



## **Why Consolidate Remote Support**

*Problems of Using Multiple Remote Control Tools for Support*

# Consolidating Remote Support

## Why More is Not Better

Almost every support center and IT department uses remote support. For most organizations, the question is not whether it uses remote support tools, but how many tools it uses. Five to ten different tools is common; for large IT outsourcers, the number may be closer to twenty.

The reasons are also multiple. The most common answer is that the organization added remote control tools as they were needed . . . in other words, without a clear strategy. An audit of the remote support tools in your organization will, in all likelihood, reveal different tools used for:

- **Support inside & outside the firewall**
- **Support of servers and workstations**
- **Support of network devices (switches, routers, etc.)**
- **Support of Windows, Linux, and Mac systems**
- **Support of Handheld Devices like BlackBerry and Windows Mobile**
- **Support from External Vendors**

Unfortunately, a break/fix approach to remote support tools is likely to break more than it fixes. Support organizations do more than resolve incidents. They must establish best practices, integrate with other parts of the organization and maintain compliance with PCI, SOX, HIPAA, GLBA, FIPS, FDCC or other of myriad regulations.

In the absence of a strategic long-term view, the multi-product "remote support solution" is proving difficult to sustain. Multiple remote support tools create problems around integration, security and cost.

## Multiplying Expenses

Rather than reducing costs, deploying multiple products often increases them. A cursory examination of the remote support products deployed will immediately reveal a significant amount of overlap. Companies often pay for products with 80 percent overlap just to get the missing 20 percent.

***"Support centers will be tasked to support more platforms and applications, usually without a corresponding increase in staff."***

The Support Center in 2011  
A Report on the Future Trends Facing the Support Industry  
Help Desk Institute

## (Continued: Multiplying Expenses)

Yet there are still gaps in support! With the uptick in mobility, non-standard support scenarios increase. As they do, technicians are tempted to stitch another tool into the mix each time they encounter an incident in which the old standby fails. For example, incidents involving:

- **Non-Windows operating systems**
- **Users outside the corporate firewall**
- **Users on unmanaged PCs**

Because the current tools fail to work in non-standard situations, many users must endure phone support, wait for an on-site support call or bring their problem computers into the office to get the help they need.

But what if the tools the organization is using are free? "Free" is often expensive in other ways. Free tools fall short on security and integration, areas that, as we shall see in the next sections, carry very high costs.

## Multiplying Risk

In 2009, the Verizon Business RISK Team updated its Data Breach Investigations Report, which drew "from over 500 forensic engagements handled by the Verizon Business Investigative Response team over a four-year period."

***"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."***

2009 Data Breach Investigations Report  
Verizon Business RISK Team

The Verizon report revealed that remote control technology was the most common attack pathway, accounting for roughly forty percent of the data breaches.

This data is not surprising when one considers that most companies would have a difficult time even identifying how many remote support sessions took place during a specific period of time, much less what happened during them. Here again, multi-tool approach to closing the gaps in support can create numerous, critical security problems.

### (Continued: Multiplying Risk)

In fact, the use of multiple tools for remote support creates security problems before an incident ever begins. Almost none of the legacy remote control tools are able to integrate with identity management mechanisms such as LDAP or RADIUS; therefore, guarding who has access to the tools is a manual exercise.

The few Software as a Service (SaaS) remote support tools that do allow LDAP integration require the company to give an external third party access to its internal user directory.

Furthermore, most remote support tools have no logging, reporting or other auditing capabilities, and since the ones that do are only partial solutions, the audit trail is never complete. The result is not just an incomplete record of support activity, but an inaccessible one, since logs of varying detail and format must be aggregated and synchronized from multiple data silos.

Ultimately, when a company has no centralized management of remote control technology, more tools just create more security holes. And when a company is blind in respect to support activity, it cannot see the security holes it does have – until after a breach has occurred.

