records the GUI of the customer screen for the entire support session. The recording also contains metadata to identify who is in control of the mouse and keyboard at any given time, during the playback of the recorded session. The period of time these recordings remain available is dependent on the amount of session activity, and the available storage, up to 90 days maximum. As with the support session logging, these recordings can be moved to an external file store using the Bomgar API or the Bomgar Integration Client.

Each Bomgar Appliance model has differing amounts of available disk space, but default is set to purge data over 90 days old. The Bomgar Integration Client can be used to export data off of the appliance and store it if needed to comply with security policies. Bomgar can also be configured to store data for a shorter period of time to help comply with security policies.

The Integration Client (IC) is a Windows application that exercises the Bomgar API to export session logs, recordings, and backups from one or more Bomgar Appliances according to a defined periodic schedule. The IC uses plug-in modules to determine the repository for the exported data.

Bomgar provides two IC plug-in modules. One handles export of reports and Flash video recordings to a file system destination. The second exports select report information (a subset of the entire data collection) to a Microsoft SQL Server database. Setup of the IC for SQL Server includes all of the procedures needed to automatically define the necessary database, tables and fields.

In practice, the Integration Client is used to export support session data that must be retained for legal and compliance reasons. The reports and recordings are archived in a file system, indexed by the Bomgar Appliance and session IDs. Data stored in the SQL Server tables may be queried to locate the Bomgar session ID corresponding to given search criteria such as date, service desk representative, or IP address.

All authentication events, such as when a representative logs into the representative console or accesses the /login or /appliance web interface, will generate a syslog event which can be redirected to a syslog server. Additionally, any configuration changes that are made to the appliance will also generate a syslog event showing the change that was made and by what user. If the syslog configuration itself is ever modified, it will result in an administrative email sent by the appliance to the configured administrative email account for the appliance.

Validation

To ensure the security and value of our product, Bomgar incorporates vulnerability scanning in our software testing process. We track the results of vulnerability scans performed prior to a software release and prioritize resolution based on severity and criticality of any issues uncovered. Should a critical or high-risk vulnerability surface after a software release, a subsequent maintenance version release addresses the vulnerability. Updated maintenance versions are distributed to our customers via the update manager interface within the Bomgar administrative interface. When necessary, Bomgar Support will contact customers directly, describing special procedures to follow to obtain an updated maintenance version. Currently, Bomgar conducts internal vulnerability assessments using tools from Qualys, McAfee, and IBM Rational App Scan.

In addition to internal scanning procedures, Bomgar contracts with Symantec for a source code level review as well as penetration testing. The source code review conducted essentially provides validation from a third party that coding best practices are followed and that proper controls are in place to protect against known vulnerabilities. Symantec follows up the review with a penetration test to confirm their findings.

Bomgar also offers distinct products that have successfully undergone FIPS 140-2 Level 2 certification. In order to receive this certification, the Bomgar software and the physical Bomgar hardware passed a rigorous review conducted by the National Institute of Standards and Technology.

Current FIPS Certified Hardware Version(s): B200, B300, B400

Current FIPS Certified Software Versions(s): 12.1.6FIPS, 13.1.3FIPS

Current FIPS Certified Firmware Version(s): 3.3.2FIPS, 3.4.0FIPS

NIST Certification for Bomgar Appliances: B200, B300, B400

NIST Certification for the Bomgar Cryptographic Engine algorithms:

- TDES
- AES
- SHA
- RNG
- RSA
- HMAC

All Bomgar Appliances, including the Virtual Appliance, make use of the same FIPS certified version of the Bomgar Cryptographic Engine that is available in the FIPS-validated appliances. The Bomgar Cryptographic Engine also supports additional, non-FIPS certified algorithms as well in order to support a broader array of potential encryption requirements.

All of the encryption algorithms included with a Bomgar Appliance can be enabled or disabled at your discretion. For information about Bomgar and FIPS, please see the appropriate Bomgar FIPS Security Policy.

About Bomgar

Bomgar is the leader in enterprise remote support solutions for easily and securely supporting computing systems and mobile devices. The company's appliance-based products help organizations improve tech support efficiency and performance by enabling them to securely support nearly any device or system, anywhere in the world — including Windows, Mac, Linux, iOS, Android, BlackBerry and more. More than 8,000 organizations across 65 countries have deployed Bomgar to rapidly improve customer satisfaction while dramatically reducing costs. Bomgar is privately held with offices in Jackson, Atlanta, Washington D.C., Paris, London and Singapore. You can find Bomgar on the web at www.bomgar.com.