BOMGAR™

Security in Bomgar Cloud Privileged Access

TC:1/30/2018

Table of Contents

Security in Bomgar Privileged Access (Cloud)

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 your organization stay secure and compliant, while improving the efficiency and success of your organization with a better user experience.

Bomgar Overview

Bomgar connects and protects people and technology with leading secure access solutions that strengthen security while increasing productivity. Bomgar Privileged Access lets you control access to critical systems without hindering the work privileged users need to perform. You can define how users connect, monitor sessions in real time, and record every session for a detailed audit trail.

Bomgar Privileged Access integrates with external user directories, such as LDAP, for secure user management. Bomgar also integrates with leading systems management and identity management solutions and includes an API for deeper integration.

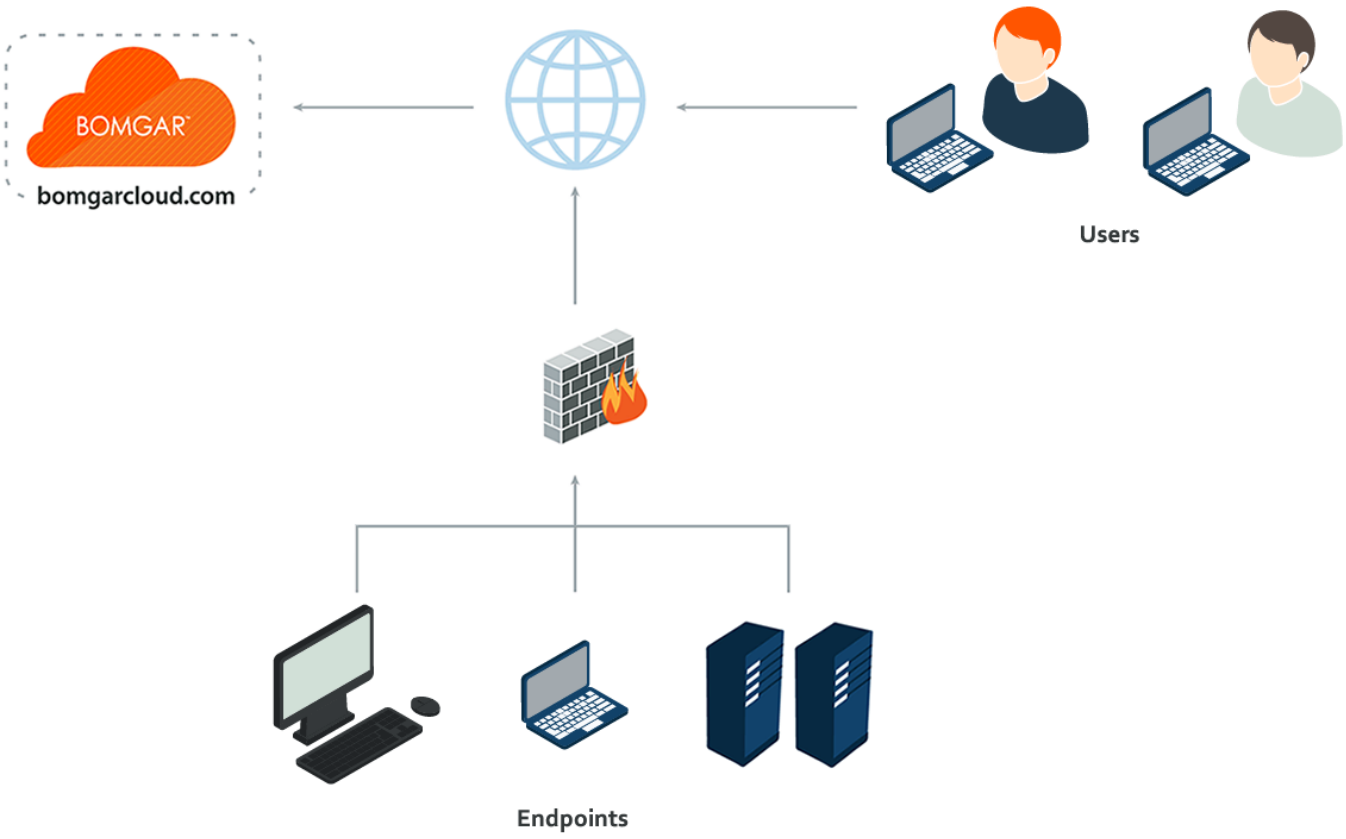
Bomgar enables remote access to multiple operating systems, including Windows, Mac, various Linux distributions, and mobile operating systems. Bomgar also enables remote control of various kinds of systems, including laptops, desktops, servers, kiosks, point-of-sale systems, smartphones, and network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

Bomgar mediates connections between users and remote systems, allowing file downloads/uploads, remote control of desktops, and access to system information and diagnostics, the command line, and the registry editor.

Architecture of Bomgar Privileged Access (Cloud)

Infrastructure

The Bomgar Cloud infrastructure is currently spread across six Tier 3 or higher data centers. Bomgar customers can designate a regional data center to host their Bomgar solution so that performance is not hindered by geographic distance between users of the solution. All data centers leverage advanced electrical and cooling systems and N+1 redundancy with uninterruptable power solutions and generator backup. The data centers have advanced networking capabilities such as 10Gb+ connectivity and a 40Gb+ core network.



