BOMGAR™

Bomgar Privileged Access Management Use Cases

Securely manage insiders and vendors on your network without sacrificing productivity.

Organizations looking to protect critical infrastructure and systems are turning to privileged access management solutions to securely manage privileged insiders and third parties on their networks. Whether you're a small business or a Fortune 100 company, security threats can arise when the proper practices and technology are not in place.

Bomgar's Privileged Access Management solutions help organizations with a variety of privileged access challenges to increase security without compromising productivity. Do any of these sound like your organization?

I have third-party vendors in my network, but little visibility into what they are doing.

Managing Vendor Access

On average, IT professionals report that nearly 90 third-party vendors access their internal network on a weekly basis. These third-parties range from HVAC vendors to software manufacturers to IT outsourcers. They often have Active Directory credentials, and most likely a VPN – enabling them to log in at any time, and stay as long as they like. Unfortunately this is well known in the hacker community, as is the fact that many of these vendors are not as secure as their clients, making them a prime entry point for an attack. Combine this with less trust than internally-vetted systems administrators and high employee turnover at some vendors, and it becomes clear that implemention solutions that provide better control and visibility of third-parties with privileged access should be a top priority.

There's no reason for all of users to have full access to every system, even if they are trusted.

Granular Privileged Access

Gaining control over administrator access by internal, authorized, privileged employees may be one of the more difficult requirements set out by various Data Privacy regulations and IT security controls frameworks.

To a certain degree the organization must trust these users and their own hiring practices or they wouldn't be able to do their jobs. But that doesn't mean every privileged user needs wide-open, unmonitored access to every system in the organization's network. This opens doors to possible errors and accidents that could be harmful to the network. Applying granular permissions and approval workflows for privileged users limits their access to only the systems and applications they need, while allowing for additional privileges to be granted in the case of an emergency.

I have situations where a user needs escalated privileges, but only temporarily.

Granting Temporary Access

Occasionally it is necessary to provide administrators or vendors with additional privileges to access systems or perform functions beyond their normal responsibillities. However, it's important these temporary privilege escalations don't become permanent, and that they don't grant more access than is needed to accomplish the task at hand.

Organizations need tools and processes in place that allow them to quickly grant additional access to privileged systems, but also timebox, monitor and systematically revoke that access based on the need. Otherwise, they are likely to circumvent prescribed security controls.

My organization is being held to strict compliance mandates that we must meet.

Meeting Compliance Guidelines

Many organizations are held to strict compliance standards such as PCI and HIPAA. Auditing procedures are in place to ensure that compliance requirements are being met, and it is the organization's job to provide evidence that they are following standards.

Detailed session logs are often required as evidence for remote access, and if an organization cannot provide these in a timely manner, they could be subject to costly penalties.

Managing privileged access is inefficient and requires too many resources.

Increase Productivity

Many legacy access management technologies leave security gaps and hinder productivity in an organization. When organizations use technologies such as VPN, time is often wasted configuring or shutting down access to critical infrastructure using traditional measures like layer 2 network segmentation and using Microsoft Group Policy.

Organizations also waste time on privileged account management solutions with lengthy implementation processes. Most organizations cannot afford to let security improvements disrupt productivity. An organization's security posture is made up of several layered components, privileged access management being just one of them. Choosing a solution that integrates seamlessly with your current technology and processes and is quick to implement will speed adoption and increase productivity.

I need to trace which credentials are being used and by whom, and ensure those credentials are being rotated and securely stored.

Shared Privileged Accounts

Accounts that have elevated rights are often times used by multiple administrators. If something is compromised while accessing one of these accounts, there is little certainty as to who last used the account and what went wrong.

When working with shared accounts, you could have the same local account in use on multiple devices, requiring the password to be changed on all these devices at the same time, or you could have services that run as these accounts, or even passwords that are hard coded in a script. Simply changing the password for these accounts could break any of these things.

Organizations must adopt tools that allow them to secure and regularly rotate credentials for shared accounts without disrupting administrator productivity.

Bomgar Privileged Access Management

Bomgar's Secure Access solutions can help your organization manage any of these use cases. Whether dealing with third-party or internal users, the key to mitigating threats is controlling, managing, and monitoring their access. Bomgar Privileged Access Management and Bomgar Vault enable organizations to do this without complex tools or lengthy implementations.

- Mitigate the threat of a compromised vendor by eliminating them as a useful foothold for a bad actor trying to gain access inside your network.
- Maintain granular control of access to your network and set approval processes for access as well as defining session parameters.
- Stop the chance of internal and third-party users accessing or accidentally making changes to areas of the network they are not supposed to access.
- Automatically record all session activity in both a video and transcript form, supporting your monitoring and auditing processes.
- Manage privileged access approvals from anywhere via your Android or iOS device.
- Use screen sharing, video, and chat features to manage privileged sessions without being physically with the vendor or user.
- Ensure credentials are protected and working, as well as set up automatic password rotation.

Bomgar Privileged Access Management and Bomgar Vault can be implemented in days, and are easy-to-use, ensuring rapid adoption by administrators and vendors. Staff can quickly become proficient in Bomgar without the involvement of consultants, allowing organizations to quickly address security issues instead of getting caught up in a long implementation process.

To learn more about how Bomgar Privileged Access Management and Bomgar Vault work or to chat with a representative, visit www.bomgar.com/access-management

CONTACT | INFO@BOMGAR.COM | 866-205-3650 (U.S.) | +44 (0)1628-480-210 (U.K./EMEA) | BOMGAR.COM