SECURE REMOTE ACCESS FOR THIRD-PARTIES

BOMGAR™

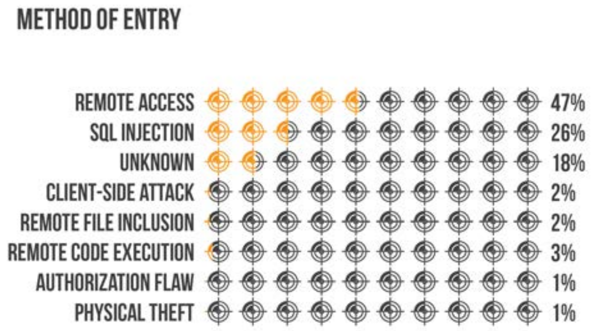
SECURE REMOTE ACCESS FOR THIRD-PARTIES

In many organisations, a significant number of external technicians may require periodic remote access to application servers, network devices, or users' desktops. This constant flow of vendor access is necessary to keep your infrastructure functioning properly, and to provide application development and support, as well as allowing for crisis management.

Vendor access can also, however, be a threat to your organisation's security and undermine your efforts to maintain regulatory compliance. Many vendors use VPN and point-to-point remote control technologies to connect to their clients' systems. These connections typically allow "all or nothing" access to a network and are often unauditable. As a result, you have multiple vendors with an always-on connection to your most mission-critical systems without any way of controlling their access levels or auditing their activity.

According to the Trustwave 2013 Global Security Report, "*Businesses are embracing an outsourced IT operations model. In 63% of incident response investigations, a major component of IT support was outsourced to a third party. Outsourcing can help businesses gain effective, cost-friendly IT services; however, businesses need to understand the risk their vendors may introduce and proactively work to decrease that risk.*"

The Trustwave report also found that "remote access" connections were the most widely used method of infiltration in 2012, stating, "*Organisations that use third-party support typically use remote access applications like Terminal Services or Remote Desktop Protocol (RDP), pcAnywhere, Virtual Network Computing (VNC), LogMeIn or Remote Administrator to access their customers' systems. If these utilities are left enabled, attackers can access them as though they are legitimate system administrators.*"



Remote Access was the number one method of entry for hackers in 2012 according to the Trustwave 2013 Global Security Report.

Any organisation that outsources part of its IT operations or allows vendors to access their network, even periodically, should have a secure and auditable way for vendors to connect to and work on their systems. Failure to do so can potentially lead to technical 'black holes' or legal disputes if something fails to operate correctly after the third-party intervention. Vendors who deliver support services also need to offer a more secure method to support their customers and systems.

The key considerations when allowing third-parties to access your infrastructure or applications should be:

- Controlled access and agile provisioning
- Trusted secure access path
- Ring-fenced access and defined privileges
- Audit and traceability
- Real-time monitoring and control

"When getting support from a vendor, the traditional approach was for them to ask us to connect to a WebEx or some other third-party tool. We take a security risk when giving someone outside our network access to our environment. Now, we make them log in with Bomgar, and I can control what they can and can't do and know that their application will uninstall whenever the session is closed."

