# Six Reasons Why Vendor Privileged Access Management Should Be a Priority

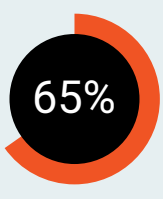
If you're using a virtual private network (VPN), privileged access management (PAM), or desktop sharing tools to manage your vendors' network access, the limitations of these tools leave you vulnerable to data breaches. When a company grants privileged access to third-party users, a tailored solution is needed.

Below are six reasons why Vendor Privileged Access Management (VPAM) should be a priority:

REASON ONE

## Increased dependence on third-party vendors


58% of organizations admit to sharing sensitive information with more than 100 third parties.[1]




More than 65% of organizations "rely heavily" on third parties.[2]

REASON TWO

## Privileged accounts are a target

74% of IT decision makers attribute a breach to privileged access abuse.[3]

80% of breaches are due to compromised credentials.[4]

85% of IT decision makers say they manage privileged accounts manually.[1]

REASON THREE

## The vendor access threat is real


61% of U.S. companies have experienced a data breach caused by a third party.[1]


Less than 40% of companies believe they have sufficient resources allocated to their third-party risk management.[1]


Only 17% of respondents rate their company's effectiveness in mitigating third-party risk as highly effective.[1]

REASON FOUR

## Bad habits and limited end-user oversight

### Managing poor security standards

65% of organizations are sharing root or privileged access to systems and data.[1]

### Controlling access

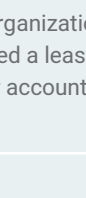
50% of organizations' privileged accounts never expire or get deprovisioned.[4]

1 in 8 organizations has implemented a least privileged policy for account access.[4]



### Authentication as a priority

Only 34% of organizations keep a comprehensive inventory of their third-party vendors.[1]



### Granular audit

54% of respondents fail to maintain an audit trail of privileged account acitivity.[4]

REASON FIVE

## Centralized access management promotes a healthy network


69% of network managers agree that a lack of centralized control is a key factor in weakening vendor privileged access security (by not having a comprehensive inventory of third parties).[1]

REASON SIX

## The stakes are high

**AVERAGE COST OF A DATA BREACH VS. THIRD-PARTY DATA BREACH**


The average cost of a data breach is $141 per record.[5]

The average cost of a data breach related to a third party is $158 per record ($17 more).[5]

If you have vendors on your network, it's time to find the right Vendor Privileged Access Management solution with:



**Multi-factor authentication** – Access only for known and approved users



**Credential management** – Eliminate shared logins



**Comprehensive audit** – Granular review of all user and application activity



**Access controls** – Based on least privileged policies; only the access needed to perform critical functions

SECURELINK

GET A CUSTOMIZED DEMO

Visit securelink.com/demo or call 833.678.4786

1 Data Risk in the Third-Party Ecosystem // 2 Auditing Third-party Risk Management // 3 Privileged Access Management in the Modern Threatscape // 4 State of PAM Maturity Report // 5 Cost of Data Breach Study