



**Bomgar**

Product Penetration Test

December 2008

**Table of Contents**

**Introduction ..... 1**

**Executive Summary..... 1**

**Bomgar Application Environment Overview ..... 1**

**Bomgar Security Architecture ..... 2**

**About Bomgar ..... 5**

## Introduction

During the period of August through December 2008, Symantec Global Consulting Services partnered with Bomgar to assess the security architecture and implementation of the Bomgar Box™ appliance. During the engagement, Symantec performed a Product Penetration Assessment to evaluate the application components and related environment against established security best practices.

A product penetration assessment is designed to provide insight into methods of attack against a specific product or suite of applications and present a reasonable example of what an attacker might accomplish. The assessment concentrates on modeling specific attack scenarios, identifying vulnerabilities, and validating exploitation possibilities.

## Executive Summary

Symantec conducted this Product Penetration Assessment to evaluate the security architecture of the Bomgar Box™ appliance and identify security vulnerabilities that might pose risk to Bomgar's customers. The purpose of this test was to ascertain the security posture of the targeted product from a hacker's or a malicious user's perspective and determine what, if any, resources could be compromised through attacks on confidentiality, integrity, or availability.

During the assessment, Symantec found the overall architecture of the Bomgar Box™ appliance to be designed and implemented with security best practices in mind. It should be noted that testing was performed against a Bomgar Box™ appliance with product version 10 installed.

## Bomgar Application Environment Overview

The Bomgar application environment is a multi-tier hardware and software environment consisting of the following different components:

- The Bomgar Box™ appliance: The Bomgar Box™ appliance is a dedicated hardware device that supports Bomgar's application server components and administrative interfaces and acts as a centralized routing interface for all application communications.
- Bomgar Representative Client: The Bomgar Representative Client is used by support desk representatives to remotely access customer workstations and perform chat, file transfer, and remote management operations.
- Bomgar Customer Client: The customer client is a small executable that is installed only for the duration of a support session and enables the support representative to gain remote access to the customer's workstation. Upon termination of the session, the program automatically uninstalls.

## **Bomgar Security Architecture**

During the assessment, Symantec identified aspects of Bomgar's security architecture that offer protection against a variety of threats that exist within this type of application architecture.

### **1. A Dedicated Hardware Appliance**

By default, the Bomgar Box™ ships as a self-contained, hardened application server appliance. In order to ensure that the installed versions of server components remain up-to-date with respect to possible security issues, the Bomgar Box™ appliance architecture supports functionality to allow an administrator to conduct a full update of critical service components deployed.

Symantec conducted port scans of the Bomgar Box™ and found that only three network ports were enabled and responsive in the default configuration. An evaluation of the server configuration revealed that the Bomgar Box™ ships with extraneous network services disabled, limiting network connectivity to HTTP (TCP 80) and HTTPS (TCP 443) ports and an alternative HTTPS port (TCP 8200). During testing, the limited exposure of network services successfully prevented access to the network interfaces of other server components.

Additionally, access to the administration interface for the Bomgar Box™ occurs over an encrypted web connection and can be restricted to the local console port and/or a specified network segment. This protects against a remote attacker with network access to the appliance gaining unauthorized access to administration functions.

Symantec found that operating system layer vulnerabilities were sufficiently mitigated by compensating controls that limited possible attack vectors.

### **2. Server-side Authentication and Authorization**

All Bomgar application servers use dedicated application accounts when accessing server functionality and data. During the assessment, Symantec conducted a variety of attack scenarios designed to circumvent the authentication mechanisms implemented in the Bomgar Box™. Symantec found that both the web-based and client-server interfaces to the Bomgar Box™'s back-end components required the user to successfully authenticate with a valid username and password. All attempts to bypass the authentication components were rejected by the application, thereby preventing access to functionality and data on the server.

Symantec also found that the Bomgar Box™ supports per-user privileges that offer more granular control over access to application functionality and data. When accounts are created, the administrator is presented with a list of privileges that can be selectively granted to the user, including the ability to view and/or control a customer's machine remotely or the ability to act as an administrator for the application. During the assessment, Symantec also attempted to bypass

access control functions and access functions and/or data that should have been restricted to more highly-privileged users. These attempts were rejected by the access control mechanisms built into the application. Finally, Symantec also notes that separate administration accounts and interfaces exist to govern administration of the Bomgar Box™ and the administration of the application itself. This provides additional segregation between user functions within the overall application environment.

