Streamline IT with Secure Remote Connection and Password Management

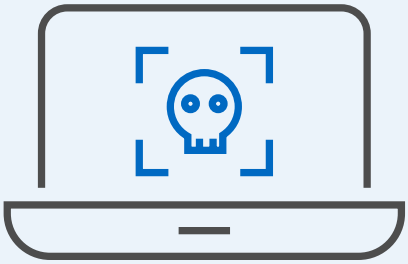
Devolutions

Table of Contents

Introduction

We hear stories all the time confirming that security continues to be a huge challenge for IT. New records were set for the number of breaches and stolen files in 2016.[1] During 4,149 confirmed breaches, more than 4.2 billion records were exposed—approximately 3.2 billion more than in 2013, which was the previous high-water mark. Businesses were hit the hardest, accounting for 55% of the breaches, followed by medical institutions and government agencies.[2]

The mega-breach reported at Yahoo last year shows just how vulnerable organizations are to hacking: 500 million user accounts were hacked in 2014 and more than 1 billion accounts were hacked in 2013.[3] The first defense against these types of attacks? *Never use the same password for different accounts.* This is especially critical for work environments where users connect to many different systems and accounts. But getting users to comply is a whole different struggle—ask any frazzled IT professional.



4,149

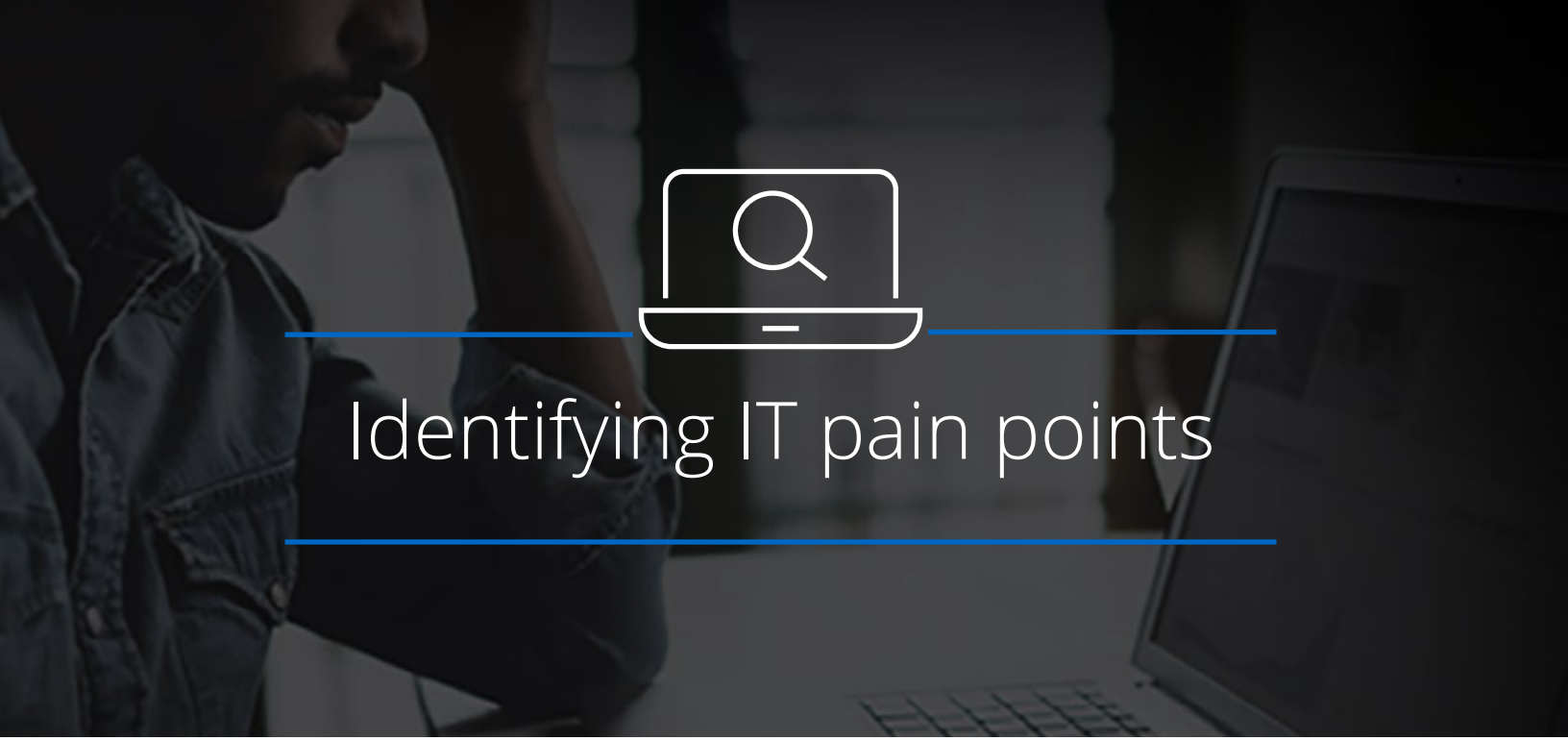
confirmed breaches in 2016

The issue becomes even more complex when you consider that between the proliferation of bring your own device (BYOD) programs and technology agnosticism, organizations face a greater variety of devices and device types connecting to different endpoints over company networks than ever before. IT must be able to access all devices in an organization's fleet, which could extend worldwide. How can IT possibly manage all these remote connections plus every different (or not-different-enough) user password—while at the same time protecting company data from catastrophic breaches?

When it comes to remote connection and password management solutions, the simpler the solution, the better. Yet, knowing what to look for can be a difficult task. From an IT perspective, a remote desktop solution should not only make it easy to view a remote user's computer, but also ensure that the network, passwords, and other credentials are secure.

This white paper explores some of the common challenges IT pros face in remote desktop environments, as well as what types of features to consider when selecting a solution. With the right tools, today's IT professionals can provide faster and more efficient support services—and help their organizations become more agile and connected in today's quickly changing technology-driven environments.

With the right tools, today's IT professionals can provide faster and more efficient support services—and help their organizations become more agile and connected in today's quickly changing technology-driven environments.



Identifying IT pain points

Whether your organization has offices throughout the world, around the country, or in just one headquarters, IT is likely required to log into user devices or systems that could be anywhere. Securely managing connection protocols, passwords, configuration settings, and device access is virtually impossible without the right solution.

IT pros face some universal challenges.

Improperly stored passwords and data

Managing different remote connections and protocols

Unmonitored access controls, permissions, and session settings

Confusing, disorganized systems

Improperly stored passwords and data

