

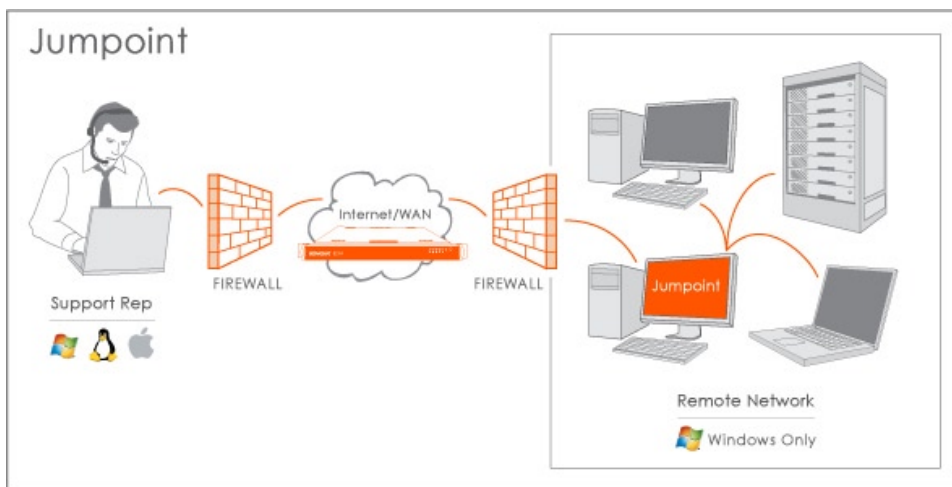
Introduction to Jump™ Technology

Jump™ Technology is Bomgar's patent-pending solution for accessing unattended remote computers and servers. With Jump™, virtual support technicians can access and control unattended remote systems through firewalls.

How Jump™ Technology Works

Bomgar's Jump™ Technology includes two methods for remote access, Jumpoint™ and Jump™ Client.

A **Jumpoint™** is an agent within a remote network that enables virtual access to all Windows computers within that network. A Jumpoint™ lets administrators troubleshoot all the Windows systems within a network without deploying virtual access software on each system prior to connecting.



Jumpoint™

When to Use:

When accessing networked Windows systems

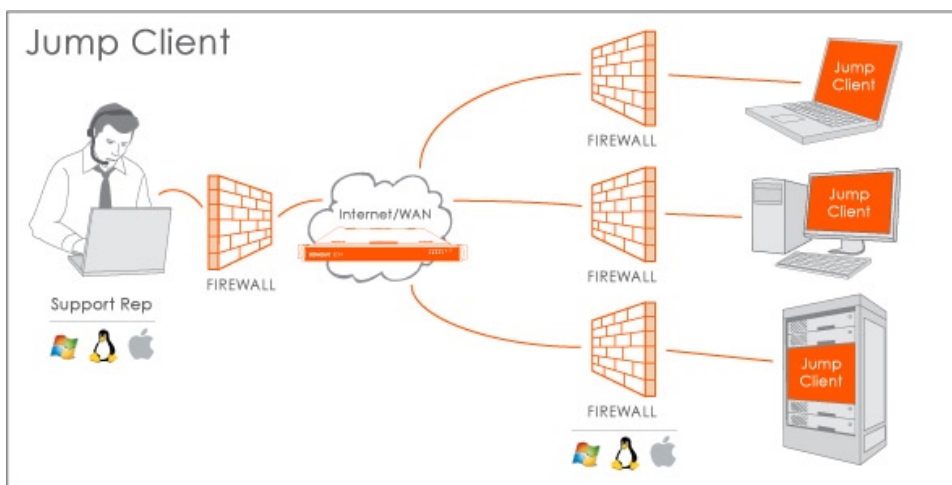
Requirement:

Installation of Jumpoint within a LAN; Windows Only

How to Deploy Jumpoint:

Download a Jumpoint agent onto a single computer or server on a remote network

A **Jump™ Client** is a pre-installed software client that enables virtual access to unattended Windows, Mac or Linux computers. Jump™ Clients allow support technicians to work virtually on any remote system, regardless of its network location or operating system.



Jump™ Client

When to Use:

When accessing unattended Windows, Mac or Linux systems in any network

Requirement:

Installation of a Jump Client on each remote computer

How to Deploy Jump Clients:

Mass deploy or install during a support session

Licensing for Jump™ Technology

Jump™ Technology is core to Bomgar's software and is included in all license offerings. It is a Bomgar feature, not a Bomgar product. While administrators may set limits on the use of Jump™ Technology, it is possible for each licensed technician to use Jump™ on an **unlimited number of remote systems**. Rather than calculating how many systems need support or the potential duration of support calls, support organizations simply need to consider how many support technicians need to be working concurrently.

