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

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:

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

- **74% of IT decision makers attribute a breach to privileged access abuse.**
- **61% of U.S. companies have experienced a data breach caused by a third party.**
- **80% of breaches are due to compromised credentials.**
- **Less than 40% of companies believe they have sufficient resources allocated to their third-party risk management.**
- **85% of IT decision makers say they manage privileged accounts manually.**
- **65% of organizations admit to sharing sensitive information with more than 100 third parties.**

**REASON ONE**

Increased dependence on third-party vendors

- **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).**

**REASON TWO**

Privileged accounts are a target

- **73% of IT decision makers believe control is a breach to privileged accounts.**
- **86% of breaches can be attributed to third-party vendors.**
- **85% of IT decision makers believe they manage privileged accounts on their own.**

**REASON THREE**

The vendor access threat is real

- **61% of IT decision makers believe privileged access to third-party vendors is a real threat.**
- **34% of organizations keep a comprehensive inventory of their third-party vendors.**
- **50% of organizations' privileged accounts never expire or get deprovisioned.**
- **54% of respondents fail to maintain an audit trail of privileged account activity.**

**REASON FOUR**

Bad habits and limited end-user oversight

- **58% of organizations admit to sharing extensive information with more than 10 third parties.**
- **More than 65% of organizations “rely heavily” on third parties.**

**REASON FIVE**

Centralized access management promotes a healthy network

- **69% of network managers agree that a lack of centralized control is an easy factor to avoid when privileged access security (by withholding compromising privileged access).**

**REASON SIX**

The stakes are high

| Average Cost of a Data Breach vs. Third-Party Data Breach |
|-----------------|-----------------|
| **DATA BREACH** | **THIRD-PARTY DATA BREACH** |
| $141 per record | $158 per record ($17 more) |

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
- **Granular audit** – Granular review of all user and application activity
- **Access controls** – Based on least privileged policies; only the access needed to perform critical functions

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.