### **3. Communications Encryption**

The architecture of the Bomgar application environment relies on the Bomgar Box™ application as a centralized routing point for all communications between application components. All Bomgar Box™ sessions between representatives and remote customers occur through the server components that run on the Bomgar Box™ appliance. Data transmitted during these sessions includes customer screen data back to the representative and, in some cases, commands from the representative that result in remote control of the customer's workstation.

To protect the integrity of the customer's screen data and prevent unauthorized eavesdropping and/or modification of application data in transit, Bomgar uses 256 bit SSL to encrypt all application communications in transit. The default installation of an application server contains a pre-generated SSL server certificate to support data encryption upon initial use. However, administrators of a Bomgar application may also create and deploy their own certificates. It is strongly recommended that customers generate and install a verifiable certificate in order to establish a valid trust relationship with clients. The security of the system, from the client perspective, is predicated on the integrity of the downloaded and installed Customer Client binary. For a client to assign appropriate trust to the binary, it has to be downloaded from a trusted source. A verifiable certificate, signed by a trusted authority, authenticates the server to the client and allows the client to make that reasonable trust assignment.

In addition to encrypting data in transit, the 256 bit SSL architecture also protects application users against the threat of a man-in-the-middle attack or the deployment of a rogue application server. In a normal configuration, application clients validate the certificate presented by the server during SSL negotiation. Symantec observed that the presence of an invalid or untrusted certificate on the server will cause the Customer Client to terminate the connection and report an error to the user.

The Bomgar Box™ ships with SSL version 2 disabled by default and provides an administrative interface to optionally enable it. The SSLv2 protocol contains design flaws and is generally considered insecure. Modern browsers support SSLv3 and TLSv1 and will not be adversely affected by the absence of SSLv2.

### **4. Application Client Security**

Bomgar requires customers receiving support in Bomgar Box™ sessions to initiate the deployment of a customer client on a workstation. During a typical support session, the remote customer must download and run a small executable that will establish a connection through the Bomgar Box™ and allow the support representative to access the customer workstation. During the installation of the customer client, the customer can choose whether or not the support representative can simply view the screen or obtain full control. The customer is also given the option to discontinue the installation and delete the client.

Once a support session terminates, the client executable automatically terminates running processes related to the support session and uninstalls itself from the customer's workstation. Any subsequent support sessions will require the customer to rerun the installation process in order to deploy the customer client again on their workstation.

During the penetration test, Symantec noted that the access controls afforded to remote customers sufficiently restrict access to their workstation. Symantec was unable to obtain control over customer machines that were granted only viewing privileges and was not able to resume a support session once the session had been terminated and the client uninstalled. Furthermore, during sessions which did provide remote control of the customer's workstation, Symantec found that the remote customer could regain control of the workstation and terminate the connection at any time during the session.

### **About Bomgar**

Bomgar Corporation's mission is to change the way work is done. Through support virtualization, Bomgar works to free the tech support community from the restraints of access barriers and geography, and from the inefficiency of traditional phone-based and on-site support. Support virtualization makes support more responsive, efficient and secure by removing the geographical and technological barriers between customers and those supporting them.

To learn more about Bomgar, visit them online at: <http://www.bomgar.com/>

## About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free (800) 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec makes this document available for informational purposes only. It may not reflect the most current legal developments, and Symantec does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to the opinions expressed herein. Changing circumstances may change the accuracy of the content herein. The information contained herein is not intended to constitute legal advice nor should it be used as a substitute for specific legal advice from a licensed attorney. This report makes no representations or warranties of any kind regarding the security of Bomgar Corporation or forward-looking statements regarding the effects of future events. You should not act (or refrain from acting) based upon information herein without obtaining professional advice regarding your particular facts and circumstances. Opinions presented in this document reflect judgment at the time of publication and are subject to change. While every precaution has been taken in the preparation of this document, Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of the information herein."

"Reproduction guidelines: You may make copies of this document unless otherwise noted. If you quote or reference this document, you must appropriately attribute the contents and authorship to Symantec. Symantec and the Symantec logo are trademarks or registered trademarks, in the United States and certain other countries, of Symantec Corporation. Additional company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged."

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s.