Device security, encryption, and password management—these critical issues are at the forefront of IT pros' minds. In an average day, an IT organization may have hundreds of credentials to manage, along with other types of sensitive data like account numbers, credit card information, licensing codes, and more. This data must be securely stored and managed, as well as made easily accessible, while also following local regulatory and compliance mandates.

Some common issues with passwords include users choosing weak passwords, reusing passwords, rotating passwords, refusing to change passwords, and sharing passwords—whether on purpose or inadvertently (e.g., sticky notes on one's monitor). In the event of a security breach, there's a good chance the hacker got into the network using weak, shared, or reused passwords. IT needs to be able to trust that no matter what choices users might make, there's a strong password management solution picking up the slack.

In the event of a security breach, there's a good chance the hacker got into the network using weak, shared, or reused passwords.

Managing different remote connections and protocols

Each help ticket in a day's task list can be different. With dozens of desktop managers and connection types to choose from, an IT pro's desktop screen can become a chaotic confusion of open windows running RDP, terminal services, Citrix, LogMeIn, Putty, TeamViewer, FTP, HP RGS, VNC, VPN, LastPass, KeePass, and more.

Manual logins across all of these types of systems can be time-consuming, especially when other tasks are beginning to stack up on the day's to-do list. Beyond workflow, staying up to date on software licensing costs and requirements is another job in and of itself. IT shouldn't discover a license has expired when they try to log in—and instead get locked out.

The diversity of user interfaces and operating systems available today only add to the challenge: Where a Microsoft-based solution might have been enough in the past, today's IT needs to function not only in Microsoft and Apple desktop environments, but also in mobile environments like Android or iOS. And, before reaching out to a user to troubleshoot a problem, IT must have the right information about that user's device to ensure they're not trying to troubleshoot a PC problem on an Apple machine.

Unmonitored access controls, permissions, and session settings

No matter the level of user in an organization, security is always an issue, and the same goes for IT. When working in remote desktop environments, sharing connection settings and credentials can be time-consuming; especially when there's a tricky problem that requires help from a colleague. At the same time, when it comes to security, certain duties and permissions must be kept separate to ensure that specific team members only see what they're cleared to see.

While IT might need a colleague's help with an issue, sharing screens or interfaces can lead to leaking sensitive information—or granting a user access to system levels they're not cleared to access on their own machines. If the access controls, permissions, and session settings aren't keyed to take each specific user into account, you've created gaps in your security protocols that can leave the organization at risk.

While IT might need a colleague's help with an issue, sharing screens or interfaces can lead to leaking sensitive information—or granting a user access to system levels they're not cleared to access on their own machines.