Compliance

Data centers hosting the Bomgar Cloud have achieved ISO/IEC 27001 certification of its information security management systems. Additionally all data centers have completed the following examinations:

- SOC II Type 1
- SSAE 16
    - SOC 1 Type II
    - SOC 2 Type II

They are also Privacy Shield certified to meet European Data Privacy compliance regulations.

Physical Security

All Bomgar Cloud servers are housed in data centers that employ a high standard of physical protection. The measures include multiple levels of physical security, such as:

- Man traps / air lock
- Badged access
- Securely locked cages
- Biometric access
- Securely isolated storage area
- 24/7 security personnel on duty

Network Security

The network architecture is built to protect all entry points assigned to customers. Highly-available edge gateways and segmented network components are dedicated and configured in Bomgar. The infrastructure is continuously monitored, and vulnerability testing is conducted regularly by internal security staff.

Customer Data

All customer data is confined to a dedicated instance of Bomgar allocated to your organization. The data physically and logically resides in a siloed Bomgar instance and is not shared between customers. This unique approach to the segregation of customers keeps your data safe.

Authentication to Bomgar Privileged Access (Cloud)

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 user authentication using Kerberos or SAML (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 user, allowing you to map existing LDAP groups to teams in Bomgar.

There are a large number of granular permissions that can be granted to users. These permissions determine which features in Bomgar a user has access to.

Credential Management in Bomgar Privileged Access (Cloud)

Bomgar Privileged Access can be integrated with Bomgar Vault to improve password security for privileged users and vendors. Bomgar Vault helps companies secure, manage, and administer shared credentials and enables administrators to manage and rotate passwords for privileged accounts. Bomgar Vault provides credential management, secure password storage, password rotation, and credential discovery.

Bomgar Vault is deployed separately from the Bomgar Privileged Access instance and requires Windows 2012, 2012 RS, or 2016 operating systems, SQL Server, and Internet Information Services (ISS). An Endpoint Credential Manager (ECM) functions as the middleware for communication, and the ECM can be used to integrate Bomgar Privileged Access with other password vaults, such as Lieberman or Thycotic.

Credential injection is a built-in feature of Bomgar Privileged Access. It allows administrators and privileged users to seamlessly inject credentials into systems without exposing plain text passwords, and this feature can also be used with third-party vault tools. The Bomgar Vault solution rotates credentials, their associated services, and even groups or clusters of servers with the same credential at the same time - all without disrupting user productivity.

Bomgar Vault can be configured for high-availability and disaster recovery systems to ensure the system is always available. Bomgar Vault communications are encrypted and undergo regular penetration testing by both internal resources and verified third parties to ensure the highest level of security is maintained.

Encryption and Ports in Bomgar Privileged Access (Cloud)

Bomgar can be configured such that it enforces the use of SSL for every connection made to the site. Bomgar requires that the SSL certificate being used to encrypt the transport is valid.

Bomgar can natively generate certificate signing requests. Configuration options also are available to disable the use of TLSv1 and/or TLSv1.1. Bomgar always has TLSv1.2 enabled to ensure proper operation of the software. Available cipher suites can be enabled or disabled and reordered as needed to meet the needs of your organization.

The Bomgar software itself is uniquely built for each customer. As part of the build, an encrypted license file is generated that contains the site 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 Cloud site.

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

Below are example firewall rules for use with Bomgar Cloud, including port numbers, descriptions, and required rules.

Firewall Rules	
Internal Network to the Bomgar Cloud Instance	
TCP Port 443 (required)*	Used for all session traffic.
Bomgar Cloud Instance to the Internal Network	
TCP Port 25, 465, or 587 (optional)	Allows the appliance to send admin mail alerts. The port is set in SMTP configuration.
TCP Port 443 (optional)	Appliance to web services for outbound events.

Auditing of Bomgar Privileged Access (Cloud)

Bomgar provides two types of session logging. All the events of an individual session are logged as a text-based log. This log includes users involved, session tools used, chat transcripts, system information, and any other actions taken by the Bomgar user. This data is available on the appliance in an un-editable format for up to 90 days, but it can be moved to an external database using the Bomgar API or the Bomgar Integration Client. 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 enabling video session recordings. This records the visible user interface of the endpoint screen for the entire screen sharing 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 depends on the amount of session activity and the available storage, up to 90 days maximum. As with the session logging, these recordings can be moved to an external file store using the Bomgar API or the Bomgar Integration Client.

The Bomgar Integration Client can be used to export data from the site 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 uses the Bomgar API to export session logs, recordings, and backups from the Bomgar Cloud site 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 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 session data that must be retained for legal and compliance reasons. The reports and recordings are archived in a file system, indexed by 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, user, or IP address.

All authentication events, such as when a user logs into the access console or accesses the /login interface, generate a syslog event which can be logged on a syslog server. Additionally, any configuration change that is made to the Bomgar Cloud instance also generates a syslog event showing the change that was made and by which user.

Validation of Bomgar Privileged Access (Cloud)

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 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 contacts customers directly, describing special procedures to follow to obtain an updated maintenance version. Additionally, Bomgar Cloud instances may be automatically updated based on the update interval chosen by the customer at the time of purchase.

In addition to internal scanning procedures, Bomgar contracts with third-parties 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. A penetration test is conducted to confirm the findings.