

Welcome

TO

HOTEL BOMGAR

Managing privileged access is like managing a hotel. Every day, guests come in and out of the hotel. Some have a long stay, while others only stay for a night, in addition to the hundreds of hotel staff. Managing the operations of all these people requires different policies and procedures to keep guests and employees safe and crime out.

▶ FRONT DESK CLERK

Access to database of guest information and able to program keys



▶ **GUESTS:** At check-in, the identity of guests is verified with photo identification, and a room key is issued. This access ends upon check-out.

▶ **EMPLOYEES:** Upon hire, employees are issued a key card, enabling access corresponding to their job duties. Access can be adjusted for job changes, and it ends upon termination of employment.



▶ **CONTRACTORS:** Vendors are issued access keys based on their activities for just a pre-defined period of time. If they need to stay longer, they must receive approval to extend their access.

▶ HOTEL GENERAL MANAGER

Access to all spaces, guest information, and the hotel safe



▶ HOTEL HOUSEKEEPER

Access to all guest rooms and laundry area



▶ BANQUET AND KITCHEN STAFF

Access all meeting and banquet rooms



▶ CONTRACT REPAIRMAN

Temporary access to the repair location only



▶ GUESTS

Access only to their rooms and public facilities while abiding by hours of operation

A VIP Guest may also have special access to a club level lounge





PERIMETER SECURITY ISN'T ENOUGH

Targeted attacks on corporate IT networks have increased in scale and public visibility. In the majority of these hacks, the hacker bypasses perimeter security by stealing legitimate credentials to gain access. With increasingly sophisticated phishing tactics and social engineering, even the most knowledgeable employees and vendors can be successfully targeted.

Just as a hotel's front doors wouldn't be the only point of entry for hotel access, perimeter security shouldn't be the only method deployed to keep a network safe. Guests should not have access to every room in the hotel, similarly, network users should not have full access to all systems. To keep a network secure, policies and permissions must be set granularly and enforced for users within the network.

"80% of all security breaches involve misuse of administrative privileges."

PRIVILEGED IDENTITY MANAGEMENT TRENDS FORRESTER, JUNE 2015



A FIVE STAR PRIVILEGED ACCESS SOLUTION

Bomgar Privileged Access Management Suite helps organizations to manage, control, and monitor privileged accounts and credentials with an easy-to-use, Five Star solution.

- ▶ **PROTECT THE ACCESS:** Enable role-based access to specific systems and define session parameters.
- ▶ **MANAGE ACTIVITY:** Actively manage the ongoing operational user of network devices and hardware on the network.
- ▶ **ANALYZE DATA:** Understand what privileged users are actually doing within the network and audit for misuse.
- ▶ **LEVERAGE EXISTING INVESTMENTS:** Integrate with existing tools such as SIEM, change management, and password management.

BOMGAR™