

Making Virtual Support Secure

Remote Access and Control The Most Common Attack Pathway

Remote access and control technologies can have a powerful influence on productivity and efficiency. However, they can have a potentially destructive impact, as well. In its *2008 Data Breach Investigations Report*, the Verizon Business Risk Team named “remote access and control” the most common attack pathway used by hackers: “In over 40 percent of the breaches investigated during this study, an attacker gained unauthorized access to the victim via one of the many types of remote access and control software.”

Does this mean that remote access and control technology should not be used, or does it simply indicate that some solutions are less secure than others? The latter is more likely. Organizations that use technology to virtually access remote systems should make every effort to ensure the security of this very common attack pathway.

In over 40 percent of the breaches investigated during this study, an attacker gained unauthorized access to the victim via one of the many types of remote access and control software. [...] In many of these cases, the remote access account is configured with default settings, making the attacker's job all too easy.

2008 DATA BREACH
INVESTIGATIONS REPORT



What Makes Bomgar Secure?

As a solution for support virtualization, Bomgar enable support reps to access and control remote computers and systems. Bomgar has been successfully audited for security by Symantec Corporation and has taken a number of measures to ensure the security of the data transferred during support sessions. This document, though not comprehensive, outlines in the following categories some of the ways Bomgar can strengthen organizations' security and compliance posture:

- 1. Architecture**
Encrypting data is not enough. A remote access and control system must give support organizations control over sensitive data and visibility into virtual support activity. Bomgar's appliance-based architecture unifies support activity and collects all the data around support in a central repository.
- 2. Authentication**
Support reps should pass through multiple authentication layers or directory authentication before being given access to or control of a remote system. Bomgar gives administrators complete control over how individuals, teams, and even customers are authenticated without slowing down support.
- 3. Access**
Access should be tiered and permission-based at every level. Bomgar focuses on each end of the support session, offering granular user management to administrators and reassuring controls to customers.
- 4. Audit**
According to IDG, 67% of CIOs are unable “to ensure all remote interactions meet security and compliance requirements.” Bomgar's robust logging and recording capabilities capture exhaustive detail about support sessions and give administrators critical visibility into support activity.

Architecture

Before evaluating specific features of any particular remote access and control system, one must consider the overall architecture of the system. Bomgar's architecture is appliance-based, as opposed to the SaaS or Point-to-Point models. This appliance-based architecture lends built-in security to the support process.

On-site Deployment

Customers deploy the Bomgar's support appliance on-site, under the security measures already in place, and control physical access to the appliance. While the Bomgar Box is secure as an internet-facing device, customers also have the option of setting a WAN/LAN limitation on it. Both of these measures are impossible with a typical SaaS solution.

When deployed, the Bomgar Box does not compromise network security. Session traffic from the customer and the support representative is outbound to the Bomgar Box. This enables the solution to connect while corporate firewalls remain intact to provide a barrier to any potentially malicious traffic.

Furthermore, each Bomgar support session is initiated by the remote client when the support issue occurs and is then discontinued automatically when the session is complete, allowing only a small, irregular period of time wherein Bomgar traffic is crossing the internet. Spontaneously generating each support session obscures the entire support process from would-be hackers.

Secure, Encrypted Connection

Finally, all Bomgar user accounts, sessions and clients work through the Bomgar Box, which offers a high level of security within a managed environment.

- All traffic passing through the Bomgar Box is 256-bit AES SSL (Secure Socket Layer) encrypted along the entire datastream.
- The login pages for the Bomgar Box interface and user administrative interface are 256-bit AES SSL encrypted and password-protected, preventing unauthorized users from accessing representative or administrator accounts.
- All Bomgar clients use 256-bit AES SSL encryption. These include Jumpoint, Jump Client, LDAP and Integration Client.

