

BOMGAR™



USING BOMGAR FOR
SECURE VENDOR
ACCESS MANAGEMENT

Using Bomgar for Secure Vendor Access Management

The Problem of Vendor Access

Your IT infrastructure requires remote support from numerous technology vendors. In a large company, hundreds or even thousands of vendor technicians may require periodic remote access to application servers, network devices, or user's desktops. This constant flow of vendor remote access is essential in order to keep your infrastructure functioning properly. But it can also be a threat to your organization's security, undermining your efforts to maintain regulatory compliance. Most current products for remote access:

- Do not allow granular security settings
- Do not provide a comprehensive audit trail
- Do not support all operating systems and scenarios

The 2008 and 2009 Data Breach Investigations Reports by the Verizon Business RISK team found that, ***"In approximately four of 10 hacking-related breaches, an attacker gained unauthorized access to the victim via one of the many types of remote access and management software. [. . .] Rather than for internal usage, most of these connections were provisioned to third parties in order to remotely administer systems."***¹

The investigation indicates that at least 2 out of every 10 breaches were the direct result vendor remote access that was not secure. Clearly, this is an area that requires closer scrutiny. Problems with secure vendor access abound:

No Granular Permissions

The principle of least privilege suggests that an employee should not be given access that exceeds what is required for his or her job function. This principle is especially applicable in dealing with vendors, where every degree of access beyond what is required exposes your organization to excess risk. For instance, if a vendor has access to a billing system while servicing a CRM application, then the corporation must account for all potential actions performed on either system regardless of the vendor's actual task.

A combination of VPNs plus point-to-point remote control tools forms the backbone of vendor remote access in many organizations. This combination gives your vendors access to a range of internal systems but does almost nothing to enforce the principle of least privilege. Many remote control tools require the tunnel to be turned either ON or OFF, without distinguishing between types or levels of access. This lack of granularity means that granting a vendor remote access often means you are

1. Granting more access than the job requires and
2. Denying a vendor access must be done wholesale, without consideration for what level of access might be acceptable.

No Audit Trail

Controlling access to your corporation's data and systems is only half of the vendor access equation. Even if you can establish authenticated, granular remote access pathways for your vendors to follow, you still cannot eliminate misuse of authorized access.

For instance, a vendor may require remote access to the CRM application in order to do data cleanup, but then use that access to steal customer records. A complete audit trail of vendor remote access is the essential counterpart to granular permissions.

However, most tools used for vendor remote access only support basic, event-level logging. Many offer no logging at all. Beyond simply recording that a remote access session took place and perhaps who performed the session, a record of what happened during the session is essential. Without this level of data, you may audit activity, but you can make no determination about whether the activity was within acceptable parameters.

Enterprise-Wide Support

Even if vendor remote access is controlled at a granular level with a complete audit trail, its value is proportionate to the scenarios in which it can be used. Many solutions for vendor remote access support only a limited range of operating systems and configurations, thus requiring the use of other limited solutions for the remaining gaps. This patchwork approach to vendor access only aggravates the security problems of control and audit-ability. If one solution is hard to manage effectively, then five is impossible.

In addition to the standard operating systems and configurations, it may be necessary to support a full range of specialized systems across numerous network configurations. Receiving vendor technical support for the extended enterprise may involve many of these scenarios:

Support for

- Systems both inside and outside the firewall
- Both attended and unattended systems
- Smartphones
- Windows, Mac, and Linux operating systems
(Sometimes multiple versions or distributions)
- Network Devices
(Supported through SSH and telnet)

Conclusion

Vendor remote access requires special consideration due to its inherent security risks and crucial role in ensuring the availability of your IT infrastructure. Current tools provide a partial solution, often introducing security risks and failing to address many non-standard operating systems and configurations.

Using Bomgar for Secure Vendor Access Management

As a solution for vendor access, Bomgar addresses the crucial security requirements of granular permissions and a complete audit trail within a consolidated solution that supports a wide array of operating systems and configurations. Bomgar acts as a centralized proxy for vendor activity throughout your enterprise, without the need to deploy hardware to every network segment.



Secure Vendor Access

Administrator can control vendors' access to the network using Bomgar's Embassy™ and Rep Invite technologies. After adding vendor accounts to the Embassy, or determining privileges for invited reps, the admin can assign security parameters, define which systems can be accessed, and manage vendor settings and permissions. Some of these parameters include:

- Whether file transfer is enabled – and if so, which directions
- Whether a vendor rep can share a session with your internal support staff
- Whether the vendor's access enables full remote control or view only
- Whether the vendor must request application-specific control from the end-user



Complete Audit Trail

The Bomgar administrator can monitor and report on all vendor activity through Bomgar historically or in real time. Video recordings of every remote support session enable the administrator to audit every click and keystroke of every vendor technician. Bomgar logs:

- Which vendor rep accessed which system
- When the access took place and how long it lasted
- What happened during each session (files transferred, settings changed, screen sharing, command line sessions, chats with the user, etc.)



A Consolidated Solution

Bomgar enables your vendors to support any of your systems, whether a Mac laptop on a WiFi hotspot or an unattended Linux server. In addition to computers, Bomgar also enables remote support of BlackBerry and Windows Mobile smartphones and remote access to command line driven network devices. With Bomgar, you can give your vendors access to:

- Windows 95 - Windows 7
- Mac 10.4 and 10.5
- Multiple Linux distros, including Ubuntu, Red Hat, Fedora, and SUSE Linux
- BlackBerry and Windows Mobile Handhelds
- Network Devices (SSH and Telnet)
- Systems both inside and outside the firewall
- Both attended and unattended systems

Bomgar's breadth of system support eliminates the need for multiple access solutions, increasing manageability along with security. And Bomgar can be used by your internal support staff as well as your vendors, enabling you to remotely support your entire organization with one secure solution.