GUIDEPOINT SECURITY

BEHIND THE LOCKED DOORS

# A Visual Guide to Privileged Access Management

Controlling access to restricted areas, sensitive information, systems and applications is like locking the door. In the world of Privileged Access Management, intruders are called threat actors. Physical keys are known as biometric identifiers.

**Here's a look at a few data points** to help you drive organizational growth, enable digital transformation and ensure individuals have only the appropriate levels of access required to perform their job responsibilities, while also allowing security teams to quickly identify and address any malicious activities associated with privilege misuse, thereby mitigating potential risks.

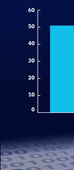
## 80%

According to industry experts, as much as **80%** of security breaches are due to user and privileged account passwords being compromised, and a majority of these breaches remain unnoticed for more than **200 days**.[1]

## WHY?

This is largely due to the prevalence of weak passwords, including well-known default passwords such as **"admin"** and **"12345,"** which are **still used by over 20% of companies.** The issue is further compounded by users utilizing the same password across multiple accounts.[1]

**Stolen passwords** account for up to **80%** of all security breaches. To exploit privileges, hackers frequently opt to steal account credentials, which they can obtain through malware or social engineering tactics, allowing them to gain unauthorized access.[1]




Most companies face the threat of a data breach by a criminal group in **51%** of the cases vs. **18%** by a state-sponsor actor.[1]

**60%** Just over **60%** of breaches involve **hacking**[1]

**81%** of hacking-related breaches leverage stolen and/or weak **passwords**[1]

**43%** of breaches involve **social attacks** (including phishing, pretexting, and spear phishing)[1]

**14%** of breaches involve employee errors, while another **14%** involve **privilege misuse**

**51%** of breaches include malware, and **66%** of that malware is delivered by **malicious** email attachments

**27%** of breaches are discovered by **third parties**

## Here's Some Good News

The **global** privileged access management solutions market size is projected to reach **$19.73 billion by 2030**[2]

The privileged access management solutions market is anticipated to experience **sustained growth**, propelled by the imperative to enhance organizational efficiency and security, and the growing frequency of global cybersecurity regulations.[2]

**North America** dominates the privileged access management solutions market due to rise in the government regulatory compliances, increase in the adoption of best practices for identity management and rise in the research and development activities in this region.[2]

## Final Thoughts

Privileged access management is critical for protecting your organization's intellectual property and confidential information, and maintaining the trust of business partners and consumers. GuidePoint Security can assist in defining policies and solutions for privileged access management, managing the lifecycle of privileged accounts and monitoring privileged user activities. Just like when you lock your doors.

Get in touch today

GUIDEPOINT SECURITY

www.guidepointsecurity.com


SOURCES:
Identity Management Institute https://identitymanagementinstitute.org/privileged-account-management-pam-blog
Allied Market Research https://www.alliedmarketresearch.com/privileged-access-management-solutions-market-A12400
Data Bridge Market Research Global Privileged Access Management Solutions Market – Industry Trends and Forecast to 2028
https://www.databridgemarketresearch.com/reports/global-privileged-access-management-solutions-market