### Multiplying Inefficiency

The difficulty of integrating multiple remote support tools hinders productivity and efficiency. For example, most remote support tools have no service desk integration. Besides service desk integration, most remote control tools lack the ability to integrate with CRM systems, knowledgebase repositories, identity management protocols, file systems, external databases, online support portals or web-based chat support.

***“... Legacy, location-based desktop support tools are not flexible, scalable or manageable enough to support the shift to anywhere, anytime business.”***

The New Service Desk  
CXO Media

Even if every one of a company's remote support tools included robust integration capabilities, trying to tie them all into a single process would be daunting. This lack of integration leaves critical gaps in the support process.

### (Continued: Multiplying Inefficiency)

The results are clear: Productivity suffers from manual processes that do not scale cost effectively. Customer satisfaction suffers from long hold times and low first call resolution. And security suffers from poor access management and weak auditing capabilities.

But these problems are only the beginning. When remote support is not an integrated part of the support process, more critical issues begin to surface:

- **Low staff utilization**
- **Low 1st call resolution**
- **Long incident handling**
- **Needless on-site visits**
- **High call escalation**
- **Low customer satisfaction**

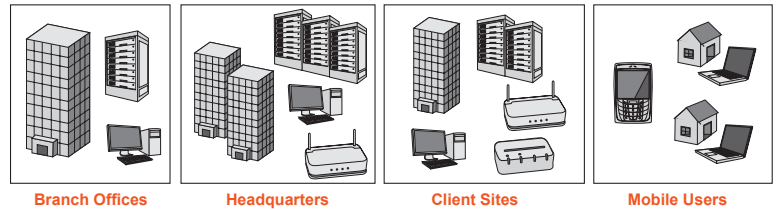
The piecemeal approach to remote support is unsustainable. It is costly, unsecure and unmanageable. A new approach is needed that allows support organizations to consolidate all the remote support functions with one tool.

# Consolidating Remote Support with Bomgar

Bomgar enables remote support consolidation by addressing with one secure, on-premise, appliance-based solution what many companies attempt to address with ten or more tools.

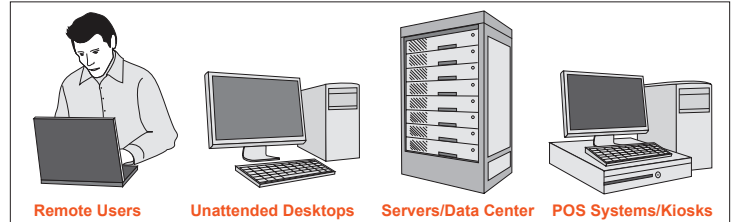
## Support inside & outside the firewall

Bomgar is firewall compatible, enabling technicians to support anyone, anywhere.



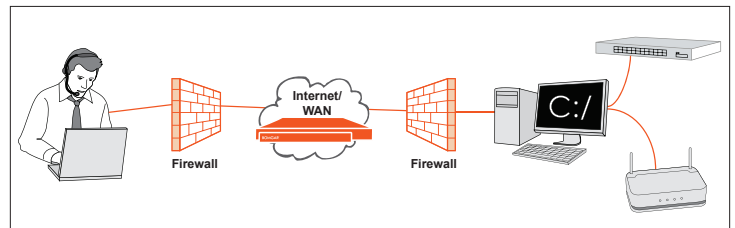
## Support of servers and workstations

Bomgar enables support for both unattended and attended systems, both the laptop user on wireless and the server in the back room.



## Support of network devices

Bomgar enables support of network devices using SSH or Telnet. This means technicians can troubleshoot environmental issues affecting remote computers.



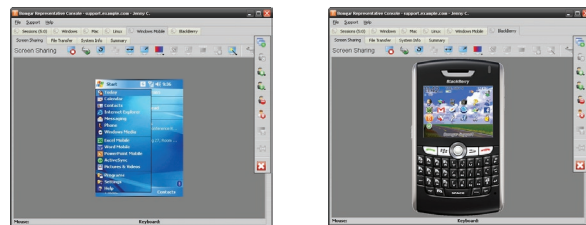
## Support of Mac, Windows and Linux systems

Bomgar supports Windows 95 – Vista, Mac 10.4 and up, and four common distributions of Linux: Fedora, Ubuntu, CentOS, and SUSE Linux Enterprise Desktop 10.