Confusing, disorganized systems

With multiple—sometimes thousands—of devices and passwords to manage, confusion can quickly set in and lower productivity. When IT pros have to move across different sessions and settings, not only are there a lot of passwords and credentials to save and remember, but it's highly likely that shortcuts will be taken, exposing the organization to security risks. Not to mention, inefficient workflows can lead to lost time and productivity, especially when important information is stored in disparate systems that either don't communicate well between each other or can't communicate at all.

User experience is another issue. As enterprise users have come to expect more of a consumer-grade experience out of their work tools, legacy technology systems can not only chase users away—but they can be frustrating to use when simple, daily tasks require specific training within a customized system interface.

Technology moves fast, so it's best to have systems that are built to grow with the organization as its needs change over time—not keep people locked into inefficient workflows and processes.

How can today's busy IT pros keep track of—and secure—all these moving parts, without investing in yet another complex, expensive system?

Selecting a secure remote connection and password management solution

Remote connection and password management solutions come in a variety of different forms, with capabilities that range in complexity. While Privileged Access Management (PAM) solutions, for example, might work for some organizations, the reality is that IT budgets are almost always tight and staff is often in short supply. But *no one* can afford an unsecure network.

An easy-to-use, affordable, and robust remote connection and password management solution may be a better option. One that can protect against security breaches, simplify the day-to-day workflow for IT, keep all passwords secure, and boost productivity organization-wide—while reducing costs and complexity. Ideally, the right solution would also make it easy to add features when necessary, as business needs evolve over time.

Here are the most important features IT pros should consider in choosing a remote connection and password management solution:

Unified password and data storage

Freedom to work in different remote environments

Role-based access controls and permissions

An intuitive and friendly user interface

Unified password and data storage

By centralizing all passwords and enterprise data in one secure location, IT can quickly access the information they need, when they need it, while also keeping remote sessions secure. When seeking a remote connection and password management solution, make sure the system allows integration with other existing password managers. That way, IT still has access, even when users store their usernames and passwords with other tools. This integration can also provide enhanced flexibility and security options for automatic login, saving time and helping to protect data.

Different users prefer different web browsers, so the solution you choose should have extensions that function the same no matter what browser users work in, from Internet Explorer, to Google Chrome, to Firefox. In addition, it's a time-saver for users—and IT—if the solution can automatically fill in web forms.

By centralizing all passwords and enterprise data in one secure location, IT can quickly access the information they need, when they need it, while also keeping remote sessions secure.

Freedom to work in different remote environments

When moving from one remote desktop session to the next, choose a solution that can cut through all the clutter. With a single interface on the remote desktop manager, IT can save time switching to different sessions, quickly access the right tools for the job, and deliver better support.

The solution should simplify connection management by allowing automatic logins for various session types. That way, IT can jump from connection to connection without having to look up—or try to remember—passwords or credentials that haven't been used for months. By saving credentials in the local database or in an external application, IT can feel confident that data is being kept secure.

For IT pros who need access to remote machines, not only do they need to trust that the connection is secure, but the ability to jump into a machine quickly saves a lot of time. The ideal remote connection solution should allow this by simply requiring a host name and IP address. Lastly, choose a solution that can easily import sessions from other remote connection management tools used, so IT can work seamlessly between environments.

Role-based access controls and permissions

IT needs a solution that can control permissions and user rights with role-based access control, so users can feel safe sharing information, knowing that the appropriate controls are in place to secure access and permissions. The right solution should secure, organize, and store all sensitive data in one system, while controlling access so only the right people can see it.

To manage documents, the right solution should enable use as a centralized data repository to store and organize comprehensive information about customers and their machines. Best of all, this solution should serve both cloud and on-premises users by providing anytime, anywhere access to documents and files. Lastly, if you need to produce reports, the solution should make it simple to retrieve and export data in an easy-to-understand format.