Secure Virtual Access with Jump™ Technology

Support organizations and those they serve do well to investigate the security of the remote access and control technologies used in their environments. Two recent reports emphasize this necessity:

- The Verizon Business "2008 Data Breach Investigations Report," remote access and control technologies as **the most common pathway for attacks and data breaches**, involved in more than **40% of the cases**. The report covers four years of forensic research and more than 500 cases.
- "The New Service Desk," published in 2008 by CIO.com [an IDG subsidiary], notes that **67% of CIOs** are not able "to ensure all remote interactions meet security and compliance requirements."

What Makes Jump™ Technology Secure?

As a solution for support virtualization, Bomgar enables support reps to access and control remote computers and systems. Bomgar has been successfully audited for security by Symantec Corporation and has taken measures to ensure the security of the data transferred during support sessions. Below are some of the ways Bomgar can strengthen organizations' security and compliance posture:

On-site Deployment

Each Jump-enabled support session passes through the Bomgar Box™, which customers deploy on-site, under the security measures already in place. Customers control physical access to the Bomgar Box. While the Bomgar Box is secure as an internet-facing device, customers may set a WAN/LAN limitation on it. The Bomgar Box helps make Jump™ Technology more secure than traditional remote access methods, which use always-on, port-listening clients that can be hacked by password-guessing.

Encrypted Connection

Bomgar guards the entire data stream with strong encryption. All Jump™ Technology sessions, user accounts, and clients use 256-bit AES SSL encryption.

User Authentication

Bomgar administrators have a variety of options for prescribing how the Bomgar Box identifies and authenticates support reps and end-users. Administrators can centrally manage support reps and administrators with security providers [RADIUS, LDAP, Kerberos], set group policies, and oversee support rep activity in real time. This ensures only authorized users can use Jump™ Technology for virtual access.

Granular User Management

Administrators are able to grant and/or restrict support rep permissions on a granular level. This includes whether and how support reps use Jump™ Technology. Bomgar's detailed user management capabilities allow administrators to assign the level of access appropriate to each rep.

Customer Controls

Bomgar also goes a long way to reassure customers who are receiving support with Jump™ Technology. All customer interaction is permission-based at every level.

Audit Capabilities

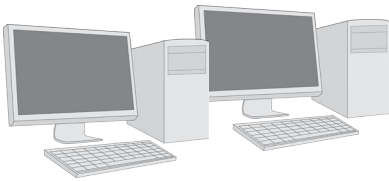
Bomgar offers support organizations clear visibility into Jump™ sessions with comprehensive tracking, customizable reports, and video-recorded support sessions. Maintain a detailed, automated audit trail for easier compliance with Gramm-Leach-Bliley, HIPAA, Sarbanes-Oxley, PCI or other requirements.

Some Applications for Jump™ Technology



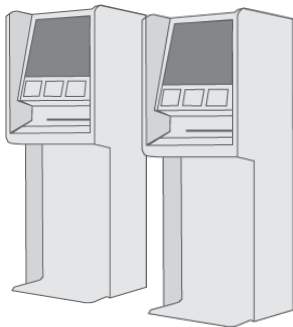
Servers

Use Bomgar's Jump™ Technology to access and maintain remote servers. Rather than licensing remote access on a per-computer basis, Bomgar includes unlimited virtual access as a feature of every license. Jump™ enables organizations to scale virtual support capacity from a few servers to an entire data center or server farm.



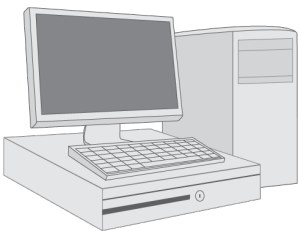
Desktop Support

Maintaining a stable desktop environment is one way IT moves the business forward. Bomgar's Jump™ Technology streamlines remote desktop support. Without traveling to branch offices, shipping systems back and forth for repairs or even walking down the hall, support staff can access and troubleshoot unattended remote desktops. Jump™ helps keep end-users productive and focused on the business.



Terminals

ATMs, terminals and other unattended, customer-facing systems are vital to your organization, so keeping them up and running is critical. Jump™ Technology cuts time to resolution whenever an unattended system experiences a problem. Without hindering PCI compliance, Jump™ allows you to access problem systems virtually rather than physically.



Point of Sale Systems

Instead of deploying technical staff to each store location when an incident arises, Bomgar's Jump™ Technology allows virtual access to point of sale systems. This reduces business interruptions, lowers the cost to provide support, and reduces frustration on both ends of the phone whenever supporting a non-technical end-user, all while satisfying industry compliance requirements such as PCI.



Vendor Access

Bomgar makes it easier to control and monitor vendors' access to the applications and systems in your organization that need support. Instead of giving vendors unmonitored access to your entire network, Bomgar's Jump™ Technology lets you:

- Specify which systems vendors may access,
- Define the credentials necessary for access, and
- Monitor and audit what vendors do when they have access.