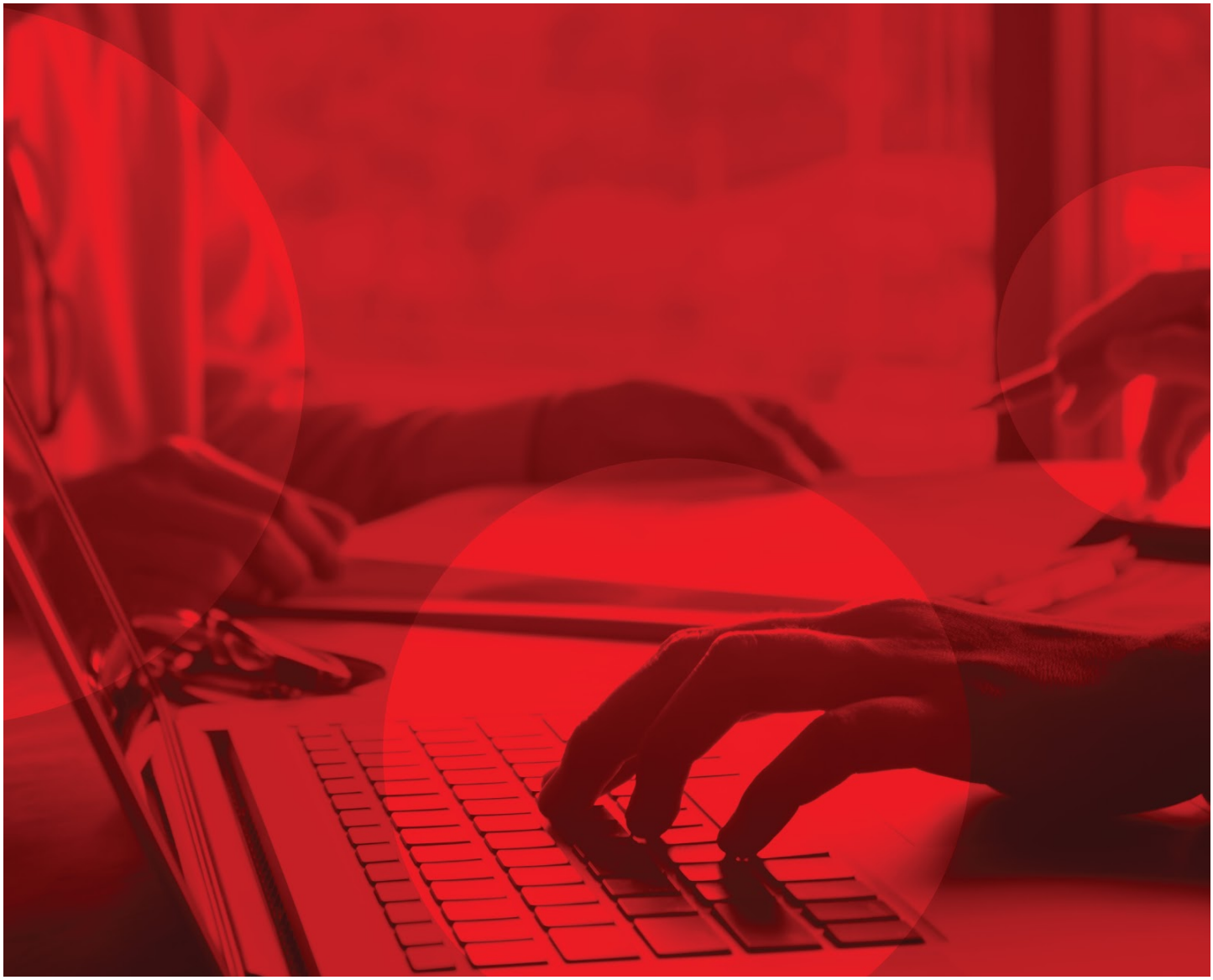
SCALED ACCESS

WHITEPAPER

Sharing Confidential Data Doesn't Require Sharing Credentials



Intro

Access management tools play an important role in confidential data industries where medical, financial and insurance information requires sharing and managing.

Access management ensures FinTech, MedTech and InsurTech employees can access and share confidential data effortlessly.

Under current IAM implementations, employees are forced to circumvent the system and share credentials and accounts to access confidential data. However, this eventually leads to risky ecosystems and data breaches.

In 2019, Comodo, ironically a cybersecurity company, suffered a data breach as a shared set of credentials got leaked on the internet.

It's evident that companies, especially ones working with confidential data, need to implement an IAM solution that prevents the need for employees to share credentials.

A new solution is needed. One that lets employees share access without sharing their credentials.

> **Under current IAM implementations, employees are forced to circumvent the system and share credentials and accounts to access confidential data.**

Traditional Access Management in the Workplace

Today, companies typically deploy static, role-based access control solutions. In these models, access policies are designed with a finite amount of roles that users can obtain, each role has a designated set of access rights assigned to it.

For example, a hospital may deploy an access policy where users (doctors, in this case) can view and update every and any section of an electronic health record (EHR), whereas nurses can only view the very same documents, or perhaps they may have the permission to modify only some particular sections of the EHR and not others. Alternatively, we can think of an insurance company that operates with an access policy where users (insurance brokers) can access all sections of an insurance claim, whereas insurance doctors only have access to the medical section of the claim.

Traditional solutions require constant back-office administration. Back-office staff need to assign permissions, privileges, entitlements, access groups and authorization roles to users.

With traditional implementations, back-office staff are generally tasked with:

- Onboarding new users.
- Assigning new roles, permissions (etc.) when users' roles and/or responsibilities change.
- Removing users when they leave.

