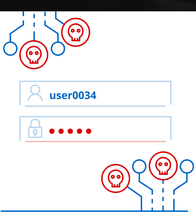
How to Stop Security Breaches

If you're not protecting your user passwords and remote connections, you're basically inviting hackers inside your network, as unsecure passwords are the easiest way to let them in. What's an overworked IT professional to do?



Start with understanding how you're at risk.

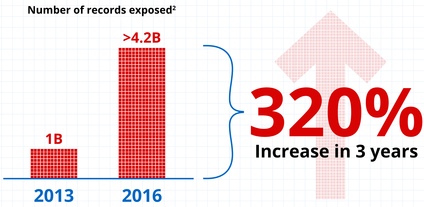
Security breaches are soaring

New records were set for the number of breaches and stolen files last year.[1]

There were **4,149** confirmed breaches in 2016.[2]

That's **A LOT** of stolen data.

Number of records exposed[2]



The first defense against these types of attacks?
Never use the same password for different accounts.

Getting users to comply is a whole different struggle—ask any frazzled IT pro.

Identify—and address—4 top security flaws

To fully assess your risk level, beware these common security flaws. But keep in mind that managing connection protocols, passwords, configuration settings, and device access is impossible without a solution that can directly address these issues.

Data breaches can be caused by:	The right solution should provide:
Improperly stored passwords and data Weak, shared, or reused passwords are just begging to be exploited by a hacker.	**Unified password and data storage** Centralizing passwords and enterprise data in one secure location keeps data safe and accessible.
Non-integrated remote connections and protocols Manual logins across dozens of desktop managers and connection types can lead to risky shortcuts.	**Freedom to work in different remote environments** Quickly switch to different settings, access the right tools, and deliver better support—from one interface.
Unmonitored access controls, permissions, and session settings When anyone in your network can access anything, you're giving hackers permission for free entry.	**Role-based access controls and permissions** Secure, organize, and store sensitive data in one system, while controlling user access.
Confusing, disorganized systems Inefficient workflows, bad user experiences, and disparate systems leave you open to security risks.	**An intuitive and friendly user interface** A powerful and flexible user experience boosts employee satisfaction and productivity.

Devolutions Remote Desktop Manager can help

The right solution doesn't have to be expensive. When it comes to remote connection and password management solutions, simpler is better—for IT, your users, and your bottom line.

Learn how Devolutions can make IT's job a little bit easier.

Download the Whitepaper

Devolutions

Sources

[1] https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

[2] http://www.nbcnews.com/tech/tech-news/more-4-billion-data-records-were-stolen-globally-2016-n714066