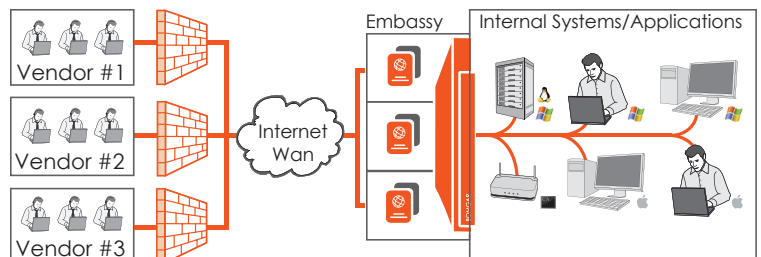
## Support of Handheld Devices

Bomgar supports Blackberry and Windows Mobile, enabling a technician to remote control smartphones.



## Support from External Vendors

Bomgar's Embassy feature is a robust functionality for vendor access that makes receiving support as easy as giving it.



## Bomgar Reduces Costs

Consolidating remote support with Bomgar reduces costs. By using one product, a support organization eliminates the cost of overlapping maintenance on products that are 80% redundant.

Bomgar also makes non-standard support scenarios a thing of the past. Technicians are simply able to connect to the end-user, wherever he may be working or whatever platform he may be using.

Technicians no longer waste time trying to decide which tool to use. And much of the time once spent installing, maintaining, or managing multiple tools can now be used resolving incidents. The time and maintenance savings often result in an ROI after only a few months.

## Bomgar Increases Security

Consolidating remote support with Bomgar increases security. Bomgar integrates with identity management protocols and external security providers (LDAP, Kerberos and RADIUS) to control authentication. Administrators have granular control over access to the remote support software

With Bomgar, administrators can set rules governing support interaction on a per-customer, a per-rep, or a per-team basis. This lets support organizations meet the compliance demands for all customers, even if what constitutes compliance differs per customer.

Every Bomgar session is logged and audit-able, creating a central repository for all remote support activity. The administrator has the ability to review every click and keystroke from every session within the organization.

Logs and videos of support sessions are not only thorough, but accessible for auditing purposes and root cause analysis. And since Bomgar is an on-premise appliance, you never have to worry about sensitive data being routed or stored outside your company.

## Contact Information

Email: [sales@bomgar.com](mailto:sales@bomgar.com)  
Toll Free: 877.826.6427  
Direct: 601.519.0123

## Bomgar Improves Efficiency.

Bomgar includes out-of-the-box integrations with HP and BMC service desk solutions, and a robust API/SDK. With Bomgar companies can approach the support process strategically, leveraging existing infrastructure and creating a seamless support workflow.

A customer who has exhausted self-help can begin a secure chat session with a support representative, open a service ticket, escalate to a remote control session, then complete a post session survey. Every detail is then recorded and associated with the specific ticket.

The results are clear. With Bomgar, companies have...

- **Increased Staff Utilization by 70-100**
- **Increased 1st Call Resolution by 35-45%**
- **Decreased Incident Handling Time by 25-50**
- **Decreased On-Site Visits by up to 90%**
- **Decreased Call Escalation by 10-30%**
- **Increased Customer Satisfaction by 10%**

## About Bomgar Corporation

Bomgar is a solution for enterprise remote support, that makes support more responsive, efficient and secure. Bomgar's appliance-base solutions integrate easily into your existing environment to ensure the quality and security of every support interaction. Bomgar helps you:

- **Support every system from one screen**
- **Resolve more incidents in 1st tier**
- **Automate audit trail**
- **Decrease on-site visits**

Since 2003, over 5,000 corporate customers in all 50 states and 52 countries have chosen Bomgar for remote support. Leading industry analysts and consultants recognize Bomgar as a technology innovator.

# BOMGAR™