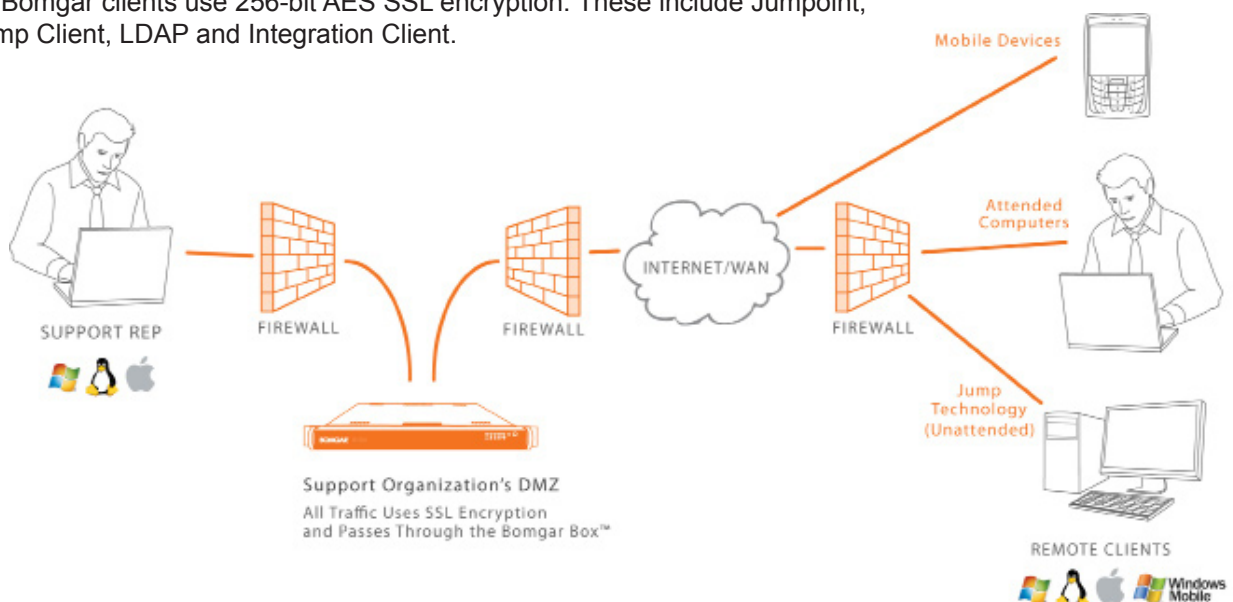
"Because we host the appliance internally, we save on monthly fees that an ASP [Application Service Provider] solution demands and we have full control over data security."
Operations Manager

PRACTICE PARTNER®
Part of **MCKESSON**

Bomgar has made support "more secure by putting all the technology in the customer's hands, not the service provider's."

Excerpt from article - *Top Ten Security Companies to Watch*

NETWORKWORLD®



Authentication

Bomgar administrators have a variety of options for prescribing how the Bomgar Box identifies and authenticates support reps and end-users. Administrators are also able to centrally manage support reps and administrators with security providers, set group policies, and oversee support rep activity in real time.

User Identification and Authentication

Bomgar administrators have the following settings around support rep passwords:

- Minimum password length: Require longer passwords
- Complex passwords: Require users to create a password with three of the four character classes
- Password expiration: Require reps to change passwords after a set time
- Password lockout: Prevent users from logging in after password attempts have failed a set number of times

The public support request page of the Bomgar Box has the option to display the names of logged-in representatives. Selecting a rep's name begins the steps to establish a remote connection. However, administrators can require sessions to be initiated via session keys -- single-use, complex codes generated by the Bomgar Box -- and set session key time out.

Security Providers

Administrators can configure the Bomgar Box to authenticate users against existing LDAP, RADIUS, or Kerberos servers, as well as to assign privileges based on the pre-existing hierarchy and group settings already specified in these servers. Kerberos enables single sign-on, while RSA and other multi-factor authentication mechanisms via RADIUS provide an additional level of security.

Group Policies

Bomgar enables administrators to set up groups of users who will share common privileges. Users may be assigned to a group from the local system or from configured security providers. Administrators can also apply individual settings [See next page] to entire groups to simplify the process.

Administrative Dashboard

Administrators or team leaders can oversee all support activities, viewing all current support sessions or drilling down to those of specific team members. Administrators can silently monitor a support session or view a support rep's entire desktop. Additionally, administrators or team leaders can transfer sessions on demand. The administrative dashboard provides increased support session management and enables administrators to intervene in support sessions if deemed necessary.

Bomgar gives administrators complete control over how individuals, teams, and even customers are authenticated without letting the process of authentication slow down support response times or hinder effectiveness.

Bomgar has been "designed and implemented with security best practices in mind."



"A company can have complete control over the appliance and make sure nothing else is on the server that can cause security risks."



"As the government becomes more security compliant, [Bomgar] continues to look better and better."

A Division of GSA



Access

Security during the support session is often more concerned with limiting access rather than enabling it. Solutions should not give complete control of the customer's system to the support rep when such control is neither necessary nor warranted. Access should be tiered and permission-based at every level.

Remote access and control through Bomgar is made secure in part by the architecture and authentication described previously. All session data, login pages and connection agents are 256-bit AES SSL encrypted and guarded by multiple authentication layers. But Bomgar also answers in-session security by focusing on each end of the support session, offering granular user management and reassuring customer controls.

Granular User Management

Administrators are able to grant and/or restrict support rep permissions on a granular level. Most of these permissions can be set with a series of simple check boxes and fields in the administrative interface. These individual permissions may also be applied to groups at large in the Group Policies section.

- Remote Control: Enable remote control or restrict to view only rights
- File Transfer: Turn on file transfer and specify file transfer paths
- Jump Technology: Define the use of Jump [remote access to unattended systems], including Jumpoint, Jump Client, and Jump on LAN
- System Info: Allow support reps to pull system info from remote systems
- Command Prompt: Permit support reps to connect to a remote computer via the command Prompt
- Presentation: Let support reps give presentations

These detailed user management capabilities allow administrators to assign the level of access appropriate to each rep. Reps in training can be limited, while seasoned rep are given access to all the powerful tools they need.

