BOMGAR™

The Bomgar Appliance and CJIS

TC:2/19/2015

Table of Contents

Overview

Bomgar is a comprehensive remote support solution using an appliance-based architecture that can enable organizations to maintain and comply with Criminal Justice Information Services (CJIS) mandated policies. The Bomgar appliance gives support technicians secure remote control of computers over the Internet or over the entire agency local networks.

Maintain Compliance

With Bomgar, a support technician can see the supported screen and control the supported system remotely as if physically present, all while maintaining compliance. Bomgar also enables streamlined third-party vendor access using a Bomgar feature referred to as Rep Invite. This enables agencies to eliminate requiring VPN access for outside vendors.

Support Systems

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.

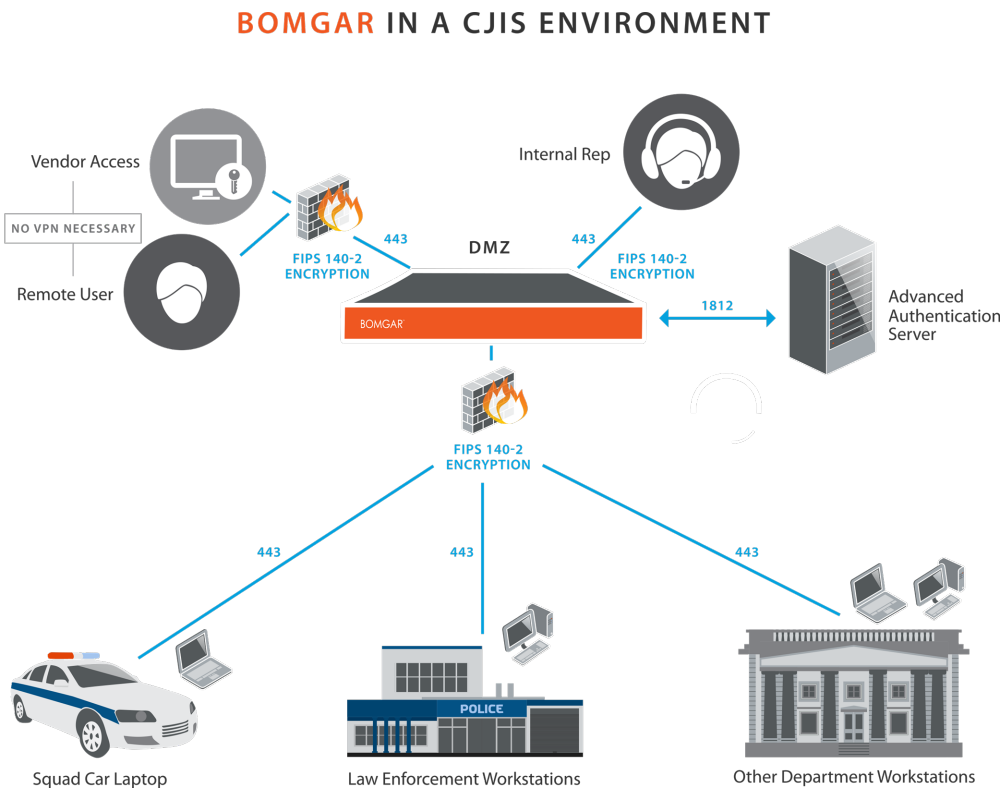
Access Anywhere

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 customer support portals hosted on a hardened appliance. Bomgar can match support requests with the appropriate technician/support representative or team. Bomgar then mediates connections between customers and technicians, 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

Using multiple features designed to ensure the security of remote support sessions, Bomgar integrates with existing advanced authentication identity management systems. This assists agencies in securing sensitive data by making sure that the technicians providing support have been validated properly. In addition Bomgar adds a layer of additional auditing capabilities via detailed session logs and video recordings of every support session conducted. Bomgar sessions are also encrypted in transmission using FIPS 140-2 compliant algorithms. The Rep Invite functionality can be carried out impromptu removing the need to create a service account over a FIPS-compliant VPN. An invited outside rep is actively monitored and controlled by an internal agency technician for the duration of the support session.

The following diagram was taken from the CJIS security policy and depicts where Bomgar would fit into a conceptual topology diagram for a law enforcement agency:



In the diagram above Bomgar would be located in the agency's DMZ. Bomgar uses the advanced authentication server to validate all technicians/reps. When supporting any end systems the session traffic is encrypted using FIPS-compliant encryption. Bomgar can be used to securely support all agency systems that are internal as well as external to the agency network. Also depicted in the diagram is the Bomgar Rep Invite feature. This Bomgar-specific functionality is applied to a third-party vendor coming in via the Internet, without requiring a VPN connection. This connection is also FIPS-compliant encrypted. The same concept can also be extended to employees who need to access internal systems while working remotely.

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 RADIUS which enables agencies to leverage their existing advanced authentication server. 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 LDAP. Each of these providers can be configured to use LDAP groups to set the permissions for the support technician, 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 technicians. These permissions determine what features in Bomgar a technician has access to, and can require end-user prompting so that the user receiving support must approve the actions of the technician or support representative. Additionally, a technician can be allowed view-only support access if the organizationally preferred permission is restricted to that level.

SSL/TLS

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 also can be configured to ensure that only FIPS 140-2 compliant algorithms are used.

Bomgar can natively generate CSR request using 2048 or 4096 bit RSA for the key length choices but also supports importing certificates generated off 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 also uniquely built for each customer and a unique encrypted license file is created that ensures all Bomgar clients are only valid for the site in which they are built. Additionally customer SSL certificates are built into the license file and must match the certificates being used on the Bomgar appliance.

Auditing

Bomgar provides two types of support session logging. All the events of an individual support session are logged to a text-based log. This log includes technicians involved, permissions granted by the customer, chat transcripts, system information, and any other actions taken by the Bomgar technician or support representative. This data is available on the appliance in an un-editable format for 90 days, but can be moved to an external database using the Bomgar Integration Client (IC). All sessions are assigned a unique session id referred to as an LSID. The session LSID is a 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 the ability to enable session recordings. This records the GUI of the customer screen for the entire support session. This recording contains metadata to also 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. As with the support session logging, these recordings can be moved to an external file store using the Bomgar IC.

Each Bomgar appliance model has differing amounts of available disk space but default is set to purge data over 90 days old. The Bomgar IC can be used to export data from the appliance and store it if needed to comply with security policies.

The Integration Client (IC) is a Windows application used to export reports, 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 ID. 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 technician/representative, or IP address.

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. Where necessary, Bomgar Technical 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.

Bomgar 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 very stringent review conducted by the National Institute of Standards and Technology.

- Current FIPS Certified Hardware Version(s): B200, B300, B300r1, B400, B400r1
- Current FIPS Certified Software Version(s): 10.6.2 FIPS, 12.1.6 FIPS, 13.1.3 FIPS
- Current FIPS Certified Firmware Version(s): 3.2.2 FIPS, 3.4.0 FIPS
- 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 running Bomgar Base software versions 3.2.2 - 3.4.0, including the Virtual Appliance, make use of the same FIPS-validated version of the Bomgar Cryptographic Engine that is available in the FIPS-validated appliances. The Bomgar Cryptographic Engine also supports additional, non-FIPS validated algorithms 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 8,500 organizations across 63 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.