


# THE TOP 5 PRIVILEGED ACCESS PROBLEMS

With the growing number of connected devices and vulnerabilities surrounding remote access tools and passwords, IT departments are faced with many issues when it comes to security. Do any of these situations face your organization?





I have third-party vendors in my network, but I don't really know what they are doing.

## 1 MANAGING VENDOR ACCESS

On average, IT professionals report that nearly 181 third-party vendors\* access their internal network on a weekly basis. These third-parties range from POS vendors to software manufacturers to IT outsourcers. They often have Active Directory credentials, and most likely a VPN – enabling them to log in to your network at any time, and stay connected as long as they like.

[\\*2017 Secure Access Threat Report](#)

## 2 “ALL OR NOTHING” PRIVILEGED ACCESS

Privileged accounts are used to perform administrative, maintenance, and other key system tasks across a network. These accounts can be accessed by multiple technicians in any given day, for regular maintenance or temporarily for an urgent task.

However, it's important these temporary privilege escalations don't become permanent, and that everyday users aren't granted more access than is needed to accomplish the task at hand.



I want to adopt a least privileged policy in my organization.

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



### 3 MEETING COMPLIANCE GUIDELINES

Many organizations are held to strict compliance standards such as PCI, GDPR 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.

### 4 PROCESS CAN HARM PRODUCTIVITY

Legacy access management technologies, like VPNs or RDP, leave security gaps. Even though technicians are often using a patchwork of tools based on the task, users may not want to give up the tools they already know.

Managing privileged access can't slow down my people.



I need to lock down shared admin account passwords & enforce corporate password policies.



## 5 PASSWORDS ARE STORED MANUALLY & INSECURELY

Privileged user accounts, or credentials, are a common network entry point for hackers. Since many IT professionals use multiple privileged accounts to access endpoints in the network, the volume of credentials to manage and secure is high. These credentials are often stored and shared insecurely using spreadsheets or sticky notes. They are often forgotten, non-compliant, repeated, and rarely or never changed.

## Solve these problems and more with Bomgar Secure Access Solutions

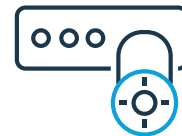
Bomgar allows employees and vendors to access systems and support people easily, while protecting credentials and endpoints from threats. Increase access speed and agility, while enforcing least privilege best practices, to simultaneously drive business performance and security.



**Support & Service**  
People & devices



**Access & Protect**  
Remote systems & endpoints



**Secure & Defend**  
Passwords & credentials

▶ Learn more about how Bomgar can help solve your privileged access problems at [www.bomgar.com/solutions](http://www.bomgar.com/solutions).

### ABOUT BOMGAR

Bomgar is the leader in Secure Access solutions that empower businesses. Bomgar's leading remote support, privileged access management, and identity management solutions help support and security professionals improve productivity and security by enabling secure, controlled connections to any system or device, anywhere in the world. More than 12,000 organizations across 80 countries use Bomgar to deliver superior support services and reduce threats to valuable data and systems. Bomgar is privately held with offices in Atlanta, Jackson, Washington D.C., Frankfurt, London, Paris, and Singapore. Connect with Bomgar at [www.bomgar.com](http://www.bomgar.com).