

SMBs



Privileged Access Requirements for Small and Mid-Size Businesses



SMBS HAVE BECOME GROUND ZERO FOR CYBERCRIME

Over the last few years, SMBs have become [ground zero for cybercrime](#). To combat this threat, we invite you to click on the link below for a new white paper from international and independent analyst organization KuppingerCole entitled, "**Privileged Access Management Requirements for Small and Mid-Size Businesses**".

What's Inside

The white paper, which was commissioned by Devolutions and prepared by KuppingerCole Senior Analyst [Paul Fisher](#), addresses the following key issues:

- Why SMBs should consider PAM essential.
- How digital transformation is impacting SMBs and presenting new identity challenges.
- How PAM can help stop cyber criminals and hackers.
- The essential PAM components for SMBs.
- Why a good PAM setup for SMBs should automate as many functions as possible, be easy to use, and deliver real-time insights.
- How new features and trends are making PAM easier for SMBs.
- Best practices for deploying and running a PAM solution that is scalable and fit for purpose.

The white paper also offers an independent analysis of Devolutions' PAM solution for SMBs.

Advises Paul Fisher:

Privileged Account Management is highly recommended for SMBs, even if they currently feel they are not big enough or do not yet process the kind of data that needs this kind of protection. Many SMBs would discover, through a careful audit of data usage and access, that they may be exposing the company to risks without realizing it through poorly managed privileged accounts. Even if we lived in a world without cyber-attacks, the efficiency and operational benefits that a well-set-up PAM solution delivers should be attractive to any business. These benefits also reduce the threat of ex-employees or temporary workers retaining access to systems, and they help keep SMBs on the right side of compliance and audit legislation.

Get the Report