Though this administrative model appears suitable for companies who have user bases of 10,000s, in practice it doesn't scale well and is incredibly inefficient, relying on too many manual processes, which can cause serious productivity and security issues.

Relying on back-office staff means in cases of failure:

- New employees can't start working.
- Employees who have been given a new role or tasks can't access additional resources needed to perform their new responsibilities.
- Ex-employees have access to confidential data after leaving.

Ultimately, when you have an over-reliance on back office administration, people start to share credentials with each other instead of waiting for back office staff to give them access. This practice, however, presents their company with serious threats.

Do Employees Actually Share Credentials?

Studies have found that a significant percentage of employees share their credentials with colleagues to access company resources, often against company policy. Worse, they even found that there are companies today who actually still permit credential sharing. This is extremely worrying.

A 2019 survey uncovered that 34% of employees share passwords or accounts with their co-workers. This means that, in the U.S. alone, there could be over 30,000,000 employees sharing credentials[1].

> **Organizations must wake up and combat the problem. Their employees are sharing credentials to access confidential data!**

The Risks Of Sharing Credentials To Confidential Data

When employees share credentials to confidential data, they pose severe security and business risks to their company.

These include:

- The risk of credentials falling into the wrong hands, allowing outsiders to access data - as in the case of Comodo's data breach.

- The risk of an employee acting maliciously without being uncovered. For example, an employee using somebody else's credentials could make an unauthorized payment, delete sensitive data or could even change account passwords, thereby locking other users out, all without anyone knowing which user did it.

[1] https://www.surveymonkey.com/curiosity/why-people-share-passwords-with-coworkers/

- The risk of zero-accountability. If employees share credentials, it becomes impossible to monitor their activity. Who processed the insurance claim? Who authorized the payment? If tasks are done incorrectly the company can face serious issues without ever being able to identify the person responsible.

- The risk of an ex-employee being able to access confidential data. As long as the credentials remain the same, ex-employees can still gain access to company resources and sensitive company data. A study by Varonis[2], a cybersecurity company, on 785 organizations found that 40% of companies still had over 1,000 stale user accounts, many belonging to ex-employees who could still get access to company resources.

> **Sharing credentials increases the risk of data breaches and productivity issues, which can result in considerable monetary losses and serious legal problems.**

Why Do Employees Actually Share Credentials?

So, why do so many employees endanger their companies by sharing credentials when there are so many associated risks?

Though the practice of sharing credentials stems from back-office staff inefficiencies and inflexible IAM deployments, the two main reasons why employees share credentials are actually quite surprising.

The above-mentioned survey discovered that 42% of employees that share credentials said they do so in order to collaborate with colleagues; another 38% said they share credentials because it's company policy.

[2] https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

Some practical scenarios that could result in employees sharing credentials to confidential data:

- When the boss has gone on holiday and has asked someone to fill in.
- When an employee asks a colleague to help them with a task e.g. file an invoice.
- Due to a shortage on the ward, a doctor asks a nurse to help them with their rounds.

A simple glance atf the numbers tells us that 90% of the employees that share credentials do so with good intentions.

However, despite good intentions the risks are still huge and any company whose policy permits employees to share credentials needs to re-evaluate their security policy immediately.

So, the solution appears to be rather simple: better IAM management can wipe out 90% of credential sharing.

Sharing Access To Confidential Data Doesn't Require Sharing Credentials

Advanced authorization platforms are designed for the modern work environment and offer solutions for employees to share access to confidential data securely, without needing to share credentials.

These advanced authorization solutions are designed knowing that users come and go, tasks and responsibilities change, and different users require different types of access to data.

These solutions solve the challenges faced by traditional IAM implementations by delegating administration to the users themselves and reducing back-office administration. This prevents back-office inefficiencies and saves time and money.

Companies can design and enforce access policies through these access platforms. This way employees can grant access to others to view, change or otherwise manage confidential data as long as it falls within the boundaries of the access policy.

Delegating administration to employees results in quicker and more secure processes when:

- New employees are onboarded.
- Employees' access rights need updating.
- Employees no longer need access to specific company resources.
- Employees need to be offboarded.

To delegate administration to employees, these advanced authorization platforms provide self-service capabilities, letting employees invite colleagues to access confidential data through their own individual account, instead of sharing credentials.

For example, a doctor can invite a nurse to view and update a patient’s EHR.

Similarly, they provide self-service capabilities to let employees remove other employees’ authorizations when they no longer require access. Has the nurse moved departments? Remove the nurse from the team.

These platforms also provide peer-to-peer validation workflows that companies can customize to let authorized users approve someone else’s invite or request for access.

These functionalities let managers approve access in real-time for employees instead of waiting for the back-office to manually give permission.

They can also notify designated people when one user invites another or when someone has requested access. This lets managers conduct an audit to see who is getting access.

The same principles apply when employees leave the company. Self-service capabilities let authorized employees immediately withdraw the ex-employee's previous access rights, thereby protecting company resources by making the offboarding process quicker, instead of leaving the job to back-office staff.

Conclusion

Advanced authorization platforms provide solutions that remove the need for employees to share credentials and accounts to share access to confidential data. These solutions reduce reliance on back-office administration and let employees invite others to use their own account share access to company resources quickly and securely.

Of course, these solutions ensure access is always subject to the company's security policy.

Reducing back-office doesn't mean sacrificing security. Quite the opposite; advanced authorization solutions offer effective collaboration which means that employees no longer need to share credentials, and that company policy no longer needs to endorse credential sharing to enable collaboration.

> **Advanced authorization platforms provide solutions that remove the need for employees to share credentials and accounts to share access to confidential data.**