- MIKE CASTILLO, DIRECTOR OF NETWORK INFRASTRUCTURE, EAT'N PARK HOSPITALITY GROUP

BOMGAR FOR VENDOR ACCESS

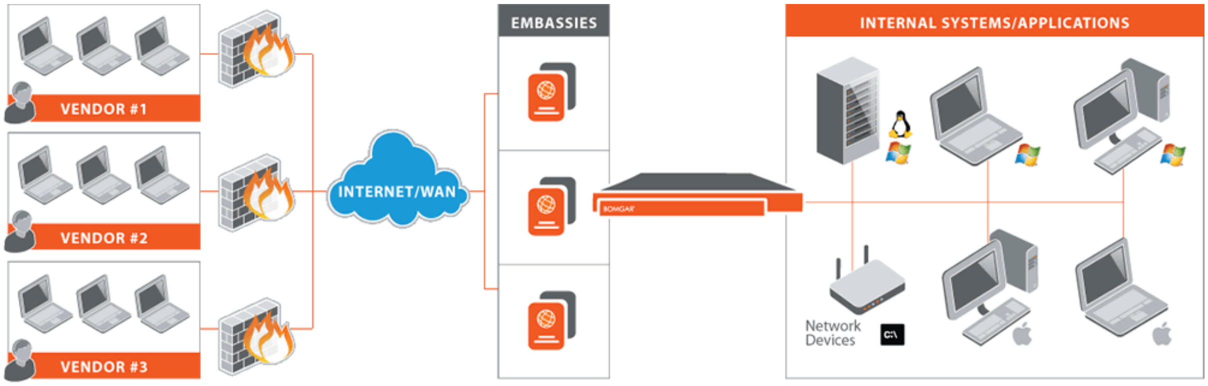
BOMGAR'S SECURE APPLIANCE-BASED REMOTE SUPPORT SOLUTION allows vendors to access all of an organisations' systems--from desktops to laptops to servers and smartphones--while addressing the crucial security requirements of granular permissions and a comprehensive audit trail. Bomgar acts as a centralised proxy for vendor activity throughout an enterprise, without the need to deploy hardware to every network segment.

EMBASSY

For internal IT organisations, Bomgar's Embassy technology is a way to provide secure, auditable, cross-platform remote access to vendors who need to regularly access specific systems. Their Bomgar Embassy profile allows for each and every vendor to granularly control what they can or cannot access. Creating Embassy teams is a much more secure and manageable alternative than giving individual vendor technicians VPN access to your internal systems, especially in crisis management scenarios.

Embassy includes more than 50 configurable access privileges for the vendor connecting to your network. Simply create an Embassy, define the specific privileges for that vendor, then add users. You can add Embassy users individually or in groups using identity management technology such as LDAP, RADIUS, or Kerberos.

With Embassy, you can also automatically route support requests related to a vendor's application to that specific vendor's support team. Whenever an end user submits an issue with that application through your support portal, he or she will be immediately directed to the vendors' queue, eliminating frustrating transfers. You can also use Bomgar's Equilibrium technology to automatically route issues that require specific expertise to vendor technicians based on their availability and/or skill.



Bomgar Embassy enables managed vendor remote access to your corporate network.

VENDOR COLLABORATION

Unlike provisioning individual VPN access, Bomgar's Intelligent Collaboration feature allows for multiple internal and/or external technicians to come together and share a common platform. Once the expert joins the session, collaborators can view the end-user's screen, share controls with the original technician and chat with everyone in the session. Used together with Embassy, Intelligent Collaboration gives your support team a seamless and secure way to work with vendors in real-time.

By working in a collaborative environment, skills can be shared, issues are resolved more efficiently, and the overall process becomes more streamlined.

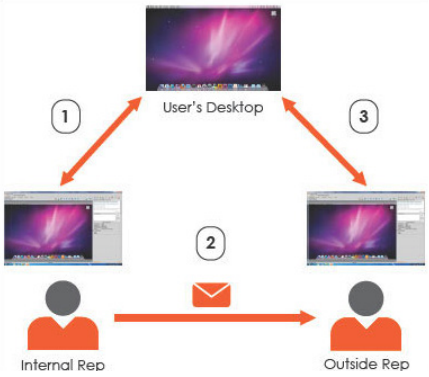
AUDIT TRAIL

Bomgar provides tamperproof logs of every action participants perform on your corporate network and systems. You can run reports detailing chat transcripts, the number of files transferred and the permissions requested and granted. Reports can be viewed online or downloaded. You can also use session recording to save videos of remote access sessions involving vendors, including annotations showing who was in control of the mouse and keyboard at any given point during the session. The audit trail is stored on your Bomgar appliance behind your secure firewall, rather than on the vendor's system, which is a common security loophole with many other access tools.

OCCASSIONAL TECHNICIAN INVITE

Your organisation's IT team may need occasional assistance from an external vendor who doesn't require regular access to your systems. Bomgar's External Rep Invite feature allows your support team to collaborate with external experts on an ad-hoc basis to view and ultimately resolve incidents, even if the expert or vendor has never used Bomgar before.