Reassuring Customer Controls

Bomgar also goes a long way to reassure customers who are receiving support through the Bomgar Box. All customer interaction is permission-based.

To begin with, support sessions are client-initiated. Then during the support session, customers are presented with a series of prompts whenever a support rep requests a broader level of control. These prompts include:

- Allow remote control or view only rights to the support rep
- Restrict remote access to specific applications
- File transfer allow/refuse notifications

Customers also maintain over-riding mouse control during the support session and see a "Stop Session" button prominently displayed. If a support rep is connecting to an unattended computer and has blanked out the screen, the customer is told how to override the screen blank.

Finally, when a support session is terminated, Bomgar completely uninstalls and the customer receives a message that the Bomgar customer client has been removed, preventing remote access unless support is requested again.

"... we needed to have control of the access and control of the logs of the access activity to minimize the number of parties that were involved."

IT Security Manager



The Bomgar Box "is more secure than hosted systems since the customer maintains control over the process."

InformationWeek

Free Online Resource:

Read Symantec's recommendations on the best way to securely deploy the Bomgar Box within your infrastructure.

Symantec's Secure Deployment Guide
[DOWNLOAD THIS DOCUMENT](#)



Audit

In the effort to ensure the security of remote access and control, many support organizations must satisfy the requirements set by federal compliance standards such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and others. These regulations set parameters around how organizations authenticate users, grant remote access, and ensure security during remote desktop support sessions. But ensuring compliance often consists as much in accounting for support activities as in securing them. Bomgar takes a number of steps to ensure a comprehensive audit trail.

Bomgar automatically logs granular details about every support session. The Bomgar Box can also track all administrative configuration changes via syslog. These logs may be exported from the Bomgar Box and archived in external databases. Administrators are able to report on support session logs and administrative configuration changes from the Bomgar Box.

Bomgar also retains flash video recordings of support sessions, annotated with details from the support session. Support session videos may also be exported to and stored in external databases. Recordings include videos of:

- Support sessions
- Support sessions via command prompt
- Presentations

These video recordings can be made available to customers and added as supplemental content to knowledgebase articles. The videos may also serve to augment the support organizations audit evidence.

Finally, Bomgar's appliance-based deployment makes it possible for support organizations to have full control over sensitive data. Unlike point-to-point solutions, an appliance-based approach centralizes support contact and, therefore, where support information is stored. And unlike software-as-a-service solutions, Bomgar prevents the routing of sensitive data through an external 3rd party.

It is unfortunate that too many support organizations are using remote access and control solutions that either provide an inadequate audit trail or store sensitive data with a third party. Support solutions that lack built-in logging and reporting mechanisms often make it impossible to verify how many support sessions occur, much less audit support activity. Bomgar offers support organizations clear visibility into support activities with comprehensive tracking and customizable reports.

67% of CIOs are not able "to ensure all remote interactions meet security and compliance requirements"



"[Bomgar] is providing a host of new features designed to help its customers better comply with corporate governance and privacy regulations."



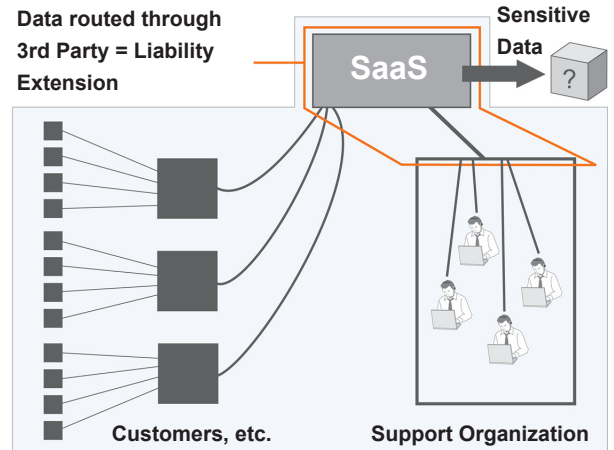
Conclusion

Ultimately support organizations can only secure what they can control. Bomgar helps to strengthen security by giving organizations more control over what happens at the service desk or help desk. This control includes not only the means of authentication, levels of access and details of an audit trail, but also the architectural storing and routing of sensitive data.

Bomgar's appliance-based architecture allows companies to avoid the liability-extending risks of routing sensitive data through a 3rd party's data center. It also eliminates the risks of point-to-point remote access by centralizing support management and reporting.

Remote access and control technologies constitute the most common path of attack for hackers. Bomgar's comprehensive approach to security is a strong deterrent for hackers, and helps support organizations guard themselves and their customers.

Service-based Remote Access



Point-to-Point Remote Access