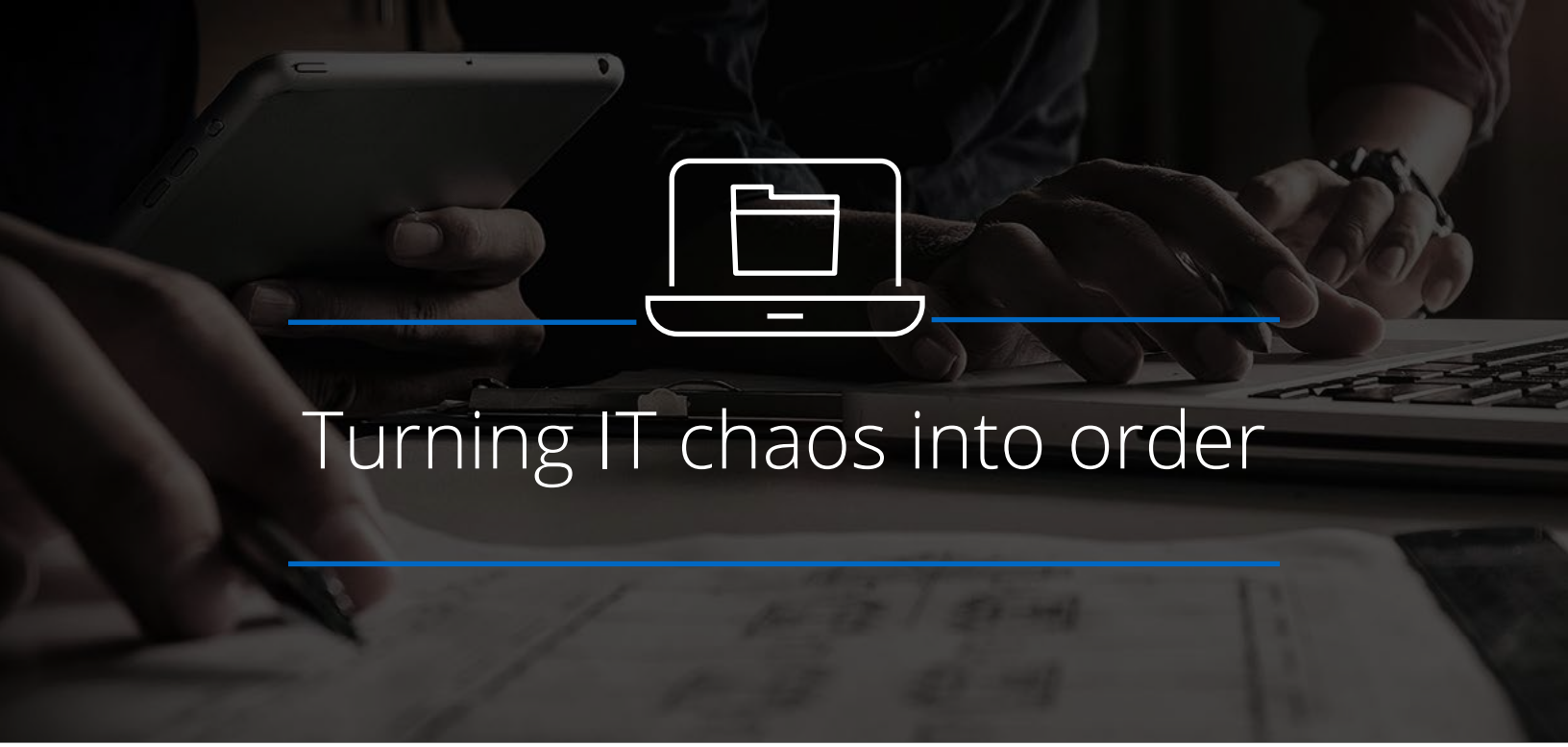
Best of all, this solution should serve both cloud and on-premises users by providing anytime, anywhere access to documents and files.

An intuitive and friendly user interface

Because users are typically the weakest link when it comes to security, the user experience is crucial. A powerful and flexible user experience can help boost employee satisfaction and productivity. Look for a customizable interface, so users can work the way they want to work.

Additionally, being able to store and access past sessions can help IT spot common problems and troubleshoot these problems faster. When there are multiple connections, device types, and user environments to manage, it's easy to get frustrated. An intuitive user interface can help IT stay organized, making it easier to store and access information while also providing a unified experience.

Similarly, look for a solution that provides access to premade troubleshooting templates that IT can share with users, so they can document or even solve their problems themselves. This feature can save IT a lot of time.



Turning IT chaos into order

IT pros are an organization's gatekeepers. Their job is to keep the organization running efficiently and productively, while also ensuring that hardware and software assets are safe. When it comes to remote connection and password management, IT needs the right tools to keep their organization secure—without breaking the bank.

For IT organizations already struggling to make do with limited resources, a robust remote connection and password management solution can cut through the complexity to provide better visibility into user behavior and more capabilities for implementing and enforcing security policies. The end goal? To empower IT and the rest of the workforce to perform more efficiently—while easing the burden on IT.

With a modern remote connection and password management solution, IT can better control the chaos by reducing the complexity and costs associated with other solutions—without sacrificing security.

When it comes to remote connection and password management, IT needs the right tools to keep their organization secure—without breaking the bank.

Devolutions Remote Desktop Manager can help

Interested in learning more? Remote Desktop Manager from Devolutions lets you centralize all your remote connections, passwords, and credentials into a unique platform that can be securely shared between users.

Download a 30-day trial ›

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

[3] https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html