

# Bomgar Privileged Access Management Supports Key Recommendations from Industry Analysts

In November 2015, Gartner published the report: *How to Secure Remote Privileged Access for Third-Party Technicians* ([download here](#)). According to the report, “most organizations granting remote privileged application or operating system-level access to third-party users leave gaps that introduce significant security risks,” highlighting the importance of privileged access management solutions.

## The report highlights the key challenges faced by administrators, including:

- Vendor access is a necessary evil and often leads to loss of productivity and agility.
- Many tools used today for vendor access leave significant security gaps that expose organizations to risk.
- Third-parties generally require only temporary remote access, restricting authentication choices.
- Monitoring and recording privileged sessions is essential.

The report states that, “by 2020, the maturation of best practices and privileged access management technology will enable more organizations to reduce the attack surface created by unsafe or incomplete remote privileged access processes; 30% of enterprises will be significantly exposed due to unsafe access, compared to 75% now.”

The security landscape is rapidly changing. With many organizations still using legacy solutions such as VPN to manage third-party access, the security threat associated with vendors continues to grow. Organizations looking to enhance their security posture are turning to privileged access management solutions, such as those offered by Bomgar.

Within the report, Gartner outlines four key recommendations for securing remote privileged access for third parties. Below, we’ve outlined how Bomgar can help organizations meet these recommendations with our Privileged Access Management solutions.

Bomgar enables security professionals to control, monitor, and manage access to critical systems by privileged users. With Bomgar Privileged Access Management, they can obtain detailed visibility into sessions and access rights. Plus provide administrators, vendors, and business users with the access they need to improve productivity, while protecting high-value infrastructure, assets, and applications.

**RECOMMENDATION: Implement a separate identity life cycle that uses sponsors and delegates to manage third-party users.**

Bomgar’s solutions dovetail into a mature security framework that incorporates an identity lifecycle. The entire Bomgar solution is predicated upon a brokered outbound connection that allows sponsors and delegates to manage their third-party users securely. Bomgar’s solution offers granular controls, enabling users to incorporate identity lifecycle parameters into privileged access sessions.





**RECOMMENDATION: Deploy a combination of processes and tools that reinforces restricted access goals.**

Bomgar Privileged Access Management is a robust solution that integrates with various other tools to help reinforce a solid security posture. Bomgar is designed to support security best practices and processes, with integrations for password management, incident response, and SIEM tools, organizations are able to tailor a solution that meets their IT and security goals.

**RECOMMENDATION: Grant ad hoc access with limits on time, and restrict the scope to prevent lateral movement within and across systems.**

Bomgar Privileged Access Management allows administrators to set granular controls to fully define session permissions including session duration and limiting access. Blacklisting capabilities allow administrators to block certain applications or areas of the network from vendors, restricting lateral movement. Approval workflow gives security professionals the means to assign accountability and attribution to vendor activity. This helps organizations keep their vendors under control and allows them to grant only as much access as needed in order to complete tasks.

**RECOMMENDATION: Take advantage of improved session recording and replay capabilities to record and review session logs regularly. Prioritizing session that need to be reviewed is essential.**

The Bomgar solution has two main purposes; one is to control access, as noted in the first three recommendations, and the other is to provide the ability to monitor and audit sessions through advanced correlations of events. Bomgar Privileged Access Management has a rich logging capability. All sessions are automatically recorded and session activity is captured in a video log and in transcriptions. Through this advanced correlation, auditors and administrators can see exactly what a vendor did during a session. This data can be automatically populated to a SIEM tool, supporting regular monitoring and helping administrators to quickly find and respond to issues.

Bomgar Privileged Access Management enables organizations to close the significant security gaps resulting from third-party access. Our solution will help you protect your most critical assets from your more dangerous vulnerability... your vendors.

To learn more about how PAM works and download the Gartner Report: How to Secure Remote Privileged Access for Third-Party Technicians, visit:

[www.bomgar.com/gartner-third-party-access-report](http://www.bomgar.com/gartner-third-party-access-report)