Your technicians who need assistance simply send an invite to an outside expert and decide which security profile should be applied when he or she joins the session. Rep Invite walks the invited expert through running the Bomgar Representative Console, which opens to the support session that requires his or her expertise. At the end of the session, the Bomgar representative console is cancelled and no longer available for use.



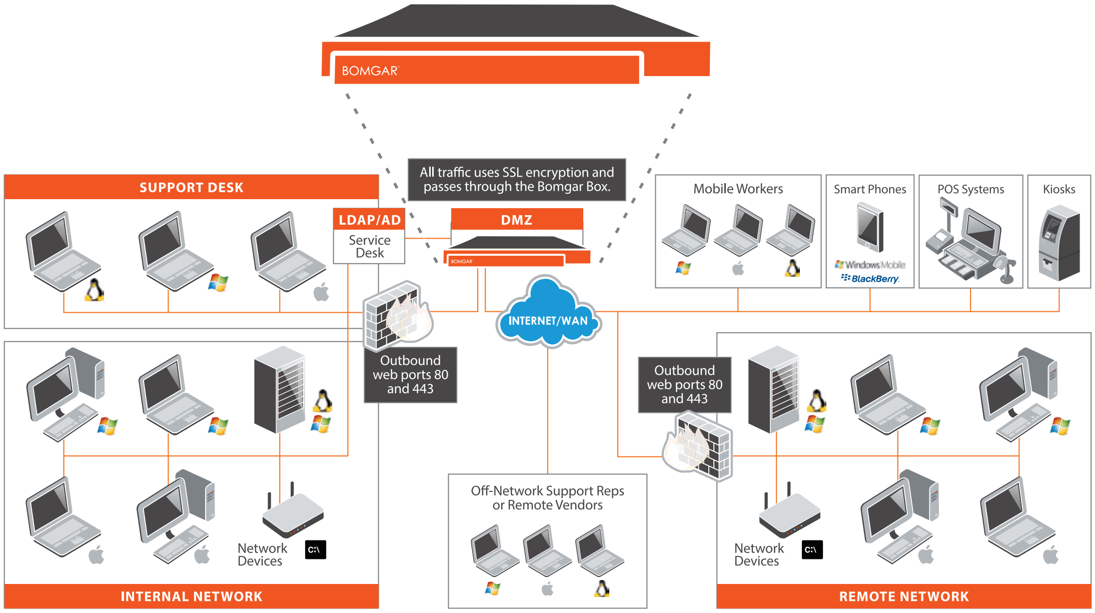
Reps can invite external vendors into support sessions on an ad-hoc basis.

> *"We wanted to ensure vendors would have access to the systems without a lot of difficulty. But at the same time, we wanted the ability to control and monitor the access. Bomgar's Embassy feature allows us to do that."*
>
> **- STEPHEN HEY, MANAGER OF TECHNOLOGY INFRASTRUCTURE AND SECURITY, 9/11 MEMORIAL**

SECURITY ARCHITECTURE

While remotely supporting all of your systems is invaluable, ensuring your solution is secure is imperative. Bomgar's on-premise appliance keeps system access and data behind your own firewall and security policies. Bomgar's security-focused design eliminates the common issues with SaaS and point-to-point remote access tools, such as always-on access, password sharing, and incomplete or non-existent audit trails.

- **ARCHITECTURE:** Centralised, security-hardened appliance - never passes data or system access through a third-party. **AUTHENTICATION:** Integrates with existing identity management and authentication methods, such as Active Directory.
- **ACCESS CONTROLS:** 75+ permissions can be administered - individually or through group policies.
- **AUDIT:** Full audit trail and video recording of session events.



Bomgar's appliance-based design enables secure support within and outside the firewall.

ABOUT BOMGAR

Bomgar provides remote support solutions for easily and securely supporting computing systems and mobile devices. The company's appliance-based products help organizations improve tech support efficiency and performance by enabling them to securely support nearly any device or system, anywhere in the world — including Windows, Mac, Linux, iOS, Android, BlackBerry and more. More than 7,500 organisations across 65 countries have deployed Bomgar to rapidly improve customer satisfaction while dramatically reducing costs.

CONTACT BOMGAR   info@bomgar.com | 866.205.3650 (U.S) | +44 (0) 1628 480 210 (U.K./EMEA)   BOMGAR.COM